UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Anita Dravec

Varovanje tajnih podatkov v Republiki Sloveniji: formalni vidiki vs. praksa

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Anita Dravec
Mentor: doc. dr. Iztok Prezelj

Varovanje tajnih podatkov v Republiki Sloveniji: formalni vidiki vs. praksa

Diplomsko delo

Ljubljana, 2009

Mami Brigiti.

Želela bi se zahvaliti mentorju dr. Iztoku Prezlju, za strokovno vodenje in konstruktivna navodila pri pisanju diplomske naloge, mag. Milanu Tarmanu, g. Gregorju Klemenčiču in g. Roku Praprotniku za čas in voljo, ki so ju namenili za intervju ter mojim »ZTP-jevcem« za pozitivne misli v času pisanja diplome.

Hvala tudi moji družini, za podporo v času študija, Iztoku za pomoč pri oblikovanju diplome in Roku za »hruške in jabolka« ter vse objeme, ljubezen in vero, ki jo je imel vame.

VAROVANJE TAJNIH PODATKOV V REPUBLIKI SLOVENIJI: FORMALNI VIDIKI VS. PRAKSA

V diplomski nalogi so v prvem delu predstavljena zakonska določila in uredbe obravnavanja tajnih podatkov ter sistem varovanja tajnih podatkov v RS. Drugi del pa vsebuje pregled primerov in vidikov povezanih z delovanjem sistema varovanja tajnih podatkov v praksi. Uvodoma je predstavljen pojem tajnosti, javnosti, (nacionalne) varnosti in politične organizacijske ter varnostne kulture. V sistemski ureditvi so bolj podrobno predstavljeni varnostni standardi EU, NATO in RS ter zakonska ureditev obravnavanja tajnih podatkov. Na konkretnih primerih, ki so posledica pomanjkljivega delovanja sistema za varovanje tajnih podatkov ter preko mnenj intervjuvancev povezanih ali vključenih v ta sistem, je v drugem delu predstavljeno izvajanje zakonskih določil na tem področju v praksi. Ocenjena je tudi varnostna kultura posameznikov v RS in opravljena primerjava med normativnimi in praktičnimi vidiki obravnavanja in varovanja tajnih podatkov.

Ključne besede: tajni podatki, varnostna kultura, varnostni standardi, obravnavanje tajnih podatkov, odtekanje tajnih podatkov.

PROTECTION OF CLASSIFIED INFORMATION IN THE REPUBLIC OF SLOVENIA: THEORY VERSUS PRACTICE

The first part of this thesis introduces the regulatory provisions and acts for the handling of classified information and the system for protection of classified information in the Republic of Slovenia. The second part contains an overview of various cases connected to the practical execution of the system for protection of classified information. The introduction explains the concepts of confidentiality, the public, (national) security and political, organisational and safety culture. The safety standards of EU, NATO and the Republic of Slovenia and the legal regulation of handling classified information are thoroughly examined. The execution of regulatory provisions in practice is presented in the second part. It bases on cases, caused by the inadequate operation of the system for protection of classified information and by the opinions and views of individuals, connected to or a part of this system. Also, safety culture of individuals in the Republic of Slovenia is evaluated. The final part of the thesis features a comparison between the regulatory provisions and the practical processes of handling and protecting classified information.

Keywords: confidentiality, the public, classified information, safety culture, safety standards, handling of classified information, disclosure of classified information.

KAZALO

SEZNAM SLIK IN TABEL:

SLIKE

TABELE

SEZNAM KRATIC

BND	Zvezna obveščevalna služba (Bundes Nachrichten Dienst)
DZ	Državni zbor
EAPS	Evroatlantski partnerski svet
EK	Evropska komisija
ES	Evropski svet
ESPJ	Evropska skupnost za premog in jeklo
EU	Evropska unija
GŠSV	Generalštab slovenske vojske
MORS	Ministrstvo za obrambo
MZZ	Ministrstvo za zunanje zadeve
NACC	Severnoatlanstki svet za sodelovanje
NATO	Organizacija severnoatlantskega sporazuma (North Atlantic Treaty Organisation)
NSA	Nacionalni varnostni organ (National security authority)
OVS	Obveščevalno varnostna služba
OVSE	Organizacija za varnost in sodelovanje v Evropi
PzM	Partnerstvo za mir
RS	Republika Slovenija
SSKJ	Slovar slovenskega knjižnega jezika
SOVA	Slovensko obveščevalno-varnostna agencija
Ur. l. RS	Uradni list Republike Slovenije
UVTP	Urad vlade RS za varovanje tajnih podatkov
VOMO	Varnostni organ ministrstva za obrambo
ZDIJZ	Zakon o dostopu do informacij javnega značaja
ZDA	Združene države Amerike
ZEU	Zahodnoevropska unija
ZTP	Zakon o tajnih podatkih

1 UVOD

"... Obstaja varnostno tveganje ne le pred tem, da informacija pade v napačne roke, ampak tudi pred informacijami, ki ne najdejo poti v prave roke. Sedanji vladni pristop k varovanju tajnih podatkov ne prepoznava tveganja neuspeha delitve…«(Zoë E. Baird[1], 2005)

»V slovenski javnosti se je ustvarilo prepričanje o pravici vèdenja in obveščenosti z vsemi podatki in informacijami.« (Čaleta 2003, 1) A le nekateri(e), ki nastanejo oz. obstajajo v državnih organih, se morajo zaradi zavarovanja določenih državnih interesov in koristi določiti kot tajni, s čimer se njihova dostopnost bistveno omeji. »Če lahko trdimo, da je bilo razmerje[2] v času življenja v Jugoslaviji močno izraženo v korist državne zasebnosti, so demokratične spremembe, ki so se odražale v novi slovenski državi to razmerje močno nagnile na stran individualne zasebnosti.« (ibid.) Določitev podatkov in informacij za tajne sta v današnjem času lahko najenostavnejša možnost in način omejevanja javnosti dela državnih organov, ki se lahko zlorabljata za prikrivanje različnih nepravilnosti ali celo nezakonitosti v teh organih. Po drugi strani pa ohlapen odnos do instituta tajnosti podatkov lahko povzroči, da pridejo v javnost tudi podatki in informacije, s katerimi se lahko ogrozijo interesi in koristi države. Navkljub temu, mora država pri izvajanju nalog s področja nacionalne varnosti delovati tajno ter zavarovati svojo zasebnost.

Del sistema nacionalne varnosti je tudi varovanje tajnih podatkov. Pomen varovanja tajnih podatkov kaže na to, da vsi podatki niso in ne morejo biti prosto dostopni različnim zainteresiranim skupinam ali posameznikom, ampak velja načelo, da se smejo s pomembnimi informacijami in podatki, kadar so tako označeni, seznaniti samo upravičeni posamezniki. To je bistvo varovanja tajnih podatkov. Države z daljšo tradicijo imajo različne sisteme varovanja tajnih podatkov, ki pa se ne razlikujejo v temeljnih načelih. Eden izmed temeljnih pogojev, ki ga je Republika Slovenija (RS) morala izpolniti pred vstopom v EU (Evropsko unijo) in Organizacijo severnoatlantskega pakta (NATO), je vzpostavitev ustreznega sistema obravnavanja tajnih podatkov. Tako je kljub svoji »kratki tradiciji«, enakovredno pripomogla k zagotavljanju mednarodnega miru in stabilnosti, kajti globalizacija ni prinesla samo

[1] Zoë E. Baird je predsednica fundacije Markle; http://www.markle.org/. Fundacija Markle deluje za uresničitev celotnega potenciala informacijske tehnologije, za reševanje kritičnih javnih potreb, zlasti na področjih zdravstvenega varstva in nacionalne varnosti.
[2] Razmerje med individualno in državno zasebnostjo.

globalne trgovine, temveč tudi globalne grožnje in varnostne izzive. Standardi obeh organizacij v duhu tega predpostavljajo, da je način varovanja tajnih podatkov pri vsaki članici na taki ravni, da omogoča popolno medsebojno zaupanje pri izmenjavi podatkov brez dodatnega varnostnega dogovarjanja ali ukrepanja.

V uvodnem delu bi želela podati še kratko kronologijo mednarodnega sodelovanja pri obravnavanju tajnih podatkov, katera je sooblikovala razvoj slovenskega zakona in sistema na nacionalni, predvsem pa na mednarodni ravni. RS je na področju varovanja tajnih podatkov sklenila tri mednarodne sporazume. Kot pravi Jazbec (2002, 34), je na začetku leta 1994, pet let po koncu hladne vojne, zveza NATO ponudila zainteresiranim državam program Partnerstvo za mir (PzM)[3], kateri sporazum je bil podpisan 13. julija 1994. Drugi najobsežnejši in po vsebini tudi najbolj dodelan varnostni sporazum[4] je RS z Združenimi državami Amerike (ZDA) podpisala na področju varovanja vojaških tajnih podatkov. Še pred sprejetjem Zakona o tajnih podatkih (ZTP), pa je RS 24. julija 1998 podpisala tretji varnostni sporazum[5] z Zahodnoevropsko unijo (ZEU).

Pri svojem dosedanjem delu sem se srečevala z inštitutom tajnosti varovanja tajnih podatkov in ZTP. To me je vzpodbudilo k poglobljenemu zanimanju za to področje in hkrati pripomoglo k izbiri tematike za diplomsko delo. Najbolj sta me zanimala praktičen vidik in izvedba ZTP, hkrati pa tudi pojavi, ki so povezani z delovanjem, nedelovanjem oz. možnimi pomanjkljivostmi pri izvajanju le tega. Še dodatno pa me je zanimala percepcija področja varovanja tajnih podatkov, tako javnosti kot posameznikov, ki delujejo na podlagi ZTP.

[3] Program Partnerstvo za mir je bil sprožen januarja 1994, ko je zavezništvo države članice Severnoatlantskega sveta za sodelovanje in druge države članice OVSE povabilo, naj v skladu s svojimi posebnimi potrebami vzpostavijo individualne programe sodelovanja z NATO. Obseg dejavnosti, v katerih danes sodelujejo partnerske države, je zelo širok. Tako lahko program PzM na primer vključuje skupne vojaške vaje in urjenje, ima pa tudi pomembno politično razsežnost, saj vsaki dejavni članici PzM, ki ocenjuje, da je njena varnost ogrožena, omogoča posvetovanje z NATO. RS je l. 2004 postala polnopravna članica zveze NATO in je iz tega naslova sprejela tudi vse obveznosti na področju obravnavanja tajnih podatkov. Ob upoštevanju, da je RS partnerska država v PzM, sta RS in NATO podpisali varnostni sporazum (MVSOSP).(Ur. l. RS-MP, 23/97)

[4] Sporazum je RS podpisala 8. maja 1996 v Washingtonu. Nanaša se pa na vse varnostne ukrepe pri varovanju zaupnih vojaških podatkov. (Ur. l. RS, 57/1996)

[5] Sporazum (MVSZU) je nastal na temelju bonske deklaracije, ob dejstvu, da je za učinkovito sodelovanje potrebna izmenjava zaupnih informacij in gradiva med pogodbenicama. (Ur. l .RS, 20/99)

2 METODOLOŠKI OKVIR NALOGE

2.1 Opredelitev predmeta in ciljev preučevanja

Namen diplomskega dela je osvetliti problem razkrivanja tajnih podatkov znotraj sistema nacionalne varnosti RS. Razkrivalci informacij, posamezniki ali skupine, se v teh primerih obrnejo na širšo javnost in kritično opozorijo na sporne podatke oz. prakse določene institucije ali v obratnem primeru zasedajo delovna mesta, ki so zanimiva za določene osebe in institucije, ki pa ne izbirajo sredstev in načinov, kako pridobiti posameznika za sodelovanje z njimi. Obstaja veliko protislovij glede nastanka takšnega ravnanja, interpretacije s strani medijev in načina posredovanja, kot tudi glede razumevanja ravnanja s strani javnosti. Prav v tem zasledimo relevantnost naloge v sedanjem času, ko smo bili in smo soočeni z nekaterimi tovrstnimi primeri uhajanja tajnih podatkov.

V prvem delu diplomskega dela bom obravnavala varovanje tajnih podatkov v RS ter njihovo formalno-zakonsko ureditev in jo primerjala s praktičnim izvajanjem v drugem delu. Pomemben del tega raziskovanja bo tudi ugotovitev, kako je od obravnavanja tajnih podatkov odvisna varnostna kultura in kako le ta vpliva na to. V začetku bom zato predstavila nekaj osnovnih pojmov, ki gradijo temelje za razumevanje celotne vsebine naloge, kot npr. tajnost, javnost, (nacionalna) varnost ter politična, organizacijska in varnostna kultura.

Nadaljevala bom z opredelitvijo varnostnih standardov EU, NATO in RS. Za podrobnejši prikaz normativne ureditve področja tajnih podatkov v RS bo potreben prikaz sedmih merodajnih točk poslovanja s tajnimi podatki v RS, ki so v kontekstu preučevane teme diplome. Sklop sistemske ureditve varovanja tajnih podatkov v RS se bo zaključil s primerjavo klasifikacij RS, EU in NATO tajnih podatkov. Sem spada tudi Urad vlade RS za varovanje tajnih podatkov (UVTP), kot nacionalni organ za varovanje tajnih podatkov, katerega glavne naloge bom opisala in predstavila njegovo delovanje.

Kot že omenjeno, smo v praksi soočeni z razkrivanjem spornih podatkov, tako notranjim kot tudi zunanjim interesnim skupinam. Zato bom v nalogi preverila hipotezo, da se posamezniki oz. skupine obračajo na zunanjo javnost z izdajanjem tajnih podatkov pogosteje, če ne obstajajo ustrezni varovalni mehanizmi znotraj institucij. Ključno vprašanje na področju

varovanja tajnih podatkov leži v zavedanju pomembnosti posameznika, v sistemu nacionalne varnosti države. Razkrivanje tajnih podatkov lahko povzroča tako etična kot moralna vprašanja posameznika oz. skupine. Ravno »zavedajoč se vrednot in pomena posameznika za delovanje sistema nacionalne varnosti je Resolucija o strategiji nacionalne varnosti, ki jo je sprejel slovenski parlament julija 2001, kot zadnji, a nikakor ne najnepomembnejši temelj opredelila varnostno kulturo.« (Đorđević v Brezovšek in Črnec 2007, 19) Varnostna kultura je v širšem pomenu v tesni povezavi z vrednotami in stališči posameznika do ključnih vprašanj s področja nacionalne varnosti. V ožjem pomenu pa posega na področje organizacijske kulture in/ali politične kulture, oz. je njun sestavni del.

Cilj diplomske naloge je torej preučiti zakonsko ureditev obravnavanja tajnih podatkov v RS ter z analizo primerov javnega odtekanja opozoriti na pomanjkljivosti oz. nedosledno izvajanje obstoječe zakonske ureditve, oz. (ne)spoštovanje varnostnih standardov v RS. Posledično je moj namen tudi oceniti varnostno kulturo posameznikov v RS. Za analizo teme uhajanja tajnih podatkov, bodo uporabljeni članki, ki opisujejo primere takega dogajanja, in sicer afera SAVA, afera SOVA, afera WASHINGTONSKA DEPEŠA in afera PATRIA.

2.2 Hipoteze

Glavna hipoteza:

V RS prihaja med normativno ureditvijo (zakoni) in varovanjem tajnih podatkov v praksi do razhajanja, zaradi nespoštovanja varnostnih standardov, ki gradijo varnostno kulturo posameznikov.

Izvedene hipoteze:

a. Uhajanje tajnih podatkov v RS je izključno politično motivirano, z najvišjo frekvenco v predvolilnem obdobju.
b. Varnostna kultura, vpliva na spoštovanje varnostnih standardov v RS in s tem daje možnost uhajanja tajnih dokumentov v javnosti.
c. Sistem varovanja tajnih podatkov v RS ni optimalen, ker je v preveliki meri odvisen od delovanja posameznikov.

2.3 Uporabljena metodologija

Odgovor na vprašanje, kako se bomo lotili preučevanja problema, ki nas zanima, je povezan s pojmom metodologije. Preprosto povedano, metodologijo razumemo kot skupek načel in metod, ki jih uporabljamo pri raziskovanju določenega problema (Bučar, Šabič, Brglez z Kalin Golob 2002, 6).

Kot glavni metodi bom predvsem uporabljala analizo sekundarnih virov, kot so knjige, članki itd. in tudi analizo primarnih virov, kot so dokumenti, zakoni, ustava, podzakonski akti, uredbe… S tem bom v naslednjem poglavju opredelila temeljne koncepte, ki so ključni za konceptualizacijo naloge.

V četrtem poglavju, ki obravnava ureditev varovanja tajnih podatkov v RS, se bom tudi posluževala predvsem analize in interpretacije primarnih virov. Vzporedno s to metodo analize si bom pomagala še s primerjalnim raziskovanjem, da bom poiskala podobnosti in razlike med klasifikacijami tajnih podatkov RS, EU ter NATO.

V petem poglavju bom uporabila metodo študije primerov, s katero bom preučevala posamezne primere uhajanja tajnih podatkov. Za pridobitev podatkov o individualnih pogledih na varovanje in odtekanje tajnih podatkov bom uporabila še metodo intervjuja. Intervjuji so uporabno sredstvo za analizo, saj nam podobno kot metode anketiranja lahko omogočijo neposreden dostop do empiričnih podatkov, mogoča pa je tudi njihova neempirična metodološka uporaba, ko na podlagi intervjujev rekonstruiramo npr. zgodovinske dogodke. Ločimo med strukturiranimi in fokusiranimi intervjuji. V diplomskem delu bom uporabila strukturirani intervju, ki je sestavljen iz polzaprtih vprašanj. Glede na dejstvo, da bom preučevala varovanje tajnih podatkov v RS, sem se odločila, da bom opravila intervju z direktorjem Urada za varovanje tajnih podatkov, g. Milanom Tarmanom, z novinarjem časnika Dnevnik, g. Rokom Praprotnikom in g. Gregorjem Klemenčičem, vodjem Službe za varovanje tajnih podatkov na Ministrstvu za zunanje zadeve (MZZ). Vsem intervjuvancem je bila ponujena možnost vnaprejšnje seznanitve z vprašanji in snemanje zvočnega zapisa med potekom intervjuja.

3 OPREDELITEV TEMELJNIH POMOV

3.1 Tajnost

Že Anžič (2000, 849) je dal »fenomenu tajnosti na eni strani pomen vrednote in na drugi pomen zla.« Ta delitev nas opominja na dualnost samega pojma, ki ga bomo raziskovali ne samo v opredelitvi, temveč tudi skozi celotno diplomsko delo, kot antipod javnosti. Je namreč jedro tematike področja varovanja tajnih podatkov in varnostne kulture v RS. Multidisciplinarni pristopi, kot so sociologija, politologija, obramboslovje, pravo in psihologija pojma tajnosti[6] po besedah Anžiča (1997, 156) niso obravnavali in pojasnjevali, temveč kvečjemu zapletali; morebiti, ker naj bi šlo za stvari, ki so že same po sebi razumljive ali pa tudi zaradi enačenja s pojmom skrivnosti[7].

Tako kot pravi Žirovnik (2005, 1), je potrebno »določene podatke in informacije podrediti določenemu pravnemu režimu, s katerim se zaradi opredeljenih, legitimnih interesov in koristi omejuje njihova splošna dostopnost in uporaba.« Tako »tajnost ni nekaj neznanega, temveč ravno obratno. Pri njeni vsebini gre za znane stvari, ki jih njen »posestnik« (posameznik, institucija ali država) ne sme ali noče narediti dostopno širši javnosti. Tajnost torej pomeni obstoj znanih dejstev o družbenih, varnostnih, obrambnih, gospodarskih in drugih podatkih in informacijah, ki so posamezniku ali instituciji zaupani v uporabo in varovanje.« (Anžič 2000, 852)

Brezovšek in Črnčec (2007, 96) se ne strinjata s trditvijo, ampak jo delno zavračata in pravita, da »SSKJ namreč jasno opredeljuje skrivnost tudi kot sinonim tajnosti. V svojem drugem pomenu je skrivnost sinonim tajnosti. Skrivnost je: kar kdo ve, kar mu je zaupano in se ne sme pripovedovati drugim. Kot primer je ponazorjena poslovna, uradna in vojaška skrivnost.«

Temeljna predpostavka vsake demokratične vlade oz. oblasti je njena odgovornost do njenih volivcev in do javnosti. Kadar je neka politika vlade označena kot tajna, te odgovornosti ni in je ne more biti, saj javnost s tem ni seznanjena (Brezovšek in Črnčec 2007, 95).Tu pa obstaja

[6] Kot pravi Anžič (1997,156), je beseda tajnost prevzeta iz drugih slovanskih jezikov. Upoštevati velja, da se je raba izraza tajnost v slovenskih predpisih povečala pod vplivom jugoslovanske zakonodaje, kjer se je uporabljal izraz »tajna«.

[7] Anžič govori, da je pomembno, da tajnosti v smislu varovanja znanega in za širšo javnost nedostopnega, ne enačimo s pojmom skrivnosti, ki je nekaj nerazumljivega, nerazložljivega, nikoli odkritega in predstavlja misterij.

nevarnost, da bi načelo zasebnosti za državo prevladovalo nad načeli zakonitosti in ustavnosti, zato mora »pravna država, pojem tajnosti skrbno, tudi kazenskopravno varovati, redko uporabljati in še to po vnaprej predvidenih pravnih pogojih in okvirih.« (Anžič 1996, 67-68)
Iz drugega zornega kota je tajnost lahko dobrina, če uspejo tisti, ki bi jo morali varovati, zavarovati in preprečiti odliv informacij in podatkov, s katerimi se lahko ogrozijo interesi posameznikov, institucij in države (Anžič 2000, 854).

V sodobni demokratični državi lahko obstoj tajnosti opravičujejo tudi naslednji razlogi:

- obstoj nasprotujočih si interesov;
- izrecno pravno opredeljeni interesi, ki so predmet varovanja tajnosti;
- kršitev tajnosti mora predstavljati posamezniku ali družbi nevarno ali škodljivo ravnanje;
- tajnost mora biti namenjena varovanju, obrambi in zaščiti obstoja države, njene ustavne ureditve ali posebnim interesom pri varovanju človekovih pravic;
- s pravno normo morajo biti določeni podatki označeni kot tajni, imenovani morajo biti upravljavci tajnosti in ti podatki morajo imeti ustrezno stopnjo in vrsto tajnosti;
- določeni morajo biti ukrepi za varovanje tajnih podatkov, s katerimi se preprečuje njihovo prilaščanje, neopravičeno odstopanje, spreminjanje ali pridobivanje (Anžič 1997, 156).

Medtem ko iz določb Ustave RS med drugim izhaja tudi obveza državnih organov, da ima »…vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon.« (Ustava RS, 39. člen), je razumljivo, da načelo javnosti dela in dostopnosti do podatkov in informacij državnih organov ne more veljati absolutno in neomejeno.

3.2 Javnost

Vprašanji javnosti (publicitete) in dostopnosti do podatkov in informacij sta neločljivo povezani z vprašanji ureditve varovanja tajnih podatkov in pojmom tajnosti. Kot ugotavlja Slavko Splichal (1997, 22), »je pojem javnost proizvod razsvetljenstva«. Od razsvetljenstva naprej so ga obravnavali na več načinov: kot specifično družbeno teorijo, ki se v odnosu do

dogajanja pojavlja kot subjekt-družbeni akter, kot specifično naravo prostora ali dejavnosti, kot neko določeno področje, kot sta domena ali javna sfera družbenega življenja in kot preplet vseh treh naštetih načinov.

Pojem javnosti dobi svoj sodobni pomen šele, ko se vzpostavi neko medsebojno razmerje med državo in civilno družbo, demokracijo in pravno državo ter med državljani, ki o javnih problemih javno razpravljajo (Škerlep 2002, 154). Kot govorita tudi Splichal in Vreg (1986), je javnost vir zakonodajne volje, legitimnosti odločitev in ne nazadnje demokratičnega nadzora, kar velja tako za državne, samoupravne, delegatske in politične strukture, kot tudi za komunikacijske sisteme.

Kljub temu da imamo v Sloveniji že od leta 1991[8] ustavno pravico dostopa do informacij javnega značaja urejeno v drugem odstavku 39. člena Ustave RS, je bil Zakon o dostopu do informacij javnega značaja (ZDIJZ)[9] sprejet šele leta 2003. Vendar pa se je že v kratkem času uporabe tega zakona izkazalo, da pomeni široko in temeljno spremembo v načinu delovanja državnih organov in drugih zavezancev za omogočanje dostopa do informacij javnega značaja. Zavedanje organov o potrebi po javni preglednosti in transparentnosti njihovega delovanja se je v kratkem času močno povečalo, kar je eden glavnih pogojev za demokratični nadzor javnosti nad izvršilno, pa tudi nad drugimi vejami oblasti.

Kot pravi Bohinc (2001, 5), predstavlja javnost dela državnih organov ter transparentnost njihovih odločitev in ukrepov temeljno sestavino sodobnih demokratičnih družbenih ureditev. Podobno meni tudi Rovšek (2001, 35-36), ki pravi, da javnost dela državnih organov, odprtost in preglednost (transparentnost) njihovega dela, v povezavi z možnostjo dostopa do tajnih podatkov in informacij javnega značaja, značilnost sodobne demokratične in pravne države. Z ustreznim obveščanjem, odprtostjo in možnostjo nadzora se krepi zaupanje državljanov v delo državnih organov in javne uprave v širšem pomenu.

Država je namreč organizacija, ki smo ji državljani zaupali izvrševanje različnih zadev, ki so v našem skupnem interesu. Za izvajanje njenih nalog ji državljani plačujemo davke in druge javne dajatve. Torej je povsem logično, da je naša temeljna pravica biti seznanjen s prav

[8] 25. junija 1991 je bila razglašena neodvisnost Slovenije od SFRJ.
[9] Zakon je bil spremenjen in dopolnjen leta 2005.

vsemi informacijami, ki zadevajo delovanje države. Država (oziroma njeni organi) lahko to pravico odreče le izjemoma (Bohinc in Pirnat 2005, 19).

V primeru, da je delovanje organov zaprto, je veliko več možnosti za nepravilnosti, zlorabe oblasti in različne oblike korupcije. Smisel varovanja tajnih podatkov, ki to niso (zaradi namenskega prikrivanja sicer javnih informacij ali neusposobljenosti javnih uslužbencev pri označevanju tajnosti podatkov), ni v prid preglednemu in javnemu delovanju organov javne uprave.

3.3 (Nacionalna) varnost

Zagotavljanje varnosti je vprašanje, ki se pojavlja na različnih stopnjah družbe in družbenih ureditev. Kot eden osrednjih družboslovnih terminov zajema zelo široko področje, zato lahko govorimo, da se nanaša na posameznika, skupnost, narod, vse od mednarodne pa do regionalne ravni. V svoji nalogi se osredotočam samo na tiste vidike varnosti, ki se dotikajo varovanja tajnih podatkov in s tem povezanih področij.

Za razumevanje problematike nacionalne varnosti je potrebno najprej razumeti koncept varnosti. Pojem varnosti posega v vsa področja človekovega delovanja, v vse njegove aktivnosti. Kot pravi Grizold (1999, 23), je varnost stanje, v katerem je uravnotežen fizični, duhovni, duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave. Tako Buzan (1991, 35) kot Grizold (1991, 1-13) ugotavljata, da si država, ko sistemsko zagotavlja varnost članom družbe, posredno krepi moč, s katero dejansko ali potencialno ogroža varnost teh istih posameznikov, katerim naj bi jo zagotavljala. Tukaj lahko vključimo vidik Anžiča in Terbovška (2003, 1) o tem, da je »varnost družbena in politična vrednota, ki označuje okvir socialne in politične skupnosti«. Iz teh istih političnih skupnosti pa naj bi izhajale nenehne napetosti, ki jih ni mogoče povsem odpraviti.

V novejšem času (predvsem po koncu hladne vojne)[10] pridobiva na pomenu preučevanje razmerij med varnostjo posameznikov in nacionalno varnostjo (Mitar 2008, 23). Zagotavljanje nacionalne varnosti oz. problematika le-te, se je pojavila z rojstvom nacionalne države (v Evropi v 16. in 17. stoletju) in se je navezala na zagotavljanje njenega nadaljnjega obstoja in razvoja (Grizold 1998, 3). Ker pa je posameznikova varnost prepletena z nacionalno varnostjo, se posledično prepletata tudi fenomena njune ogroženosti (Anžič 1997, 37). Grožnje nacionalne varnosti na splošno opredelimo kot vse družbene ali naravne pojave, ki zmanjšujejo nacionalno varnost oziroma njene definicijske prvine. To se še posebej nanaša na onemogočanje fizičnega obstoja prebivalstva, motenje ali onemogočanje normalnega delovanja temeljnih družbenih in državnih struktur (oziroma infrastruktur), onemogočanje izvajanja politične suverenosti in preprečevanje relativno nemotenega družbenega razvoja (Prezelj 2007, 7).

»Sodobne družbe imajo na razpolago različne institucionalne in neinstitucionalne mehanizme in instrumente zagotavljanja svoje varnosti. Strukturno–metodološki izraz prvih je nacionalno-varnostni sistem.« (Grizold 1998, 11) Nacionalno-varnostni sistem vsake države je temeljnega pomena, saj ima funkcijo »varovanja in uresničevanja vrednot družbe«[11].
Edmonds (Grizold 1998, 12) ugotavlja, da civilna družba in politična država postavljata nacionalno-varnostnemu sistemu zahteve in pričakovanja tako glede učinkoviti opravljanja funkcije zagotavljanja varnosti, kot tudi, da bo ta funkcija opravljena v skladu z zakoni in institucijami demokratičnega političnega sistema. V primeru neusklajenosti med okoljem in nacionalno-varnostnim sistemom lahko pride do prevladovanja zahtev in pričakovanj okolja ali nacionalno-varnostnega sistema, kar vpliva na nestabilnost nacionalne varnosti. Idealna rešitev tega problema je ravnotežje vrednot in prepričanj, ki temelji na zaupanju med javnostjo, politično državo in nacionalno-varnostnim sistemom. To zaupanje pa je mogoče doseči le v primeru, ko je sodelovanje vseh sodelujočih javno, odgovorno in je izpostavljeno kritiki ter nadzoru.

[10] Konce hladne vojne je prinesel pomembne in opazne spremembe v pojmovanje varnosti kot enega klasičnih in osrednjih družboslovnih terminov. Tradicionalno pojmovanje varnosti je verjetno najbolj očitno oz. prepoznavno, kadar je postavljeno v koncept mednarodnih odnosov, kjer je s tradicionalnega vojaško-političnega vidika varnost razumljena kot preživetje (Buzan, Waever, de Wilde 1998, 195).
[11] Deklaracija o zunanji politiki Republike Slovenije, Ur. l. RS, št. 108/99.

3.4 Politična, organizacijska in varnostna kultura

Koncept politične kulture je v obliki in vsebini, kakršni ji danes pripisujemo, precej kratek. Na drugi strani je definicij veliko, popolnoma pa je pojem vpeljal šele Gabriel A. Almond, ki je izhajal iz teoretičnih del Talcotta Parsonsa (Južnič 1989, 205). Gabriel A. Almond je v petdesetih letih prejšnjega stoletja v svoji klasifikaciji političnih sistemov natančneje opredelil politično kulturo kot »določen vzorec usmerjenosti v politično akcijo« (Almond v Lukšič 2006, 37). Na drugi strani pa Kolenc (1993, 111) pravi, da je politična kultura »mreža individualnih orientacij in stališč pripadnikov družbe do političnega sistema, pri čemer je ravno politična kultura tista, ki vpliva na politični sistem.« Almond in Verba (1963, 493) ugotavljata, da je civilna kultura tista politična kultura, ki povzroča in vzdržuje stabilnost demokracije.

Varnostna kultura v ožjem pomenu posega na področje organizacijske kulture in/ali politične kulture, oz. je njun sestavni del. Vrednote v uspešni organizaciji morajo biti jasne, o njih mora v kolektivu obstajati soglasje in zaposleni se morajo intenzivno oz. čustveno čutiti zavezane ključnim vrednotam. Vrednote so zelo pomembne tudi za učinkovito in uspešno delovanje nacionalno-varnostnega sistema. Vrednote so vir vsakršnega družbenega dogajanja, delujejo pa na dva načina: posameznika lahko motivirajo in usmerjajo v ustvarjalno dejavnost ali pa ga zavirajo. V tem primeru je človek demotiviran in lahko deluje asocialno, destruktivno. Posamezniki in skupine uveljavljajo svoje vrednote le v odnosih med ljudmi in v odnosu do okolja. Okolje (pravna, demokratična država) je lahko zdravo, lahko pa je nezdravo (diktature ipd.) (Anžič 1997, 25). Organizacijska kultura je sredstvo, ki ga vodje lahko uporabijo za oblikovanje učinkovite organizacije (Žurga 2001, 34) ter za oblikovanje učinkovitega sistema. Nadzor in razumevanje sta ključni odgovornosti vodij ter temeljno orodje (Žurga 2004, 46) za doseganje rezultatov, v skladu s potrebami sistema nacionalne varnosti.

Izjemno pomembna je človekova predstava o tem, kaj »človek sploh je« in iz tega izvirajoče domneve in stališča, ki zadevajo, pripadništvo človeški vrsti. Pa ne le to, gre za vrednotenje te pripadnosti, ki lahko variira glede na svetovni nazor kot »strukture stvari«, ki se jih človek zaveda. Med njimi se seveda najbolj zaveda človeškosti, ki pa ji prav gotovo pripisuje različne pomene (Južnič 1989, 53).

Vršec (2003, 8) ugotavlja, da varnostna kultura pomeni »zavest, da ima vsakdo pravico in dolžnost poskrbeti za lastno varnost in hkrati prispevati k varnosti bivalnega, delovnega, poslovnega in širšega okolja. Toda vedeti je treba, da je raven varnostne kulture odvisna od organizacijske kulture, zavarovalniške kulture in poslovne etike delovnih in poslovnih okolij. Profesionalno in osebno dolžnost razvijanja varnostne kulture zaposlenih in ostalih državljanov imajo torej državne institucije, izobraževalne organizacije, lastniki premoženja, management in varnostni strokovnjaki.« Tudi Kavčič (1991, 129) ugotavlja, da so vrednote in stališča posameznika neposredno povezane s percepcijo in razumevanjem politične, organizacijske in varnostne kulture. Varnostna kultura oz. bezbednosna kultura (Đorđević v Brezovšček in Črnčec 1986, 23) je »del splošne kulture posameznika, določene skupnosti ali organizacije. Zbir znanj s področja varnosti…, ki omogočajo posamezniku, skupini ali organizaciji, da prepozna metode, oblike in sredstva, ki jih ogrožajo, ter da prepozna vire ogrožanja, ne glede na to, kje in kako se izkazujejo.«

V okvir širšega pojmovanja varnostne kulture bi lahko umestili vprašanja, kot so: v kakšni vlogi se vidijo posamezniki znotraj sistema nacionalne varnosti, kakšen je njihov odnos do vojaškega poklica, do Slovenske vojske, do mirovnih gibanj, ali so pripravljeni sodelovati z obveščevalno-varnostnimi službami, kako bi se obnašali ob oboroženi agresiji na Slovenijo ipd.(Grizold 1998, 125-130).

Vsekakor so z varnostno kulturo v tesni povezavi pojmi, kot so verodostojnost, lojalnost, varovanje tajnosti, zanesljivosti ipd., ker pa je »varnostna kultura pojem, ki vključuje tudi vedenje ljudi, se le-to kaže v obvezi in delovanju vsakega posameznika in vseh za varnejše in bolj zdravo življenje. K takemu vedenju prispevajo znanje o varnosti, pozitivna stališča do varnega vedenja in spretnosti ter navade, pomembne za varnejše vedenje. Ponavadi se zgodi, da so pri ljudeh stališča in vrednote pozitivni, zavzemajo se za večjo varnost, njihovo vedenje pa s tem ni skladno. To je treba upoštevati tudi pri izobraževanju, saj ni dovolj, da se prenaša zgolj znanje (zakonitosti in spoznanja), ampak mora izobraževanje potekati tudi na ravni vedenja. Le tako lahko pričakujemo, da se bodo spremembe prenesle tudi v vsakdanje situacije, v realno življenje (Zabukovec 2000, 15).

4 SISTEMSKA UREDITEV VAROVANJA TAJNIH PODATKOV V REPUBLIKI SLOVENIJI

Kozlevčar (2007,8) ugotavlja, da se je sistem varovanja tajnih podatkov v RS pričel vzpostavljati v obdobju osamosvojitve, ko je država morala na novo urediti zakonodajo, kar je bil velik projekt. Sicer so se področja delovanja države urejala postopoma, pa vendarle. Prvi predpis, ki se je lotil urejanja področja tajnih podatkov, je bil Zakon o obrambi in zaščiti (ZOZ) (Ur. l. RS, št. 15/91), v katerem je bila tudi pobuda za sprejetje podzakonskih predpisov, ki bodo urejali varovanje tajnih podatkov. Na tej osnovi sta bila sprejeta v letu 1992 Odlok o varnostnih ukrepih na obrambnem področju (Ur. l. RS, št. 49/1992) in v letu 1993 Navodilo za izvajanje posebnih ukrepov za varovanje dokumentov in drugih predpisov, ki so določeni kot obrambna državna skrivnost oz. vojaška ali uradna skrivnost s stopnjo »strogo zaupno« (Ur. l. RS, št. 38/1993). Tako sta področje tajnih podatkov do leta 2001 urejala navedeni odlok in pravilnik.

Ko govorimo o sistemski ureditvi varovanja tajnih podatkov, se moramo zavedati dejstva, da je pomembna izvedba vseh ukrepov, s katerimi se gradi. Sistem varovanja tajnih podatkov mora zagotavljati kontinuirano izvajanje teh ukrepov (fizičnih, organizacijskih in tehničnih)[12], ki jih predvideva ZTP, po drugi strani pa mora zagotavljati operativnost v svojih postopkih, ki morajo biti čim manj moteči za posameznika in delovanje sistema (Čaleta 2003, 1). Zavedati se namreč moramo, da še tako dober sistem varovanja tajnih podatkov ne pomeni ničesar če nimamo dobro usposobljenih ljudi, ki se z njimi ukvarjajo (Korošec 2006, 57).

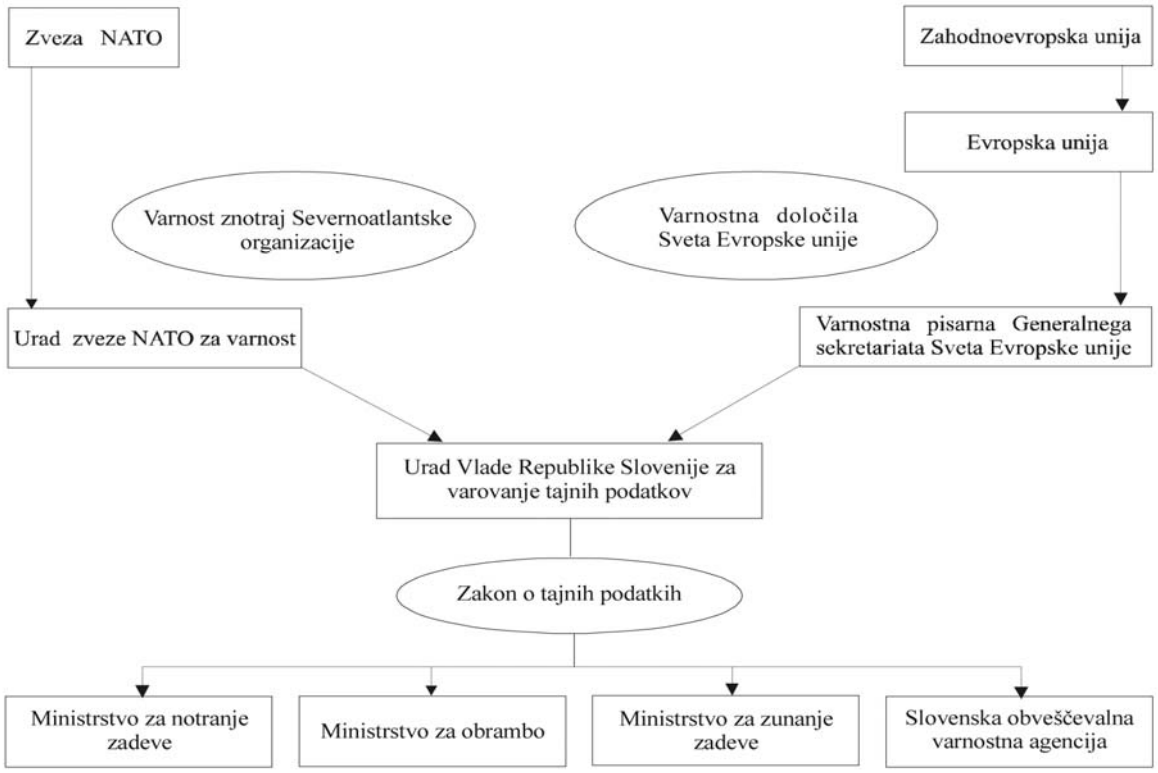
»Ker danes živimo v svetu globalizacije, si je nemogoče predstavljati, da slovenski varnostni sistem ne bi bil vpet v mednarodnega. Še bolj je to dejstvo postalo očitno in pomembno ob vključitvi RS v EU in v zvezo NATO. Izgradnja sodobnega sistema varovanja tajnih podatkov je bil nujni predpogoj za dobro sodelovanje na področjih varovanja tajnih podatkov. Slovenija ob svojem delovanju v okviru teh dveh organizacij namreč razpolaga s številnimi tajnimi podatki drugih držav članic zveze. In varnostni sistem oziroma sistem varovanja v organizacijah, kot sta NATO in EU, je trden le toliko, kolikor je trden najšibkejši sistem

[12] Terminologija, ki jo poznata NATO in EU, se nekoliko razlikuje od opredelitve, ki jo za varovanje tajnih podatkov poznamo v Sloveniji.

države članice.« (Črnčec 2003, 17) Prav tako je pomembna vzpostavitev vseh delov sistema v vseh državnih organih. Država, ki ustrezno varuje svoje in tuje državne podatke, je v mednarodni skupnosti sprejeta kot zaupanja vreden partner (Hartman 2007, 93). Zahteve NATA in EU v procesu približevanja Slovenije obema zvezama so bile usmerjene predvsem v postavitev takega nacionalnega sistema varovanja tajnih podatkov, ki bo primerljiv z njihovimi standardi. Ni nujno, da je nacionalni sistem varovanja tajnosti države članice enak zahtevam EU ali NATA, mora pa omogočiti spoštovanje njunih standardov in predpisov, kadar v državah članicah obravnavajo tajne podatke ene ali druge zveze (Čaleta 2004).

Slika 4.1 prikazuje sistem varovanja tajnih podatkov v EU, kateri je sestavljen iz varnostne pisarne Generalnega sekretariata Sveta EU, ki je bila ustanovljena z namenom koordiniranja, nadziranja in uvajanja varnostnih ukrepov. Ena izmed nalog vodje varnostne pisarne je tudi, da koordinira delo z nacionalnimi UVTP EU. Urad zveze NATO za varnost (slika 4.1.) pa usklajuje, spremlja in uresničuje NATO varnostno politiko ter prav tako koordinira tudi delo z nacionalnimi UVTP.

SLIKA 4.1: Sistem varovanja tajnih podatkov v zvezi NATO, EU in RS



Vir: Černetič in Brožič (2003, 578).

4.1 VARNOSTNI STANDARDI VAROVANJA TAJNIH PODATKOV

4.1.1 Varnostni standardi EU

Za članstvo v EU je od marca 1994 do junija 1996 zaprosilo deset evropskih držav, med njimi tudi Slovenija. Evropski svet (ES) je decembra 1997 v Luksemburgu sprejel poročilo Evropske komisije (EK), naj se uradno začnejo pogajanja s šestimi državami, in sicer s Češko, z Estonijo, z Madžarsko, s Poljsko, s Slovenijo in s Ciprom. S sklepom vrha v Helsinkih konec leta 1999 so se t.i. luksemburški skupini držav kandidatk v pogajanjih pridružile še Bolgarija, Latvija, Litva, Romunija in Slovaška. Uradna pogajanja Slovenije z EU so se začela 31. marca 1998 s prvo pristopno konferenco na ravni glavnih pogajalcev (zunanjih ministrov). 2. aprila 1998 je vlada imenovala ožjo pogajalsko skupino za pristop RS k EU. Ožja pogajalska skupina se je pogajala o prevzemu pravnega reda EU do leta 2002, ki predstavlja podroben pregled zakonov in drugih predpisov, ki jih je potrebno sprejeti za prilagoditev slovenskega pravnega reda pravnemu redu Skupnosti kot pogoj za vključitev Slovenije. Pogajanja so bila razdeljena na 30 pogajalskih področij. Področje, ki je za to nalogo najbolj aktualno, je področje »pravosodje in notranje zadeve«. Področje obravnava migracije, azil, varstvo osebnih in tajnih podatkov (Černetič in Brožič 2003, 577).

Varnostni standardi v EU so neposredno povezani z ZEU. ZEU in Severnoatlantski pakt sta osnove varnostnih standardov gradili na vojaških in obrambnih osnovah, kar je razvidno iz varnostnih sporazumov. V dodatku[13] h končnemu aktu iz Amsterdamske pogodbe[14] je bilo dogovorjeno, da se ZEU integrira v EU v procesu razvoja skupne zunanje in varnostne politike v okviru zavezništva zveze NATO. V skladu s tem dogovorom je bila izdana deklaracija[15] o razširjenem sodelovanju med EU in ZEU. Deklaracija določa, da se z namenom razširitve sodelovanja skliče konferenca, kjer bo navzoč Svet EU. Glavni cilj konference bo določitev in uskladitev varnostnih standardov s področja varnostnega preverjanja v Generalnemu sekretariatu Sveta EU. Navedena je bila osnova za pripravo

[13] *Declaration No. 3, Declaration of Western European Union on role of Western European Union and its realtions with European Union and with the Atlantic Allience, 22. julij 1997*
[14] Amsterdamska pogodba je bila podpisana 2. oktobra 1997 in je začela veljati 1. maja 1999.
[15] *Declaration No. 2, Declaration on enhanced cooperation between the European Union and the Western European Union, 22. julij 1997*

Varnostnih določil Sveta EU. Varnostna določila Sveta EU[16] (*Security Regulations of the Council of the Europoean Union*) so bila sprejeta 19. marca 2001 v Bruslju in so pričela veljati 1. decembra 2001. Varnostna določila urejajo organizacijo varnosti v Svetu EU, klasifikacijo in označevanje dokumentov glede na stopnjo tajnosti, fizično varnost v objektih in okoliših, osnovne principe dostopa do tajnih podatkov[17] in varnostno preverjanje, pripravo, distribucijo, pošiljanje, hranjenje in uničevanje tajnih podatkov EU. Varnostna določila predpisujejo ustanovitev posebnega registra za hranjenje strogo tajnih podatkov EU. Posebno poglavje obravnava varovanje tajnih podatkov s področja informacijske tehnologije in komunikacijskih sistemov in postopke za odobritev dostopa do tajnih podatkov tretjim državam, torej nečlanicam EU. Varnostna določila Sveta EU veljajo za Svet EU, Generalni sekretariat Sveta EU in vse države članice. Definirajo pojem tajni podatki in oblike potencialnega ogrožanja tajnih podatkov. Določajo, da mora vsaka država članica imeti nacionalni varnosti urad[18] (*National Security Organisation*). Varnostna določila Sveta EU določajo, da imajo dostop do tajnih podatkov EU samo osebe, ki se morajo s takimi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog[19]. Navedeno pomeni, da bodo v državah članicah morali biti varnostno preverjeni vsi tisti zaposleni, ki bodo pri svojem delu potrebovali tajne podatke EU v sami državi članici in pa vsi tisti, ki bodo državo članico predstavljali v institucijah EU in bodo pri svojem delu potrebovali njene tajne podatke (Černetič in Brožič 2003, 579).

4.1.2 Varnostni standardi NATO

Varnostne zahteve in postopki za varovanje NATO tajnih podatkov[20] so temeljni akt oziroma predpis, ki v zavezništvu NATO ureja področje varovanja tajnih podatkov. Nekateri avtorji standardizirane postopke v zavezništvu NATO na kratko imenujejo Dokument C-M (55) 15 (FINAL), kar pa je samo delno ime predpisa. Predpisani standardi veljajo v vseh državah članicah NATO. Prvotni standardi so bili sprejeti s soglasjem vseh držav članic NATO v letu

[16] *Security Regulations of the Council of the Europoean Union, Official Journal of the European Communities (2001/264/EC) L 101/*
[17] Princip »*need to know*« pomeni, da oseba, ki je sicer preverjena za dostop do določene stopnje tajnosti in ima ustrezno varnostno potrdilo oziroma dovoljenje, dostopa do podatkov v okviru navedene stopnje tajnosti, vendar samo v okviru svojega dela.
[18] V Sloveniji je to UVTP.
[19] *Need to know*.
[20] *Security Requirements and Procedures for the Protection of Nato Classified Information and Meetings (Document C M (55) 15 (Final), 1997)*

1955 in veljajo v vseh državah članicah. Do standardov, ki veljajo danes in so bili nazadnje spremenjeni 1997. leta, je bilo potrebnih dve večji in več manjših prenov, predvsem z varnostnega in tehnološkega vidika. V povezavi z dogodki 11. septembra 2001 je prišlo na področju varnosti do nekaterih sprememb, kar se je odrazilo tudi na varnostnih standardih zveze NATO. Tako je s 17. junijem 2002 zgoraj navedene standarde zamenjal dokument CM (2002)49, C-M(2002)50 in AC/35-D/2000 (Černetič in Brožič 2003, 577).

Urad zveze NATO za varnost usklajuje, spremlja in uresničuje NATO varnostno politiko. Direktor je glavni svetovalec generalnega sekretarja za varnostna vprašanja in predsednik NATO odbora za varnost. Poleg tega tudi usmerja Varnostno službo na sedežu NATO in je zadolžen za celovito koordinacijo varnosti znotraj NATA. Urad zveze NATO za varnost koordinira delo z nacionalnimi UVTP (*National Security Autority*)[21].
17. junija 2002 so pričeli veljati novi varnostni standardi zveze NATO. Varnost znotraj Severnoatlantske organizacije (*Security Within the North Atlantic Treaty Organisation, Document CM (2002)49*) sestavljajo naslednja poglavja:

- AC/35-D/2000; Direktiva o varnostnem preverjanju- določa načine in postopke varnostnega preverjanja, stopnje tajnosti, postopke ponovnega varnostnega preverjanja, kriterije za varnostno preverjanje.
- AC/35-D/2001; Direktiva o fizični varnosti- določa načine in postopke izvajanja fizičnega varovanja objektov in okolišev, ki so posebnega pomena za varovanje tajnih podatkov in objektov.
- AC/35-D/2002; Direktiva o informacijski varnosti- določa načine in postopke ravnanja na področju informacijske varnosti, predvsem s poudarkom na tehničnih rešitvah informacijske varnosti.
- AC/35-D/2003; Direktiva o industrijski varnosti- določa načine in postopke varovanja tajnih podatkov, ki so posredovani drugim organizacijam ali izvajalcem, pri čemer je vključeno tako varnostno preverjanje zaposlenih kot tudi zagotavljanje fizične varnosti objektov in opreme.
- AC/35-D/2004; Osnovna direktiva za INFOSEC18- določa načine in postopke ravnanja na področju informacijske varnosti, predvsem s poudarkom na informacijskih rešitvah informacijske varnosti.

[21] V Sloveniji je to UVTP.

- AC/35-D/2005; INFOSEC direktiva za organizacijo CIS19- določa načine in postopke ravnanja na področju informacijske varnosti, predvsem s poudarkom na organizacijskih rešitvah in uvajanju novih tehnologij na področju informacijske varnosti (Černetič in Brožič 2003, 579).

K dokumentu CM(2002) 49 sodi tudi dodatek o varnostnih merilih proti terorističnim grožnjam (*Protection Measures for Nato Civil and Military Bodies Deployed Nato Forces and Installations against Terrorist Threats*). V povezavi z varnostnimi standardi zveze Nato je potrebno vzpostaviti enotna merila za ugotavljanje lojalnosti, zanesljivosti in vrednosti zaupanja v posameznika, ki bo imel dostop do tajnih podatkov zveze Nato. Da bi navedeno dosegli, mora vsak posameznik, ki pri svojem delu potrebuje dostop do tajnih podatkov, pridobiti ustrezno varnostno potrdilo (*Personnel Security Clearance - PSC*) z določeno časovno veljavnostjo (Černetič in Brožič 2003, 579).

4.1.3 Varnostni standardi RS

Černetič in Brožič (2003, 579) ugotavljata, da smo s sprejetjem ZTP v RS zadostili zahtevam pogajalskih izhodišč za vstop v EU v poglavju 24 »Pravosodje in notranje zadeve[22]«. Zakon je na nivoju države združil nekatera področja varovanja tajnih podatkov, ki so sicer že bila delno urejena v posameznih zakonih oziroma podzakonskih aktih. ZTP je v splošnih določbah opredelil temeljne pojme, kot so tajni podatek, dokument, določanje tajnih podatkov, prenehanje tajnosti podatkov, varnostno preverjanje, varnostni zadržek. Poleg splošnih določb vsebuje še poglavja o določanju tajnih podatkov, dovoljenju za dostop do tajnih podatkov, dostop do tajnih podatkov in njihovo varovanje ter nadzor nad izvajanjem zakona. V skladu z določbami ZTP so bili v letu 2002 sprejeti še naslednji podzakonski akti:

- Uredba o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov, ki ureja označevanje, obdelavo in shranjevanje, prenos tajnih podatkov, razmnoževanje, evidentiranje in uničevanje in arhiviranje, načrte varovanja in usposabljanje na področju tajnih podatkov;

[22] Področje »Pravosodje in notranje zadeve« je bilo v procesu pogajanj razdeljeno na štiri podpodročja, in sicer na migracije, azil ter varovanja osebnih in tajnih podatkov.

- Uredba o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov, ki ureja začetek postopka, definira, kdo so udeleženci v postopku, opredeli varnostni vprašalnik, določa ravnanje z vprašalnikom in varnostno preverjanje, preverjanje podatkov iz vprašalnika, razgovor s kandidatom, oceno o ugotovitvah varnostnega preverjanja, izdajo odločbe, vročitev dovoljenja, preklic dovoljenja in odločanje o ugovoru;
- Uredba o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi, ki ureja oblike nadzora, splošni nadzor, tematski nadzor,opravljanje nadzora, preverjanje odprave pomanjkljivosti, izvajalce nadzora, vsebino nadzora in poročilo o nadzoru;
- Pravilnik o načinu in postopku določanja tajnih podatkov s področja obrambe v gospodarskih družbah, zavodih in organizacijah;
- Uredba o ugotavljanju izpolnjevanja pogojev za posredovanje tajnih podatkov drugi organizaciji. Po tem zakonu se morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev, katerim se tajni podatki posredujejo zaradi izvršitve naročil organa. Varovanje in dostop do tajnih podatkov tuje države ali mednarodne organizacije se izvaja v skladu z ZTP ali s predpisi, izdanimi na njegovi podlagi, oziroma v skladu z mednarodno pogodbo, ki jo je s tujo državo ali z mednarodno pogodbo sklenila RS. Pravico do dostopa do tajnih podatkov imajo 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 tiste stopnje tajnosti, ki je določena v dovoljenju;

ZTP je bil sprejet v DZ (Državnem zboru) 23. novembra 2001 in je stopil v veljavo decembra l. 2001. Kot pravita Brezovšek in Črnčec (2007, 15) postavil je »pravila igre« na področju varovanja zasebnosti države, v nasprotju s preteklostjo, ko je to področje bilo urejeno le do neke mere in je »ravnanje z zaupnimi podatki[23] bilo relativno urejeno v posameznih organih,

[23] Do sprejetja ZTP se je uporabljalo več terminov. V obrambi vojaška skrivnost, v davčnem postopku davčna tajnost, v državni upravi pa se je uporabljal termin uradna tajnost (skrivnost), ki je imela tri stopnje, INTERNO, ZAUPNO in STROGO ZAUPNO, poleg teh pa je bila v uporabi še državna tajnost (skrivnost), kot najvišja tajnost. Tako ZTP v prehodnih določbah 48. člena določa, da je tajnim podatkom, ki jim je bila oznaka stopnje tajnosti določena ped uveljavitvijo tega zakona, treba določiti stopnjo tajnosti skladno s tem zakonom najkasneje dve leti po uveljavitvi tega zakona, sicer jim bo tajnost prenehala:

- podatki z oznako državna tajnost ali državna skrivnost kot STROGO TAJNO
- podatki uradna tajnost, uradna skrivnost ali vojaška skrivnost, strogo zaupno kot TAJNO
- podatki uradna tajnost, uradna skrivnost ali vojaška skrivnost, zaupno kot ZAUPNO in
- podatki uradna tajnost, uradna skrivnost ali vojaška skrivnost, interno kot INTERNO.

vendar brez vnaprej znanih kriterijev glede dostopa, določanja, varovanja in prenehanja tajnih podatkov.« (Žirovnik 2005, 7) ZTP je bil dopolnjen in spremenjen oktobra 2003 in marca 2006. Marca 2003 je posledica pritožbe na ustavno sodišče bil Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (ZTP-A). Ustavno sodišče je 08.05.2003 sprejelo sklep (objavljen 23.05.2003 v Ur. l. RS št. 43/03) o začasnem zadržanju izvajanja 25. člena ZTP, ki predpisuje vsebino in obseg varnostnega preverjanja. Z začetkom veljavnosti 22.10.2003 pa je uvedel bistvene spremembe na področju varnostnega preverjanja, in sicer: uvedene so bile tri vrste preverjanja-osnovno, dodatno in varnostno s poizvedovanjem, ki se ga izvede glede na stopnjo zaupnosti podatkov, do katerih bo imela oseba dostop.

Dne 04.04.2006 je vlada sprejela nov Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (ZTP-B), ki je prinesel kar nekaj novosti na področju varovanja tajnih podatkov. Dosedanja praksa izvajanja ZTP na nacionalni ravni je pokazala, da so bile potrebne določene rešitve, ki so dopolnile, oziroma nadgradile nacionalni sistem obravnavanja in varovanja tajnih podatkov. Predlagane spremembe in dopolnitve ZTP so bile usmerjene predvsem v večjo učinkovitost sistema in posledično večjo varnost nacionalnih in tujih tajnih podatkov. V spremembah ZTP je sedaj podrobno opredeljena vloga informacijskega pooblaščenca in postopek, v katerem se ugotavlja javno interes glede razkritja podatkov.

Razloge za spremembe in dopolnitve ZTP so razvrstili v naslednje skupine:

- spremembe, ki jih je pokazala praksa;
- postopkovne določbe, ki so urejale varnostno preverjanje oseb in jih je bilo potrebno prilagoditi posebnostim obravnavanja tajnih podatkov;
- natančneje je bilo potrebno razmejiti pristojnosti organov, pristojnih za izdajo dovoljenja za dostop do tajnih podatkov;
- opredelitev pristojnega organa in postopek izdaje dovoljenja fizični osebi ter varnostnega dovoljenja organizaciji za dostop do tujih tajnih podatkov;
- vzpostavitev inšpekcijskega nadzora nad izvajanjem predpisov s področja tajnih podatkov;
- uskladitev ZTP z določbami Zakona o prekrških;
- dopolnitve ureditve posredovanja tajnih podatkov izvajalcem naročil (organizacijam), t.i. industrijska varnost;

- dopolnitve določb o določanju tajnih podatkov, spremembi in preklicu tajnosti ter njihovem posredovanju tretjim osebam;
- druge spremembe, ki so bile potrebne za učinkovitejše izvajanje zakona.

Spremembe in dopolnitve ZTP ne odstopajo od ciljev in načel, na katerih sloni že sedanja ureditev tega področja. Poglavitni cilj spremembe zakona je bil izboljšati učinkovitost sistema in posledično varnost tajnih podatkov in osebno varnost oseb, ki morajo zaradi opravljanja funkcije delovnih nalog imeti dostop do tajnih podatkov.

4.1.3.1 Primerjava klasifikacij EU, NATO in RS

V varnostnih določilih EU je tajni podatek definiran kot »podatek ali sredstvo, katerega nepooblaščeno razkritje bi povzročilo različne stopnje škode interesom EU ali eni izmed njenih članic, ne glede na to, ali je podatek nastal v EU, bil posredovan od držav članice EU, drugih držav ali mednarodni organizacij«[24]. Skupščina EU je leta 2001 sprejela Varnostne predpise Skupščine EU[25], v katerih je opredelila klasifikacijo podatkov, ki so v rabi med članicami EU. Leta 2005 je EK sprejela odločitev, da se tovrstna klasifikacija zaupnih podatkov uporablja v vseh članicah (tudi v RS). Tako so države članice do 01.02.2005 morale prilagoditi svoje stopnje tajnosti stopnjam, ki so v veljavi v EU, kar kaže spodnja preglednica na naslednji strani:

TABELA 4.1: Klasifikacija po »*European Union Classification Standard*«

STOPNJA TAJNOSTI	OBRAZLOŽITEV:
EU TOP SECRET	za informacije, katerih neupravičeno odkritje bi povzročilo izjemno hudo škodo bistvenim interesom EU ali kateri izmed njenih članic;
SECRET UE	za informacije, katerih neupravičeno odkritje bi lahko huje škodovalo bistvenim interesom EU ali kateri izmed njenih članic;
CONFIDENTIEL	za informacije, katerih neupravičeno odkritje bi lahko škodovalo bistvenim interesom EU ali kateri izmed njenih članic;
RESTREINT	za informacije, katerih neupravičeno odkritje bi lahko pomenilo neugodnosti interesom EU ali kateri izmed njenih članic;

Vir: Dvoršak in Radulj (2005, 9).

[24] *2. točka 1. dela Security regulations of Council of the EU, Official Journal of the European Communities L 101, 2001*
[25] *Security regulations of the Council of the European Union*

NATO je v letu 2002 sprejel ključne dokumente s področja varovanja tajnih podatkov. Nekatere rešitve so bile nadgrajene v skladu z novimi varnostnimi izzivi, nekatere pa so bile narejene na novo. Vse skupaj pa predstavlja varnostno politiko zveze NATO. V dokumentu C-M (2002) 49[26] je tajni podatek (*NATO classified information*) definiran kot:

a. Podatek je védenje, ki je lahko posredovano v kakršnikoli obliki;
b. Tajni podatek pomeni podatke ali določena sredstva, ki potrebujejo zaščito pred nepooblaščenim razkritjem in so bili kot takšni označeni pri varnostni klasifikaciji;
c. Beseda »sredstvo« vključuje dokumente in tudi vsak del tehnike, opreme ali orožja, ki je bilo izdelano ali v izdelavi;
d. Beseda »dokument« pomeni vsak zabeležen podatek, ne glede na njegovo fizično obliko ali karakteristiko, vključujoč, pisane ali tiskane zadeve, kartice in trakove za obdelavo podatkov, karet, tabele, fotografije, slike, risbe, gravure, skice, delovne beležke, indigo kopije in črnilne trakove…

Članice NATO, pa uporabljajo za označevanje tajnosti podatkov naslednje oznake:

TABELA 4.2: Klasifikacija po »*NATO Classification Standard*«

STOPNJA TAJNOSTI	OBRAZLOŽITEV:
COSMIC TOP SECRET (CTS)	za informacije, katerih neupravičeno odkritje bi povzročilo izjemno hudo škodo za NATO (oznaka *COSMIC* je dodana stopnji *TOP SECRET* zaradi dokazovanja, da gre za označbo v lasti NATO;
NATO SECRET (NS)	za informacije, katerih neupravičeno odkritje bi povzročilo resno škodo za NATO;
NATO CONFIDENTIAL (NC)	za informacije, katerih neupravičeno odkritje bi škodovalo interesom NATO;
NATO RESTRICTED (NR)	za informacije, katerih neupravičeno odkritje bi pomenil neugodnost interesom NATO;
ATOMAL	gre za oznako za podatke, ki jih določa "*Atomic Energy Act*" (Zakon o atomski energiji) iz leta 1954 in je enaka oznakam Združenih držav Amerike "*U.S. Restricted Data*" in Velike Britanije "*United Kingdom ATOMIC*". Uporablja se v kombinaciji z drugimi stopnjami tajnosti: *COSMIC TOP SECRET ATOMAL* (CTSA), *NATO SECRET ATOMAL* (NSA), *NATO CONFIDENTIAL ATOMAL* (NCA).
NATO UNCLASSIFIED (NU)	za uradne informacije v lasti NATO, ki ne zadostujejo kriteriju klasifikacije. Dostop do informacij s strani nečlanic je dovoljen pod pogojem, da ne bo odločilen za NATO.

Vir: Dvoršak in Radulj (2005, 9).

[26] V aneksu 1, priloge »A«

S sprejetjem ZTP se je v Sloveniji poenotila terminologija, ki se uporablja pri ravnanju s tajnimi podatki, ter določila enovit sistem označevanja stopenj. Tajni podatek je definiran 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.« (2. člen ZTP)

ZTP v svojem 13. členu določa tudi kategorije oz. stopnje tajnosti in jih razvršča v štiri nivoje: INTERNO, kot najnižji, ZAUPNO, TAJNO IN STROGO TAJNO, kot najvišji nivo zaščite. V naslednji tabeli bom prikazala navedene oznake in njim ustrezne razlage, ki lahko nastanejo v primeru razkritja tajnih podatkov. Predvsem so to škodljive posledice za varnost države ali za njene politične in gospodarske koristi.

TABELA 4.3: Klasifikacija po ZTP

STOPNJA TAJNOSTI	OBRAZLOŽITEV:
STROGO TAJNO	za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese RS ali jim nepopravljivo škodovalo;
TAJNO	za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom RS;
ZAUPNO	za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom RS;
INTERNO	za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa;

Vir: Dvoršak in Radulj (2005, 8).

V RS je od leta 2001 v veljavi ustrezna zakonodaja s področja varovanja tajnih podatkov. Stopnje tajnosti so si po primerjavi subjektov enake. (glej Tabelo 4.1, Tabelo 4.2 in Tabelo 4.3). Tako je mogoče govoriti o poenotenju klasifikacije zaradi lažjega in hitrejšega izmenjevanja podatkov med članicami (ali NATO ali EU ali znotraj obeh). Poenotenje pomeni, da bo imel podatek, ki v državi Sloveniji nosi oznako »Zaupno« tudi v NATO enako stopnjo tajnosti, vendar z oznako NATO Confidential. Enako stopnjo bo užival tudi v EU ali v katerikoli njeni članici. Podatek bo glede varovanja in zaščite obravnavan ravno tako, kakor bi ga obravnavali v lastni državi. Poenotenje je vsekakor dobrodošlo za vse članice tako zavezništva NATO, kakor EU, ker so s tem postavljeni temeljni standarda, kateremu pravimo varnostni standard EU, varnostni standard NATO in varnostni standard RS.

4.2 NORMATIVNA UREDITEV OBRAVNAVANJA TAJNIH PODATKOV RS PO PODROČJIH

Temeljni predpis, ki v RS ureja določanje in ravnanje s tajnimi podatki je ZTP. Trbovšek (2004, 61) pravi, da je pred sprejetjem zakona predlagatelj poudaril, da so vprašanja, povezana z ureditvijo dostopa do tajnih podatkov in določanja varovanja z delovnega področja državnih organov RS, pomembna z več vidikov, in sicer: ustavno-pravnih, mednarodnih, upravno-organizacijskih, političnih, kadrovskih in strokovno-tehničnih. Pravna ureditev teh vprašanj mora v demokratični državi upoštevati vsa tista temeljna načela, na katerih takšne države temeljijo ter vse temeljne pravice in svoboščine državljanov.

Varstvo tajnosti je seveda potrebno legitimirati v vsaki demokratični državi. RS je vprašanja, povezana z določanjem in dostopom do podatkov in informacij, ki jih je zaradi interesov in koristi države potrebno opredeliti kot tajne, rešila v ZTP. Na njegovi podlagi je Vlada RS sprejela štiri uredbe, s katerimi podrobneje ureja način varnostnega preverjanja oseb in izdajo dovoljenj za dostop do tajnih podatkov, varovanje in označevanje, ugotavljanje pogojev za posredovanje tajnih podatkov izvajalcem določenih naročil in notranji nadzor nad izvajalcem ZTP. Vendar pa so vsi ti sprejeti pravni akti s področja varovanja tajnih podatkov do danes doživeli nekaj dopolnitev in sprememb (Perenič 2005, 97). V tem poglavju bom s predpisi za podrobnejše določanje ravnanja s tajnimi podatki opredelila sprejem, evidentiranje, dodeljevanje, posredovanje, razmnoževanje, uničenje in hranjenje.

4.2.1 Sprejem tajnih podatkov

Sedmi odstavek 21. člena Uredbe o varovanju tajnih podatkov (Ur. l. RS, št. 74/05) določa, da mora »vsak organ določiti, kje se sprejemajo nosilci tajnih podatkov in kdo jih sprejema. Naslovnik ali oseba, ki je pooblaščena za sprejem nosilcev tajnih podatkov, potrdi njihov prejem z vpisom v dostavno oziroma kurirsko knjigo.«

Uredba o upravnem poslovanju (Ur. l. RS, št. 20/05) v drugem odstavku 93. člena govori o tem, da »javni uslužbenci v glavni pisarni upravljajo z dokumentarnim gradivom, kar obsega naloge sprejemnega prostora oziroma vložišča, evidentiranja zadev, dosjejev in dokumentov,

odpravništva, ter skrb za varovanje dokumentarnega gradiva. Vodijo in skrbijo za pravilno in enotno vodenje evidenc o zadevah, dosjejih in dokumentih ter v sodelovanju s predstojnikom, z vodji notranjih organizacijskih enot in drugimi pooblaščenimi javnimi uslužbenci usklajujejo in nadzirajo ravnanje z dokumentarnim gradivom v notranjih organizacijskih enotah ter pri javnih uslužbencih organa.« Tretji odstavek nadaljuje, in sicer, da »javni uslužbenci v glavni pisarni smejo po pooblastilu odpirati pošto v fizični obliki, ki je prejeta v zaprtih ovojnicah in pošto v elektronski obliki, prejeto na uradni elektronski naslov organa.« Pri poslovanju s tajnimi podatki lahko funkcijo glavne pisarne opravljajo registri[27] in podregistri[28] ali kontrolne točke.

97. člen Uredbe (ibid.), se v odstavkih od 1 do 8 ukvarja s sprejemom pošte in vlog ter določa več odstavkov za ravnanje s tajnimi podatki. »Pošto v fizični obliki sprejme javni uslužbenec, ki je pooblaščen za sprejem pošte. Javni uslužbenec, ki prevzema pošto v imenu organa pri poštnem podjetju, mora imeti pooblastilo. Za prevzem pošte pri poštnem podjetju morata biti pooblaščena najmanj dva javna uslužbenca. Pošto, naslovljeno na organ ali na javnega uslužbenca tega organa, sprejme, pregleda in evidentira glavna pisarna v skupno evidenco dokumentarnega gradiva. Vse zaznamke, ki jih javni uslužbenci v glavni pisarni ob sprejemu pošte zapišejo na dokument ali poseben list papirja, je treba opremiti z datumom, imenom in podpisom. Če zaznamek vnese neposredno v informacijski sistem, se v sistemu zabeležita ime javnega uslužbenca, ki je zaznamek vnesel in datum vnosa. Pošto, poslano po poštni, kurirski ali dostavni službi, prevzema javni uslužbenec, iz prvega odstavka tega člena, v glavni pisarni. Ta javni uslužbenec ne sme prevzeti priporočene pošte in pošte, na kateri je označena vrednost (paketi, vrednostna pisma), če ugotovi, da je pošta poškodovana, ali če obstaja sum, da je bila odprta, ali je v njej nevarna vsebina. V tem primeru mora od poštnega podjetja zahtevati, da se stanje in vsebina pošte komisijsko ugotovita. Potem je pošto mogoče prevzeti skupaj z izvodom zapisnika o komisijski ugotovitvi. Elektronska sporočila organ prejema preko elektronske pošte, telefaksa, elektronske izmenjave podatkov, spletnih obrazcev ali preko centralnega informacijskega sistema za sprejem vlog, vročanje in obveščanje. Sporočila

[27] Glavne naloge centralnega registra so sprejemati, evidentirati, distribuirati in arhivirati dokumente zveze NATO za RS s tajnimi in uradnimi podatki brez stopnje tajnosti. CR NATO sprejema vse TP, ki so namenjeni v RS ter jih kasneje posreduje v svoje podregistre. Centralni register tudi usmerja delovanje vseh podregistrov in nadzornih točk zveze NATO v RS.

[28] Za uporabnike, ki izpolnjujejo vsa varnostna merila za seznanitev s TP NATO, so v RS vzpostavljeni podregisti ali kontrolne točke. Podregistre je mogoče primerjati z glavnimi pisarnami v naših ministrstvih in drugih upravnih organizacijah. V RS so vzpostavljeni podregistri in kontrolne točke; trenutno jih je sedem: podregister Nacionalnega centra za krizno upravljanje, podregister MORS, podregister OVS MORS, podregister GŠSV, podregister SOVA, podregister MZZ.

v elektronski obliki, ki so bila neposredno naslovljena na javne uslužbence, posredujejo ti javni uslužbenci glavni pisarni ali jih sami evidentirajo, če imajo za to pooblastilo. Javni uslužbenci ne smejo sami odpirati novih zadev, razen s pooblastilom predstojnika. Če vsebine dokumenta trenutno ni mogoče shraniti v evidenco oziroma vsebina dokumentov ni vidna v elektronski obliki, je potrebno elektronsko prejeti dokument natisniti. S tako natisnjenim dokumentom se ravna v skladu z določili za fizični dokument. Pošta, prejeta v elektronski obliki, se lahko natisne na papir, če je bila elektronska oblika uporabljena izključno za prenos (sporočila, prejeta po telefaksu, skenirani dokumenti in podobno).«

Prvi in tretji odstavek 99. člena Uredbe (Ur. l. RS , št. 20/05) opredeljujeta čas sprejema pošte. «Pošta v fizični obliki se sprejema ves poslovni čas organa. Pošta v elektronski obliki se sprejema tudi izven poslovnega časa. Če ima organ organizirano dežurno službo, se lahko pošto oddaja dežurni službi ne glede na čas. Dežurni javni uslužbenec ne odpira prevzete pošte, razen če ima za odpiranje nujne pošte in za predajanje sporočil drugim javnim uslužbencem upravnega organa posebno pooblastilo. Na prejeto pošto dežurni javni uslužbenec zapiše datum in čas (uro in minuto), ko jo je prejel.«

Člen 100. Uredbe (ibid.) v tretjem odstavku določa odpiranje pošte, označene s stopnjo tajnosti, ki jo »odpira predstojnik organa oziroma drug, za dostop do tajnih podatkov pooblaščeni, javni uslužbenec.« V nasprotju s členom 100, pa 101. člen Uredbe (Ur. l. RS , št. 20/05) v odstavkih 1, 2 in 4 opredeljuje prepoved odpiranja pošte: »Javni uslužbenec, ki je določen za odpiranje pošte, ne sme odpreti pošiljke, ki je naslovljena na javnega uslužbenca in je na ovojnici navedeno, da se vroči osebno naslovniku. Če se izkaže, da takšna pošiljka vsebuje vlogo in priloge ali druge dokumente, pomembne za delo organa, jo mora naslovnik nemudoma dostaviti javnemu uslužbencu, ki je določen za odpiranje pošte, z ustrezno pisarniško odredbo. Javni uslužbenec, določen za sprejem pošte, ne odpira pošte, ki je naslovljena na drug organ, pravno ali fizično osebo in je pomotoma dostavljena. Elektronskega dokumenta ni dovoljeno presneti na drug nosilec, oziroma prenesti v drug informacijski sistem, preden se ugotovi, da se s tem ne povzroči nevarnosti za informacijski sistem organa (zaščita pred zlonamerno programsko opremo).«

118. člen Uredbe v odstavkih 1, 9 in 12 (ibid.) pa opredeljuje prejemno štampiljko in njeno uporabo ter pravi: »Na vsak fizični dokument, ki ga glavna pisarna prejme od poštnega podjetja, dostavne ali kurirske službe, ali ga prinesejo stranke in druge osebe, uslužbenec

glavne pisarne odtisne prejemno štampiljko, praviloma na zgornji desni del prve strani fizičnega dokumenta, tako da ne prekrije besedila dokumenta. Pooblaščeni javni uslužbenec najprej preveri v evidenci, ali prejeti dokument nadaljuje obstoječo zadevo. V tem primeru v prejemno štampiljko prejetega dokumenta prepiše šifro zadeve in signirni znak delovnega mesta. Namesto prejemne štampiljke se smejo uporabiti zapisi z drugimi tehničnimi sredstvi.« Zadnji odstavek, pomemben za poglavje sprejema tajnih podatkov, pa se nanaša na vročanje tajnih podatkov: »Z dostavno knjigo oziroma kurirsko knjigo se vroča nosilce tajnih podatkov, vrednostna pisma, vrednotnice ali pakete«(Ur. l. RS , št. 20/05, člen 170).

4.2.2 Evidentiranje tajnih podatkov

ZTP (Ur. l. RS, št. 50/06-UPB2) v 2. členu prvega poglavja določa, da je »obravnavanje tajnih podatkov določanje, označevanje, dostop do, uporaba, evidentiranje, razmnoževanje, posredovanje, prenos, uničevanje nosilcev tajnih podatkov, hramba, arhiviranje ter drugi ukrepi in postopki, s katerimi se zagotavlja njihova varnost.«
38. člen Zakona (ibid.) nadalje govori, da se »v vsakem organu in organizaciji mora v skladu s tem zakonom in predpisi, sprejetimi na njegovi podlagi, vzpostaviti sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza določeni stopnji tajnosti in onemogoča njihovo razkritje nepoklicanim osebam. Postopki in ukrepi iz prejšnjega odstavka morajo obsegati: splošne varnostne ukrepe, varovanje oseb, ki imajo dostop do tajnih podatkov, varovanje prostorov, varovanje dokumentov in medijev, ki vsebujejo tajne podatke, varovanje komunikacij, po katerih se prenašajo tajni podatki, način označevanja stopenj tajnosti, varovanje opreme, s katero se obravnavajo tajni podatki, način seznanitve uporabnikov z ukrepi in postopki varovanja tajnih podatkov, kontrolo in evidentiranje dostopov do tajnih podatkov, kontrolo in evidentiranje pošiljanja in distribucije tajnih podatkov.«

Uredba (Ur. l., št. 74/05) v 28. členu za evidentiranje tajnih podatkov v RS določa naslednje določbe:

- uredbe o varovanju tajnih podatkov,
- predpise, ki urejajo poslovanje organov javne uprave z dokumentarnim gradivom,
- druge predpise, ki urejajo poslovanje z dokumentarnim gradivom.

Pri evidentiranju je treba zagotoviti, da se iz posameznih vpisov, ki jih vsebuje evidenca, ne da razbrati vsebine tajnega podatka. Kadar se za evidentiranje ali hrambo dokumentov, ki vsebujejo tajne podatke, uporablja informacijska tehnologija, je pogoj ločene hrambe tovrstnega dokumentarnega gradiva izpolnjen, če se uporablja rešitev, ki je fizično ločena od drugih informacijskih rešitev, ali rešitev, ki temelji na tehnologiji navideznega zasebnega omrežja in uporablja kriptozaščitne postopke in ukrepe, ustrezne stopnji tajnosti obdelovanih tajnih podatkov ter izpolnjuje druge pogoje, določene v predpisu iz 39. člena[29] te Uredbe. Pri uporabi tehnologije navideznega zasebnega omrežja mora biti dostop do tega dela informacijskega sistema dovoljen samo osebam, ki:

- imajo dovoljenje ustrezne stopnje tajnosti,
- dokumente potrebujejo zaradi opravljanja delovnih nalog in
- so se uspešno identificirale z digitalnim potrdilom ter dokazale njegovo izvirnost.

Uredba (Ur. l. RS, št. 20/05) v 124. členu določa, da je »evidenca dokumentarnega gradiva temeljna evidenca o opravljanju del in nalog organa in je podlaga vsem drugim evidencam, ki se nanašajo na delo organa. Da se evidenca dokumentarnega gradiva vodi o vseh zadevah, dosjejih in dokumentih, ki jih organ prejme ali nastanejo pri njegovem delu.«

127. člen Uredbe (ibid.) še natančneje določa evidentiranje dokumentarnega gradiva v elektronski obliki, ki mora zagotavljati evidentiranje ravnanja z dokumenti, in sicer tako, da »se shranjujejo podatki o tem, kdo in kdaj je izvajal posamezna opravila v zvezi s posameznim dokumentom. Pri skeniranih dokumentih se shranjujejo tudi podatki o tem, kdo in kdaj je dokument skeniral. Javni uslužbenec, pooblaščen za skeniranje dokumentov, mora zagotoviti, da se dokument skenira v celoti, skupaj s pripadajočimi prilogami. Priloge se skenirajo v celoti, če je to izvedljivo glede na njihov obseg. Paziti mora tudi na čitljivost in identičnost skenirane slike dokumenta in pripadajočih prilog z originalom v fizični obliki. Notranja kontrola pravilnosti skeniranja dokumentov mora zagotavljati redno in izredno preverjanje skeniranih dokumentov. Redno preverjanje se izvaja najmanj enkrat na tri mesece, izredno pa najmanj dvakrat letno. Notranja kontrola iz prejšnjega odstavka obsega preverjanje

[29] 39. člen Uredbe določa varovanje tajnih podatkov v komunikacijsko-informacijskih sistemih. Fizične, organizacijske in tehnične ukrepe ter postopke varovanja tajnih podatkov, ki se obdelujejo, prenašajo ali hranijo v komunikacijskih, informacijskih in drugih elektronskih sistemih, ureja poseben predpis ob upoštevanju določb 17. člena te uredbe, da varnostnotehnična oprema varnostnih območij mora ustrezati pogojem, ki jih na predlog nacionalnega varnostnega organa določi Vlada Republike Slovenije in četrtega odstavka 39. člena ZTP.

pravilnosti skeniranja za tekoče dokumente in dokumente, skenirane v preteklih letih. Predstojnik organa določi obseg letnega pregledanega vzorca, ki mora biti primeren glede na obseg celotne zbirke dokumentarnega gradiva. Predstojnik organa za izvajanje notranje kontrole pravilnosti skeniranja dokumentov pooblasti posameznega javnega uslužbenca ali pa skupino javnih uslužbencev.«

V 128. členu Uredbe (Ur. l. RS, št. 20/05) je določen način evidentiranja pošte, ki se vedno evidentira, če je bil potrjen prejem tega dokumenta oziroma pošte ali če je dokument oziroma pošta naslovljena na drug organ. Dokument oziroma pošta se nato na primeren način pošlje pravemu naslovniku. O tem dejanju se sestavi zaznamek. Dokument, ki ga organ prejme v fizični obliki, evidentirajo javni uslužbenci v glavni pisarni pod nadzorom in ob strokovni pomoči predstojnika oziroma vodje notranje organizacijske enote ali drugega za to pooblaščenega javnega uslužbenca. Prejeti dokument v elektronski obliki evidentira s podatki v skladu s 148. členom Uredbe (ibid.) glavna pisarna. Javni uslužbenci, ki imajo za to pooblastilo predstojnika oziroma vodje organizacijske enote, evidentirajo dokumente, ki jih prejmejo na svoj elektronski naslov. Če ima organ ustrezno informacijsko opremo, se gradivo, prejeto v papirnati obliki tudi ustrezno skenira v elektronsko evidenco zadev, dosjejev in dokumentov. Predstojnik organa določi, katere vrste gradiva se zaradi preobsežnosti ali iz razlogov učinkovitega poslovanja organa ne skenira.

V primeru tajnih podatkov lahko funkcijo glavne pisarne opravlja register, podregister ali kontrolna točka. Predstojnik organa določi, da se dokumentarno gradivo, ki vsebuje tajne podatke, ne skenira, oziroma se.

4.2.3 Dodeljevanje oz. signiranje tajnih podatkov

»Pravico dostopa do tajnih podatkov imajo 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.» (Ur. l. RS, št. 50/06, 31. člen)

V 4. členu Uredbe (Ur. l. RS, št. 20/05) je določeno, da »predstojnik lahko pisno pooblasti enega ali več javnih uslužbencev organa za izvrševanje posameznih pravic in dolžnosti po tej uredbi (Pooblastilo za dodeljevanje zadev in dokumentov). V kolikor je organizacija dela razvidna že iz sistemizacije delovnih mest ali pa je področje urejeno v drugih internih aktih organa, posebna pooblastila niso potrebna.«

V skladu z dodeljevanjem zadev in dokumentov, ki je opredeljeno v 121. členu (ibid), mora »delo v organu biti organizirano tako, da se vsaka zadeva nemudoma dodeli v reševanje (signira) pristojni notranji organizacijski enoti ali pooblaščenemu javnemu uslužbencu. Postopek dodeljevanja in pooblastila v zvezi z dodeljevanjem odredi predstojnik oziroma vodja notranje organizacijske enote. Zadeve, ki jih organ rešuje po ustaljenem postopku, glavna pisarna v skladu z notranjimi pravili organa o načinu dodeljevanja in o pooblastilih v zvezi z dodeljevanjem pošlje v reševanje neposredno notranji organizacijski enoti ali javnemu uslužbencu, odgovornemu za reševanje zadeve. Če se zadeva pošlje v reševanje neposredno javnemu uslužbencu, odgovornemu za reševanje zadeve, se zadeva označi s signirnim znakom, ki poleg označbe organizacijske enote vsebuje tudi znak delovnega mesta (popolno dodeljevanje). Zadeve iz prejšnje točke se lahko dodelijo tudi projektni skupini, komisiji ali drugemu delovnemu telesu, ki vodi projekt ali rešuje posamezno zadevo. Glede tega dodeljevanja se smiselno uporabljajo določbe te uredbe o dopolnilnem dodeljevanju dokumentov, ki se dodelijo organizacijski enoti. Zadeve, ki se kasneje dodelijo v reševanje drugi organizacijski enoti ali drugemu javnemu uslužbencu, se presignirajo. Zadeve, ki obravnavajo načelna in vodstvena vprašanja, glavna pisarna po zahtevnosti zadeve predložijo predstojniku organa ali vodji notranje organizacijske enote. Take zadeve se označijo samo s signirnim znakom vodstva organa oziroma vodstva notranje organizacijske enote (nepopolno dodeljevanje).«

4.2.4 Posredovanje (distribucija) tajnih podatkov

ZTP v 34. členu Zakona (Ur. l. RS, št. 50/06-UPB2) govori, da se »tajni podatki lahko drugim organom, ki morajo ravnati po tem zakonu, oziroma osebam v teh organih, posredujejo samo na podlagi pisnega dovoljenja predstojnika organa, ki je tajni podatek določil, ali če tako določa zakon.« 36. člen (ibid.) prepoveduje, da »upravičeni uporabnik, ki je od organa dobil

tajne podatke, brez soglasja tega organa posreduje te podatke drugim uporabnikom, razen v primerih, določenih s predpisi.«

Pooblaščena oseba organa in organizacije po 37. členu Zakona (Ur. l. RS, št. 50/06-UPB2) »mora vzpostaviti ažuren pregled in nadzor nad distribucijo tajnih podatkov zunaj organa. Iz pregleda mora biti razvidno, kdaj in komu so bili tajni podatki posredovani.«
»V vsakem organu se mora v skladu s tem zakonom in predpisi, sprejetimi na njegovi podlagi, vzpostaviti sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza določeni stopnji tajnosti in onemogoča njihovo razkritje nepoklicanim osebam.
Postopki in ukrepi iz prejšnjega odstavka morajo obsegati:

- kontrolo in evidentiranje dostopov do tajnih podatkov,
- kontrolo in evidentiranje pošiljanja in distribucije tajnih podatkov. « (ibid., 38. člen)

Elektronsko pošto ter posredovanje podatkov in evidentiranje določa 73. člen Uredbe (Ur. l. RS, št. 20/05), ki govori, da »varovanih podatkov javni uslužbenci ne smejo posredovati naprej po elektronski pošti brez predhodnega dovoljenja predstojnika organa. Tajni podatek se lahko pošilja po elektronski pošti samo v kriptirani obliki in v skladu s predpisi, ki urejajo obdelavo, prenašanje in hrambo tajnih podatkih v komunikacijskih, informacijskih in drugih elektronskih sistemih.«

Zahteve za evidentiranje danes dajejo prednost »informacijskim rešitvam, ki obsegajo informacijsko in komunikacijsko opremo ter morajo omogočiti vodenje evidenc v skladu z zahtevami te uredbe. Informacijska rešitev mora zagotavljati informacijsko varnost in sledljivost zadev in dokumentov (varovan dostop do podatkov, varnostne kopije itd.).« (ibid.,člen 75)

Nadalje 169. člen Uredbe določa »pošiljanje in izročanje dokumentov s tajnimi podatki, ki jih v skladu s predpisi določi strokovni javni uslužbenec, ki je dokumente pripravil za odpravo. Ta tudi določi, kako je treba zavarovati in opremiti pisemsko ovojnico, v kateri se pošiljajo takšni dokumenti.« (Ur. l. RS, št. 20/05)

Pošiljanje tajnih podatkov je določeno z Zakonom (Ur. l. RS, št. 50/06) v 39. členu, kjer je potrebno »tajne podatke v organih hraniti na način, ki zagotavlja, da imajo dostop do teh

podatkov samo osebe, ki imajo dovoljenje za dostop do tajnih podatkov, in ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij. Tajni podatki se lahko pošljejo izven prostorov organa samo ob upoštevanju predpisanih varnostnih ukrepov in postopkov, ki morajo zagotoviti, da jih prejme oseba, ki ima dovoljenje za dostop do tajnih podatkov in je do teh podatkov upravičena. Postopki in ukrepi varovanja pošiljanja tajnih podatkov izven prostorov organa se predpišejo glede na stopnjo tajnosti teh podatkov. Organi tajnih podatkov ne smejo prenašati ali posredovati po nezaščitenih komunikacijskih sredstvih.«

»Tajni podatki se prenašajo v zaprti, neprosojni ovojnici. Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo po lastni prenosni mreži ali priporočeni pošti s povratnico, tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti pa po lastni prenosni mreži ali s kurirsko službo. Tajni podatki stopnje tajnosti ZAUPNO in višje stopnje se prenašajo v dveh ovojnicah. Zunanja ovojnica je iz trdnega, neprosojnega in neprepustnega materiala. Na njej morajo biti podatki o naslovniku, pošiljatelju in šifra dokumenta. Iz oznak na zunanji ovojnici ne sme biti razvidno, da vsebuje tajni podatek. Notranja ovojnica mora imeti oznako stopnje tajnosti, šifro dokumenta, podatke o naslovniku in pošiljatelju ter druge podatke, pomembne za varnost. Pri prenosu tajnih podatkov stopnje tajnosti ZAUPNO in TAJNO zunaj varnostnega območja lahko zunanjo ovojnico nadomesti zaklenjen ali zapečaten kovček, škatla ali torba. Pri prenosu tajnih podatkov stopnje tajnosti STROGO TAJNO zunaj varnostnega območja mora biti notranja ovojnica v zaprtem kovčku, škatli ali torbi z zapiranjem na ključ ali šifrirno kombinacijo. Prenos opravita najmanj dve osebi. Kadar se tajni podatki iz četrtega in petega odstavka tega člena prenašajo znotraj varnostnega ali upravnega območja, morajo biti zakriti tako, da se prepreči opazovanje njihove vsebine. Kurirji in druge osebe, ki prenašajo tajne podatke (v nadaljnjem besedilu: kurirji), morajo biti varnostno preverjeni glede na stopnjo tajnosti tajnih podatkov, ki jih prenašajo.«(Ur. l. RS, št. 74/05, 21. člen)

»Organi morajo za prenose tajnih podatkov stopnje tajnosti TAJNO ali višje stopnje zunaj varnostnih območij izdelati načrt poti in varovanja prenosa. Načrti varovanja prenosov tajnih podatkov stopnje tajnosti TAJNO ali višje stopnje mora vsebovati tudi postopke in ukrepe ob morebitnem poskusu odtujitve, poškodbe ali uničenja, prometnih in drugih nesrečah, zastojih, postankih, prenočevanju in drugih podobnih dogodkih. V načrtu morajo biti opredeljene glavne in pomožne poti. Kurirji, ki prenašajo tajne podatke stopnje tajnosti TAJNO ali višje stopnje, morajo biti ustrezno usposobljeni ter seznanjeni s postopki in ukrepi pri varovanju

prenosa tajnih podatkov. Kurirji, ki prenašajo tajne podatke, se usposabljajo najmanj enkrat letno. Njihovo usposabljanje usklajuje nacionalni varnostni organ, izvajata pa ga MORS) in Policija, razen usposabljanja uradnih oseb SOVE, ki prenašajo pošto, povezano z delom agencije, za katerih usposabljanje skrbi ta agencija.« (ibid., 22. člen)
»Kurirji, ki prenašajo tajne podatke stopnje ZAUPNO ali višje stopnje, morajo imeti pisno pooblastilo predstojnika organa za prenos le-teh in ga morajo pokazati na zahtevo osebe, ki pošto predaja ali prevzema. Vsebina in oblika pooblastila sta določeni z obrazcem OBR-KU, ki je v prilogi III te uredbe in je njen sestavni del.« (Ur. l. RS, 74/05, 23. člen)

Prenos tajnih podatkov po komunikacijskih in informacijskih sistemih zunaj varnostnih območij oziroma upravnega območja je dovoljen le v šifrirani obliki. V sistemih se lahko uporabljajo le šifrirne rešitve, ki jih potrdi komisija iz 15. člena te Uredbe, če v drugih zakonskih predpisih ni drugače določeno. Izjemoma se lahko v izrednih okoliščinah tajni podatki stopnje tajnosti INTERNO, ZAUPNO in TAJNO prenašajo v nešifrirani obliki. Za vsak tak prenos mora izdati dovoljenje predstojnik organa ali oseba, ki jo je pooblastil. Take izredne okoliščine so:

- preteče ali dejanske krize, spopad ali vojne razmere ali
- kadar je hitrost dostave bistvenega pomena in pri tem niso na voljo sredstva in metode za šifrirno zaščito ter se ocenjuje, da je možnost zlorabe poslanih tajnih podatkov zelo majhna.

Šifrirani tajni podatki se z uporabo pomnilnih medijev zunaj varnostnega oziroma upravnega območja prenašajo skladno s tem členom. Nešifrirani tajni podatki se z uporabo pomnilnih medijev zunaj varnostnih območij oziroma upravnega območja prenašajo skladno z Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS 48/07, 14. člen).

4.2.5 Razmnoževanje tajnih podatkov

Uredba (Ur. l. RS, št. 74/05) 25. členu določa prepoved razmnoževanja, kopiranja ali prepisovanja tajnih podatkov. »Tajnih podatkov stopnje tajnosti STROGO TAJNO se ne sme

razmnoževati, kopirati ali prepisovati. Dodatne izvode zapisa tega tajnega podatka sme izdelati le pooblaščena oseba organa, v katerem mu je bila določena stopnja tajnosti.«

26. člen (ibid.) določa »kopiranje tajnih podatkov stopnje tajnosti INTERNO, ZAUPNO ali TAJNO, ki se lahko kopira le na podlagi pisarniške odredbe predstojnika organa ali osebe, ki jo za to pooblasti predstojnik organa. Kopija se izdela v ustreznem varnostnem območju na podlagi pisarniške odredbe. Iz kopije tajnih podatkov mora biti razvidno, iz katerega zapisa ali dela zapisa izhaja kopija (šifra in datum dokumenta ter številka strani). Organ, ki je določil podatek za tajnega stopnje INTERNO, ZAUPNO ali TAJNO, mora na dokumentu vidno označiti morebitno prepoved kopiranja.«

27. člen ureja še področje prevajanja tajnih podatkov in govori, da »organ ali organizacija, ki zaradi opravljanja nalog dokument, ki vsebuje tajni podatek, prevede v drug jezik, mora na prevod napisati vse oznake tajnosti in evidenčne številke izvirnega dokumenta. Prevod dokumenta iz prejšnjega odstavka je priloga izvirnika.«(Ur. l. RS, št. 74/05)

4.2.6 Uničenje nosilcev tajnih podatkov

Uredba (Ur. l. RS, št. 74/05) v 30. členu določa uničenje tajnih podatkov. »Poleg ukrepov, določenih v predpisih, ki urejajo poslovanje organov javne uprave z dokumentarnim gradivom, je treba pri uničenju tajnih podatkov zagotoviti, da:

- predstojnik organa ali oseba, ki jo predstojnik organa za to pooblasti, imenuje najmanj tričlansko komisijo za uničenje tajnih podatkov, v katero mora biti vključena oseba, ki je v organu odgovorna za varovanje tajnih podatkov;
- vsak organ po opravljenem letnem pregledu prejetih tajnih podatkov izloči in po potrebi uniči vse tajne podatke, ki jih je dobil informativno;
- se v zapisnik o uničenju tajnih podatkov vpišejo šifra, datum in stopnja tajnosti uničenega podatka, ki je bil na nosilcu;
- se o uničenju tajnih podatkov stopnje tajnosti STROGO TAJNO pisno obvesti organ, ki je določil stopnjo tajnosti;

- se za druge tajne podatke, ki so del tekoče ali stalne zbirke dokumentarnega gradiva, uporabljajo predpisi, ki urejajo poslovanje organov javne uprave z dokumentarnim gradivom.

Seznam vpogledov iz prejšnjega člena se priloži zapisniku o uničenju tajnih podatkov. Uničiti se morajo na način, s katerim se zagotovi, da postane tajni podatek nerazpoznaven in neobnovljiv.«

87. člen Uredbe (Ur. l. RS, št. 20/05) določa uničevanje nosilcev podatkov na način, »da mora organ zagotoviti fizično uničevanje odpadnih nosilcev podatkov (papir, disketa, magnetni in optični diski itd.), ki vsebujejo tajne ali varovane vsebine na način, ki zanesljivo onemogoči branje oziroma dostop do dela ali vseh podatkov.« Enako določa tudi 88. člen, za »zagotovitev uničevanja pomožnega gradiva, ki je bilo uporabljeno ali je nastalo ob pripravi podatkov.«(ibid.)

Po 196. členu, ki določuje izločanje in odbiranje gradiva iz zbirk, se najmanj vsakih pet let izloči ali izbriše gradivo, ki mu je potekel rok hrambe. Pri tem se v informatizirani evidenci izbriše samo vsebina gradiva, ne pa tudi evidenčni podatki. Dokumentarno gradivo, za katero je pristojni arhiv določil, da ima lastnosti arhivskega gradiva, se odbere iz stalne zbirke dokumentarnega gradiva in hrani v izvirnikih, dokler se v skladu s posebnim predpisi ne izroči pristojnemu arhivu.(Ur. l. RS, št. 20/05)

Komisija za izločanje in odbiranje dokumentarnega gradiva je določena v 197. členu in jo imenuje predstojnik. Naloge komisije so:

- določi, katero gradivo se izloči iz zbirke dokumentarnega gradiva in o tem sestavi zapisnik;
- pisno obvesti pristojni arhiv o začetku odbiranja arhivskega iz dokumentarnega gradiva in navede, iz katerih letnikov dokumentarnega gradiva bo odbrala gradivo v skladu z navodilom pristojnega arhiva;
- skrbi, da se ne izloči dokumentarno gradivo, za katero je pristojni arhiv določil, da ima lastnosti arhivskega gradiva. Komisija najmanj vsakih 5 let odbere arhivsko in trajno gradivo organa. Komisija najmanj vsakih 5 let izloči ali izbriše iz stalne zbirke dokumentarno gradivo, ki mu je potekel rok hrambe in je bilo predhodno iz njega

odbrano arhivsko in trajno dokumentarno gradivo. Komisija opravlja svoje naloge skladno s pisnimi navodili ter dodatnimi navodili pristojnega arhiva. Komisija je praviloma sestavljena iz javnih uslužbencev iz glavne pisarne in strokovnih javnih uslužbencev, ki rešujejo zadeve iz vsebinskega področja, na katerega se nanaša dokumentarno gradivo.(ibid.)

V 198. členu komisija iz prejšnjega člena poskrbi, da se izločeno dokumentarno gradivo, ki vsebuje zaupne oz. tajne podatke, tako uniči, da ga ni več mogoče prebrati. O oddaji izločenega dokumentarnega gradiva v industrijsko predelavo oziroma o njegovem uničenju sestavi komisija zapisnik (Ur. l. RS, št. 20/05).

4.2.7 Hranjenje tajnih podatkov

39. člen Zakona (Ur. l. RS, št. 50/06) določa, da se morajo »tajni podatki v organih hraniti na način, ki zagotavlja, da imajo dostop do teh podatkov samo osebe, ki imajo dovoljenje za dostop do tajnih podatkov, in ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij.«

19. 20. in 31. člen Uredbe(Ur. l. RS, št. 74/05) opisujejo mesto hrambe, kombinacije in ključe in uporabo predpisov o arhiviranju. Tajni podatki stopnje tajnosti INTERNO se hranijo v pisarniških ali kovinskih omarah. Tajni podatki stopnje tajnosti ZAUPNO in TAJNO se hranijo v blagajnah, ki morajo ustrezati najmanj protivlomni stopnji II, določeni s standardi, ki v RS urejajo to področje. Tajni podatki stopnje tajnosti STROGO TAJNO se hranijo v blagajnah, ki morajo ustrezati najmanj protivlomni stopnji III, določeni s standardi, ki v RS urejajo to področje.

V zgornji levi kot vrat blagajne na zunanji strani se glede na stopnjo tajnosti podatkov, ki se hranijo v njej, prilepi nalepka primerne velikosti z veliko tiskano črko oziroma črkama:

- Z za stopnjo tajnosti ZAUPNO,
- T za stopnjo tajnosti TAJNO,
- ST za stopnjo tajnosti STROGO TAJNO.

Če se v varnostni omari hranijo podatki različnih stopenj tajnosti, mora vrsta blagajne ustrezati najvišji stopnji tajnosti podatkov, ki se hranijo v njej, in se s tako stopnjo tajnosti tudi označiti. Posamezno nastavitev kombinacije elektronskih ali mehanskih ključavnic na varnostnih omarah oziroma blagajnah lahko poznajo samo osebe, ki jih določi predstojnik organa. Predstojnik organa mora delovne naloge v organu razporediti tako, da je število oseb, ki so seznanjene s posameznimi kombinacijami, čim manjše.
Nastavitve kombinacij elektronskih in mehanskih ključavnic se zamenjajo:

- po namestitvi,
- vsakih šest mesecev,
- potem, ko oseba iz prejšnjega odstavka preneha opravljati naloge v organu, zaradi katerih je bila z nastavitvijo kombinacije seznanjena in
- kadar tako odloči predstojnik organa.

Ključi varnostnega območja oziroma ključi prostorov iz varnostnega območja se hranijo v posebnem prostoru zunaj tega območja, tako da je nepooblaščenim osebam onemogočen dostop. Dokumenti, ki vsebujejo tajne podatke, se arhivirajo skladno s predpisi, ki urejajo arhivsko dejavnost.

4.3 NACIONALNI ORGAN ZA VAROVANJE TAJNIH PODATKOV

V RS deluje UVTP kot nacionalni organ za varovanje tajnih podatkov (NSA) v okviru samostojne vladne službe. Z njegovo ustanovitvijo sta Urad zveze NATO za varnost in Varnostna pisarna Generalnega sekretariata Sveta EU dobila konkretnega sogovornika za sodelovanje na področju varnostnih zadev, kajti s sprejetjem ZTP je bil izpolnjen formalni pogoj za ustanovitev »varnostnega organa z nacionalno odgovornostjo« in posledično je ustanovitev zadostila minimalnim standardom za vstop v EU in zvezo NATO.

43. člen ZTP (Ur. l. RS, št. 50/06) določa, da »vlada za spremljanje izvajanja tega zakona in drugih predpisov, sprejetih na njegovi podlagi, ustanovi UVTP.« V 3. odstavku 46. člena

Zakona je zakonodajalec določil šestmesečni rok za ustanovitev urada, ki je s sklepom vlade[30] bil ustanovljen 26.01.2002. Dela in naloge UVTP so opredeljena v Sklepu UVTP (Ur. l. RS, št. 6/2002), v ZTP (Ur. l. RS, št. 50/06) ter v Aktu o notranji organizaciji in sistemizaciji delovnih mest v UVTP.

UVTP v skladu z njimi opravlja sledeče poglavitne naloge:

1. Spremlja stanje na področju določanja in varovanja tajnih podatkov in skrbi za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja tajnih podatkov v državnih organih, organih lokalnih skupnosti, pri nosilcih javnih pooblastil ter v gospodarskih družbah in organizacijah, ki pridobijo ali razpolagajo s tajnimi podatki.
2. Skrbi za izvrševanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju tajnih podatkov ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij. Skrbi za zagotavljanje varnosti tajnih podatkov v nacionalnih organih in v tujini ter v zvezi s tem opravlja zlasti naslednje naloge:

- izdaja dovoljenja za dostop do tajnih podatkov,
- izdaja varnostna potrdila pravnim osebam,
- izdaja varnostna potrdila za sisteme in naprave za prenos, hranjenje in obdelavo 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,
- nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države oziroma mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni nemudoma izvršiti ter

[30] Sklep o ustanovitvi, nalogah in organizaciji UVTP (Uradni list RS št. 6/02)

- izmenjuje podatke z nacionalnimi varnostnimi organi in mednarodnimi organizacijami.

3. Pripravlja predloge predpisov, potrebnih za izvajanje ZTP.
4. Daje mnenje o skladnosti splošnih aktov o določanju, varovanju in dostopu do tajnih podatkov.
5. Koordinira delovanje državnih organov, pristojnih za varnostno preverjanje.
6. Predlaga ukrepe za izboljšanje varovanja tajnih podatkov.
7. Vodi evidenco:

   - dovoljenj za dostop do tajnih podatkov (Ur. l. RS, št. 50/06, 22. člen),
   - dovoljenj fizičnim osebam za dostop do tujih tajnih podatkov (ibid. 43. člen),
   - izdanih varnostnih dovoljenj organizacijam (Ur. l. RS, št. 50/06, 35. člen),
   - izdanih varnostnih dovoljenj organizacijam za dostop do tujih tajnih podatkov (ibid., 43. b člen) in
   - začasnih dostopov do tajnih podatkov (Ur. l. RS, št. 50/06, 30. člen).

8. Organizira in izvaja usposabljanja s področja varovanja tajnih podatkov.
9. Opravlja druge naloge, ki so določene s predpisi, sprejetimi na podlagi ZTP.

UVTP na podlagi Akta o notranji organizaciji in sistemizaciji delovnih mest v UVTP organizira in izvaja usposabljanja s področja varovanja tajnih podatkov za osebe, ki jim je bilo izdano dovoljenje za dostop do tajnih podatkov EU ali zveze NATO stopnje TAJNO in STROGO TAJNO. Za organe in organizacije UVTP izvaja osnovno in dodatno usposabljanje s področja varovanja tajnih podatkov. Za organizacije (družbe) UVTP usposabljanja izvaja brezplačno, vendar le pod pogojem, da je na usposabljanju ustrezno število mest dano na razpolago državnim organom. Osnovno in dodatno usposabljanje v organih in organizacijah izvajajo izvajalci (osebe ali organizacijske enote), ki jih določi predstojnik. Program osnovnega in dodatnega usposabljanja lahko izvaja nacionalni varnostni organ, UVTP ali organizacija, katere osnovna dejavnost je usposabljanje in izobraževanje posameznikov (Ur. l. RS, 71/06 in 138/06, 23. člen). Urad s pristojnostmi, ki jih ima in ki jih bo morda v prihodnosti še imel, ne more v celoti preprečiti razkritja tajnih podatkov, vendar pa se možnosti ob bistvenem izvajanju zakona ter uredb lahko zmanjšajo.

Prvi del diplomske naloge lahko torej sklenemo z ugotovitvijo, da RS poseduje sodoben sistem varovanja tajnih podatkov, ki upošteva vse sodobne in uveljavljene standarde. Klasifikacija tajnih podatkov je primerljiva in kompatibilna z ostalimi klasifikacijami v EU in zvezi NATO, kar zagotavlja enako stopnjo varovanja tajnih podatkov, tako v RS kot tudi na nadnacionalni ravni. S spremembami ZTP, podzakonskih aktov in uredb so se spreminjali tudi postopki obravnavanja tajnih podatkov v RS in se s tem približali mednarodnim merilom. Na razvoj in vsebino sistema varovanja in ZTP so predvsem vplivale smernice EU in NATO, lahko rečemo, celo bolj kot pa same potrebe državnih institucij. V ospredju oblikovanja ZTP je tako mogoče zaslediti predvsem tendenco k prilagajanju in prevzemanju njihovih minimalnih standardov. Sprejetje ZTP je enotno uredilo celotno nacionalno področje obravnavanja in varovanja tajnih podatkov, saj je poenotilo terminologijo in strnilo dotedanje uredbe, ki so imele veljavo samo za določene organe. ZTP je od sprejetja v nekaj letih hitro in ustrezno dozorel z implementacijo nadnacionalnih in mednarodnih standardov, ki pa so morda prekomerno vplivali na njegovo vsebino.

Z ugotovitvijo, da je varovanje tajnih podatkov v RS normativno ustrezno urejeno, se postavlja vprašanje, kako ta sistem funkcionira v praksi. V naslednjem poglavju bom poskušala preko primerov napak v obravnavanju in zlorabah varovanja tajnih podatkov, analizirati predvsem potencialne vplive na obstoječi sistem. Prav tako pa bom s pridobitvijo mnenj posameznikov, ki so bodisi izvajalci ali opazovalci, poskušala ugotoviti funkcionalno stanje in percepcijo sistema varovanja tajnih podatkov v RS.

5 POJAVI ODTEKANJA TAJNIH PODATKOV V RS

V tem delu diplomske naloge se bom natančneje posvetila fenomenu javnega odtekanja tajnih podatkov. Pomanjkljivosti in napake so sestavni del delovanje organa, institucije ali organizacije. Označimo jih lahko kot nekaj, kar ni v skladu z določenim pravilom oz. normo. Medtem ko je pomanjkljivost primerjava zahtevane kakovosti na eni strani in realnega stanja na drugi strani, lahko napako pripišemo človekovemu delovanju. Ko govorimo o napakah človeka, imamo v mislih pravilnosti izvajanja določenega postopka, lahko pa tudi napake človeka v pogledu kršitve načel etičnega kodeksa, ki npr. velja za delavca javne uprave.

Scheppele (v Rajko 1997, 192) je prikazal dve možnosti ravnanja s tajnimi podatki:

1. tajnost tajnih podatkov lahko sporoči
    - A pove B neposredno tajnost (odkritje)
    - B pove C serijsko tajnost (izdaja)
    - A ali B pove C kolektivno tajnost (odtok),
2. tajnost tajnih podatkov lahko skrije
    - A skrije B neposredno tajnost (enostavna tajnost)
    - B skrije C serijsko tajnost (rabljena tajnost)
    - A ali B skrijeta pred C kolektivno tajnost (zarota).

Kot je razvidno, se je Scheppele osredotočil na dva generalna načina manipuliranja s tajnimi podatki, na nepooblaščeno sporočanje in skrivanje tajnosti. Za potrebe diplomske naloge je zanimiv prvi vidik, nepooblaščeno posredovanje podatkov, o katerem bo govora v nadaljevanju. Večina tajnih podatkov ostane tajnih do konca predvidenega časovnega obdobja. Niso pa redki primeri, ko pride do odtoka in se tajni podatki znajdejo na prvih straneh časopisov in v »prime timu« elektronskih medijev. Takrat govorimo o izdaji tajnih podatkov, njihovem razkritju.[31] Kot bomo videli v nadaljevanju, je veliko primerov razkritih tajnih podatkov predvsem z obveščevalno-varnostnega področja[32], vendar to niso edine informacije, ki so zaželene.

[31] Odtoki ali razkritje TP v tujini niso neznanka in tudi Slovenija pri tem ni nobena izjema. Tajni podatki različnih organov državne uprave se posredujejo v javnost.
[32] V preteklosti pa se je zvrstilo še več primerov kot npr: afera HIT, VIS, prenašanje dokumentov VIS v javnost.

5.1 PRIMERI JAVNEGA ODTEKANJA TAJNIH PODATKOV

"Poglejte v zgodovino slovenske države," je rekel Milan Kučan[33] in pojasnil, da ima tudi sam izkušnje s tem, kako se je na te stvari z levo roko zamahnilo, ko so prišli v javnost dokumenti, ki so nekomu ustrezali. *"Ta velik problem se zdaj celo skuša reševati z očitkom, da gre za nepatriotska dejanja. Če že to kvalifikacijo sprejmemo, potem je sleherno odtekanje zaupnih informacij nepatriotsko dejanje, in ne samo to."* je še dejal (TV Slovenija-Studio City, 29. januar 2008).

Primeri javnega odtekanja tajnih podatkov v RS imajo zgodovino, sedanjost in prihodnost. V nadaljevanju bom prikazala primere javno objavljenih tajnih podatkov, katerih vsebina je povzeta iz časopisnih in internetnih virov. Primeri analize bodo javno objavljeni članki na temo uhajanja tajnih podatkov, in sicer afera SAVA, afera SOVA, afera WASHINGTONSKA DEPEŠA in afera PATRIA. Glavni namen je, ugotoviti ali, je bil ZTP ustrezno implementiran, ali sistem varovanja tajnih podatkov deluje, ter, ko ne deluje, najti ključne razloge in dejavnike za njegovo nedelovanje. Posledično pa je moj namen tudi do določene mere prepoznati, oz. klasificirati varnostno kulturo v RS. Primeri so bili izbrani, ker vsak predstavlja delovno področje državnih organov RS, ki se nanašajo ali na javno varnost, obrambo, zunanje zadeve ali obveščevalno-varnostno dejavnost države, preko katerih bom poskušala analizirati predvsem potencialne vplive na obstoječi sistem obravnavanja tajnih podatkov.

5.1.1 PRIMER »SAVA«

10. junija leta 2000 je novinar Večera Blaž Zgaga objavil dokument, ki dokazuje in opisuje tajno operacijo »SAVA«. Šlo je za sodelovanje slovenske in ameriške obrambne obveščevalne službe (*Defence Itelligence ageny-DIA*) pri zbiranju podatkov o tedanji vojski Jugoslavije. Zgaga je prišel do dokumentov OVS (ti so bili označeni kot zaupni), ki naj bi ameriškim vohunom predvsem pomagali pri zbiranju informacij, a jim je na drugi strani tudi razkril mrežo svojih agentov. DIA naj bi brez mednarodnega sporazuma, se pravi brez pravne podlage in dokumentov, vodila in financirala operativce slovenske OVS v tretjih državah. Po

[33] Intervju z nekdanjim predsednikom RS, z mandatom v letih 1992 do 2002.

pisanju Zgage, direktor OVS-a Bojan Vavtar operacije SAVA sicer takrat ni odobril, pa vendar je stekla brez njegove vednosti (Bukovec, 2007).
Treba je omeniti, da je vsa ta zadeva potekala v času državnozborskih volitev l. 2000, ko je bila izvoljena nova vlada. Hkrati pa so takrat potekala pristopna pogajanja za članstvo v zvezi NATO. Po navedbi medijev, bi lahko primer razkritega dokumenta negativno vplival na pristopna pogajanja (K.N.S./M.E., 2000). Dejanskih učinkov v zvezi s tem pa ni bilo mogoče zaslediti, možna so le ugibanja. Po objavi članka je bila izvedena hišna preiskava v stanovanju novinarja Večera Blaža Zgage in v ljubljanskem dopisništvu časnika. Zaradi domnevne izdaje vojaške tajnosti je bil proti Blažu Zgagi, Zvonetu Murku (agent VOMA) in še enemu obtoženemu uveden pregon, vendar se je zadeva končala v njihov prid že v predkazenskem postopku. Sodišče je namreč v postopku ugotovilo, da so bili ti dokumenti neupravičeno in nepotrebno označeni kot zaupni. Prav tako tožilstvo ni dokazalo, da so bile povzročene kakršnekoli škodljive posledice za državo, ter da niso bili podani znaki kaznivega dejanja (Štamcar, 2000).

Iz tega primera ni jasno razvidno, na kateri točki je varovanje tajnih podatkov odpovedalo, saj ni poznano, kako je bil dokument odtujen, poleg tega pa ni dovolj podatkov, ki bi osvetlili povezavo in motive obtoženih (posrednikov dokumenta). Lahko domnevamo, da je do kritičnega dogodka, zaradi katerega je prišlo do uhajanja tajnih podatkov, prišlo na stopnji bodisi razmnoževanja, uničenja nosilcev ali hranjenja tajnih podatkov. Po mojem razmišljanju so to edini postopki obravnavanja tajnih podatkov, pri katerih je mogoče ustvariti duplikate dokumentov, hkrati pa so bili ti dokumenti že vneseni v sistem tajnih podatkov, kar pomeni da so bili predhodni postopki domnevno ustrezno izvedeni. Pri tem bi izpostavila dva bistvena problema, in sicer ustrezno sledljivost in pa možnost nekontroliranega prenosa dokumentov tako iz sistema kot iz varnostnega območja, kjer se obravnavajo tajni podatki. Iz pridobljenih virov ni mogoče ugotoviti, kako so bili identificirani tisti, ki so odtujili dokumente, ter kako so bili posredovani, hkrati pa je tudi motiv tega početja nejasen. Glede na to, da sem v tem obdobju zasledila intenzivnejše politično dogajanje na katerega pa ta zadeva ni imela učinka je mogoče, da so bili motivi, ki so privedli do tega bolj osebne narave. Politični motivi pa so predvsem vplivali na klasifikacijo oz. označevanje tajnih podatkov.

Pred sprejetjem ZTP (ZTP je bil sprejet l. 2001, do domnevnega razkritja pa je prišlo že l. 2000) je bilo varovanje tajnih podatkov relativno urejeno po posameznih organih, vendar brez vnaprej znanih kriterijev. S tem, kot je že bilo omenjeno, je prišlo do poplave tajnih podatkov.

Afera SAVA je pokazala, da je nepotrebno vsakršen dokument označevati kot tajen, ter da je sistem narekoval zakonsko vzpostavitev področja varovanja tajnih podatkov, v nasprotju z dotedanjo prakso. Zanimiva je torej tudi ugotovitev, da je lahko politično motivirano tudi označevanje tajnih podatkov in ne samo razkritje. Podobne ugotovitve sem zasledila tudi v intervjuju s Praprotnikom[34], ki pravi, da so se kriteriji označevanja dokumentov izboljšali v tolikšni meri, da več ne prihaja do nepotrebnega označevanja stopenj tajnosti dokumentov. Ugotavlja, da je to posledično tudi vplivalo na zmanjšanje celotnega števila tajnih podatkov. S tem primerom je bilo jasno pokazano, da je klasifikacija tajnih podatkov zelo kritična točka obravnavanja le teh. Opozarja pa tudi, da navkljub uveljavitvi novih kriterijev, se le ti še vedno zlorabljajo za neutemeljeno označevanje. Slednje sem zasledila že pri Scheppele-ju, ki je prikazal dve možnosti manipuliranja s tajnimi podatki, nepooblaščeno sporočanje in skrivanje tajnosti, kar lahko opazimo tudi v tem primeru.

Z jasno izraženimi kriteriji se zmanjšuje možnost napačne ali manipulativne označbe dokumentov, kot pa bomo videli sami kriteriji teh pojavov ne izključujejo. Postavlja se potreba po sistemu, ki dokument obravnava ne samo na podlagi kriterijev določene stopnje tajnosti in določene oznake ampak tudi z varnostnimi mehanizmi, ki pogojujejo višji nivo sledljivosti in večstopenjsko preverjanje dokumenta kot tudi okoliščin ob njegovem nastanku (Primer MZZ).

5.1.2 PRIMER »SOVA«

Razkritje tajnih dokumentov SOVE se je zgodilo 21. 03. 2007, ko je časnik Dnevnik objavil prvi članek z naslovom »Dolgi politični prsti v bazah najbolj zaupnih podatkov« (Praprotnik, 2007). Po navedbah novinarja Dnevnika, Roka Praprotnika, naj bi Vlada ustanovila 10-člansko delovno skupino za pregled tajne dokumentacije SOVE. Takratna poizvedovanja novinarja so sicer pripeljala do zaključka, da je Vlada na seji sprejela sklep o imenovanju delovne skupine, katere ena izmed nalog, zapisanih v tajnem sklepu je, ugotoviti zakonitosti in smotrnost hranjenja arhivskega gradiva SOVE, vendar informacija o tem ni bila nikjer objavljena. Med drugim tudi ni bilo jasno, zakaj je skupina bila ustanovljena, kdo so njeni člani, kakšna sta njen mandat ter zakonska podlaga za delovanje.

[34] Glej intervju s Praprotnikom v prilogi C, vprašanje 3.

Med afero SOVA se je odkrilo še več tajnih dokumentov, ki so zaznamovali leto 2007, v duhu ene največjih afer v zgodovini Slovenije. Eno izmed razkritij je bilo tudi, da obstaja črni fond SOVE, v katerem je bila večina denarja iz sodelovanja z nemško obveščevalno službo, (*Bundesnachrichtendienst-BND*). Slovenska in nemška vlada sta namreč sklenili tajni sporazum o operativnem sodelovanju. Težava je bila v tem, da »črni fond«, kot že samo ime pove, nima zakonske podlage. Obstoj fonda je vodil še naprej v razkritje tajne lokacije v bližini stavbe Telekoma v Ljubljani, kjer naj bi SOVA v sodelovanju z BND, prisluškovala predvsem pogovorom na področju bivše Jugoslavije (Hrvaške, Srbije in BIH). Priključitve za prisluškovanja so namreč bile tajno izvedene na glavni mednarodni optični vod. S tem naj bi tako SOVA kot BND prisluškovali oziroma snemali pogovore med hrvaškim premierom Ivom Sanaderjem in takratnim slovenskim premierom Janezom Janšo. To je vso afero še dodatno razpihnilo, saj je prišlo do medpolitičnega obračunavanja tudi glede vsebine teh posnetkov (obtožba Antona Ropa za insciniranje incidentov v Piranskem zalivu po dogovoru med premieroma). Vse to naj bi imelo po navedbah medijev paralizirajoč učinek za delovanje SOVE v mednarodnem okviru (Praprotnik, 2008). Domnevamo lahko, da so se tuje obveščevalno-varnostne službe vsekakor odzvale na to razkritje in najbrž ukrepale ter se dodatno zavarovale, oz. prekinile določeno sodelovanje s SOVO. Poleg tega pa je SOVA s tem izgubila najbrž kar precejšen delež mednarodne kredibilnosti.

Kot v primeru SAVA lahko tudi v primeru SOVA ugotovimo podoben problem pri ugotavljanju načina razkritja tajnih podatkov. Kot poprej predvsem najbrž zaradi novinarskega varovanja virov ni jasno, na kateri stopnji obravnavanja so bili dokumenti odtujeni. Spet je to prepuščeno domnevi, najverjetneje pa se je to dogodilo bodisi pri razmnoževanju tajnih podatkov ali pa je prišlo do odtujitve iz varnostnih območij, namenjenih hranjenju podatkov. Lahko sklepamo, da takšno delovanje brez odkritih krivcev dopušča le pomanjkljiva sledljivost kot tudi pomanjkljiva kontrola dostopov do tajnih podatkov. V zvezi s tem primerom je potrebno omeniti tudi nivo varnostne kulture. Vprašljivo je namreč razkrivanje tajnih podatkov, kjer je Anton Rop javnosti odkrito posredoval detajle informacij, pridobljenih v okviru delovanja SOVE in BND. V intervjuju Praprotnik ugotavlja namreč prav te slabosti, kjer funkcija avtomatično odpira dostop do vseh tajnih podatkov, ne glede na need to know princip. Hkrati pa opozarja na odsotnost varnostne kulture v tem primeru[35].

[35] Poglej odgovor na 8. vprašanje intervjuja, v prilogi številka C.

Če se vrnemo nazaj k prej omenjeni 10-članski skupini, ki je po pisanju medijev tudi večkrat vstopila v poslopja SOVE, je po neuradnih virih bila sestava sledeča: vodja skupine je bil nekdanji minister za pravosodje, g. Lovro Šturm, člani pa so bili nekdanji minister za šolstvo, Milan Zver, nekdanji minister za, okolje Janez Podobnik, Karl Erjavec, Vinko Gorenak (uslužbenec Kabineta predsednika vlade), dr. Tone Jerovšek (nekdanji ustavni sodnik), dr. Milko Mikola (Sektor za popravo krivic in narodno spravo), Peter Ješovnik, Aleksander Lavrih (uslužbenec Kabineta premiera in bivši delavec Vojaške obveščevalne službe) ter Branko Cvelbar (SOVA, prišel v takratnem mandatu z obrambnega ministrstva) (Praprotnik, 2007).

Takratna parlamentarna komisija za nadzor nad tajnimi službami je javno izrazila skrb nad motivi delovanja takratne delovne skupine za oceno dela SOVE. Davorin Terčon, takratni predsednik parlamentarne komisije za nadzor nad tajnimi službami, je kot zelo verjetno označil izjavo podpredsednika te komisije, Dušana Kumra, da delovna skupina ne pregleduje tistega, kar bi morala, temveč tisto, kar je v interesu politične pozicije.

»Ti pregledi imajo še najmanj zveze z obdobjem pred letom 1990 in arhivi SDV(arhiv nekdanje komunistične tajne službe), ampak je to samo izgovor za rovarjenje po podatkih iz sedanjega obdobja.« (Kumer D. za Dnevnik, 2007)

V zbranih člankih je prikazano, da si je takratna politična pozicija, samovoljno in prikrito z izkoriščanjem načela tajnosti, odprla vrata do tajnih podatkov in si omogočila nadzor in izkoriščanje le-teh. Prva kritika tega delovanja je sama sestava tako imenovane delovne skupine, ki so jo sestavljali koalicijski partnerji oz. ožji krog predsednika Vlade, brez neodvisnega nadzora. To dejstvo je predhodno že ugotovil dr. Iztok Prezelj, ki je v intervjuju za časnik Dnevnik izjavil, da je » v strokovnem smislu sestava skupine nenavadna, saj dva člana le-te nista dovolj kompetentna za takšen nadzor«(Caharijas, 2007). Po Prezljevem mnenju bi s strokovnega vidika morala biti skupina sestavljena izključno iz »državotvornih ministrstev«. Druga kritika je namen te skupine, ki je bila opredeljena kot »delovna skupina za oceno dela SOVE «. V medijih so se pojavljale informacije, da je skupina delovala izven svojega okvira, saj naj bi dostopala do izredno občutljivih tajnih podatkov. Tudi takih, ki so vitalnega pomena za obstoj in delovanje SOVE[36], hkrati pa je tudi ogrozila sodelovanje s

[36] Agenturna mreža in denarni skladi.

povezanimi osebami, podjetji ter tujimi obveščevalnimi službami. Vlada je namreč odprla dostop neustrezno usposobljenim, nenadzorovanim osebam in s tem ogrozila integriteto tajnosti podatkov in delovanja SOVE. »Vsaka prekomerna politizacija delovanja obveščevalnih služb je za državo in za te službe škodljiva,« zaključuje Prezelj (Caharijas, 2007).

5.1.3 PRIMER »WASHINGTONSKA DEPEŠA«

Časnik Dnevnik je v januarju 2008 objavil novico o razkritju zapisnika MZZ. Natančneje je dokument vseboval zapis pogovora predstavnikov MZZ s predstavniki ameriške administracije v Washingtonu, ki so ga opravili 24. decembra 2007. V pogovoru so predstavniki obeh držav obravnavali regionalne in geopolitične zadeve, sodelovanje med ZDA in EU (katere predsedstvo je prevzela Slovenija v januarju 2008) ter svetovna krizna žarišča. Hkrati so ameriški predstavniki izrazili tudi želje ZDA glede takrat aktualnega stanja Kosova, Bližnjega Vzhoda in Kavkaza ter kakšna so pričakovanja glede vrha EU in ZDA ter vsebina skupne deklaracije tega vrha. (Roglič in Mekina, 2008)

Časnik Dnevnik je dokument prejel v celoti in ga povzetega tudi (javno) objavil. Dokument namreč zaradi neznanega razloga ni bil ustrezno označen kot zaupen, hkrati pa se je zaradi tega znašel v širše dostopni, pri čemer je potrebno poudariti, interni računalniški mreži, do katere ima dostop večje število uslužbencev MZZ. Neznana oseba je nato iz te mreže prenesla dokument ter ga posredovala časniku. Kljub obširni preiskavi dogodka, na MZZ domnevni storilec niti ni bil identificiran, s čimer se ponovno postavlja vprašanje sledljivosti, čeprav gre v tem primeru sicer za javno odprt dokument, ki pa lahko nemoteno in brez evidentiranja zapusti državni organ.

Vsebina dokumenta je bila medijsko obravnavana kot diktiranje politike s strani ZDA Sloveniji, kot predsedujoči državi EU. V odzivih na pisanje časnika so na MZZ večkrat poudarili, da je interpretacija tega dokumenta medijsko polarizirana ter neustrezno in nestrokovno povzeta kot politična izjava, ki »predsodi« odziv slovenske zunanje politike na težnje in želje politike ZDA. Saj »branje takšnih zapisnikov (poročil, depeš, brzojavk ...) predpostavlja ustrezno izobrazbo in znanje. Navsezadnje pa tudi kulturo!« ((ds), (STA,pn), 2008)

Profesor fakultete za družbene vede, doc. dr. Milan Brglez, je v izjavi, prav tako za časnik Dnevnik, ob poročanju o aferi pomembno izpostavil dvojnost problema objave in vsebine dokumenta. Priznava sicer, da so pritiski velesile ZDA realnost, vendar obenem dodaja, da je to tudi način tesnega sodelovanja za oblikovanje političnega sodelovanja. Hkrati pa je to tudi možna praksa ameriške politike. Poleg tega pa ostaja vedno odprto vprašanje odziva države na izražene zahteve, pa tudi sama implementacije teh zahtev. Zaradi tega in posledičnega vpliva na pretok informacij med ZDA in Slovenijo, te zadeve po njegovem mnenju niso javno dostopne. Hkrati pa je po njegovem mnjenu pomembno tudi, katera država sodeluje v takih pogovorih, saj je na tem primeru mogoče tudi reči, da se zadeva tudi zaradi udeležencev lahko medijsko stigmatizira.

»Najverjetneje je zadeve teže implementirati, če se ve, da so to ameriške zahteve.« (Roglič in Mekina, 2008)

Če povzamemo te izjave, že sami ti vplivi kot tudi izvajanje politik narekujejo s tem povezanim dokumentom določeno stopnjo tajnosti. Brglez zaključuje, da je objava takih dokumentov lahko kontra-produktivna za odnos med državama oz. za oblikovanje politike (podoben učinek smo lahko ugotovili za delovanje SOVE v omenjenih pregledih vladne skupine, predvsem v oziru na sodelovanje s tujimi varnostnimi službami).

V primeru MZZ ne moremo govoriti o odpovedi postopka obravnavanja tajnih podatkov, kot tudi ne določiti kritičnih točk že zaradi samega dejstva, da ta dokument sploh ni bil vključen v sistemsko ureditev varovanja tajnih podatkov. Problematičen je predvsem postopek klasifikacije dokumenta, pa tudi varnostna kultura vključenih subjektov, ki dokumente obravnavajo zgolj na podlagi oznak. Po mojem mnenju sta bistvenega pomena v tem primeru predvsem obravnava procesa ter sistema, ne pa zavestnega ali nezavednega delovanja posameznikov. Ni namreč vzpostavljenega dodatnega preverjanja dokumentov, saj je kljub vsebini, ki narekuje oznako zaupno, ta dokument ostal brez oznake. Po definiciji ZTP je »tajni podatek 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 navedenem zakonu, zavarovati pred nepoklicanimi osebami.« (2. člen ZTP) Glede na to, da pooblaščena oseba po ZTP določa, kdaj se podatki označijo kot tajni, bi bilo smotrno, da je v tem procesu potreben tudi varovalni mehanizem, ki lahko morda tudi brez poznavanja vsebine iz okoliščin, udeležencev in drugih dejavnikov preveri ustrezno

označbo dokumenta. Prav tako bi sam informacijski sistem moral zahtevati večkratno preverjanje ustrezne označbe dokumenta pred vnosom v interne mreže. Še bolj kritično pa je dejstvo, da je kljub napaki v tem primeru mogoče dokumente brez sledljivosti (kljub navedbi, »da se posegi v interne dokumente beležijo« (Bernard R. V., 2008)). pridobiti že iz internega sistema. Slednje bi lahko imeli tudi za pokazatelj, da je v praksi že sam dokumentni sistem slovenskih ministrstev pomanjkljiv, posledično pa je lahko zanesljivost sistema za varovanje tajnih podatkov tudi vprašljiva. Dodatno pa je ob tem primeru mogoče reči, da je posameznik zelo labilen del sistema za varovanje podatkov, saj izkoristi vsakršno napako za odtekanje tajnih podatkov, dodatno pa se na sistem tudi preveč zanaša samo v primeru, ko dokument nosi oznako.

Potrebno pa je dodati, da v tem primeru obstaja še dilema, ali gre tu res za uhajanje tajnih podatkov. Glede na to, da omenjeni zapisnik ni imel oznake, se nam poraja vprašanje, ali ga sploh lahko obravnavamo v okviru ZTP in seveda, ali gre tukaj posledično za javno odtekanje. Po ZTP tajnosti dokumenta ne določa le oznaka ampak tudi vsebina. Seveda pa se je treba ob tem tudi vprašati ali naj ima vsak dokument v interni mreži »prost izhod« ali pa naj se vsaj podreja smotrnemu vodenju in evidenci dokumentov.

Morda je bila najbolj proaktivna pot za vzpostavitev stabilnega sistema prav reakcija MZZ na ta dogodek. MZZ je takrat javno napovedalo tako sistemske (poostritev dostopa v računalniški sistem do informacij) kot tudi normativne ukrepe za ureditev dostopa do dokumentov MZZ.

5.1.4 PRIMER »PATRIA«

Razpis nakupa oklepnikov za Slovensko vojsko je v javnosti znan kot afera PATRIA. Mogoče ne gre toliko za sam razpis kot vso dogajanje okrog njega, ki se je pričelo v letu 2006 in se po dveh letih raziskovanja in preiskovanja še ni dokončno razrešilo. Tudi dogajanje pred tem je pomembnega značaja za razumevanje nastale situacije.

Namreč v letu 2004, proti koncu mandata nekdanjega ministra za obrambo, dr. Antona Grizolda, je bilo podpisano pismo o nameri nakupov oklepnikov 8x8 v podjetju Sistemska tehnika. Po zamenjavi takratne vlade, je novi minister za obrambo Karel Erjavec v letu 2006 razpisal mednarodni razpis za pridobitev oklepnikov, kljub pismu o nameri. Na razpis sta

prijavila že omenjena Sistemska tehnika in Rotis, vsak s svojim izdelkom. Sistemska tehnika je ponudila Krpana, Rotis Patrio. Oba bi se proizvajala v Sloveniji. V času testiranja oklepnikov, sistemska tehnika še ni imela proizvedenega prototipa vozila, zato je sodelovala z avstrijskim Pandurjem II. V večini preizkusov je zmagala Patria ter kmalu za tem, natančneje 12. junija 2006, je MORS napovedal podpis pogodbe z Rotisom in posledično nakup oklepnikov Patria (Zgaga, 2008).

Afera je dobila svoje razsežnosti po tistem, ko je iz opozicijskih poslanskih vrst prišel poziv za revizijo postopka razpisa in pogodbe. Tudi Sistemska tehnika je vložila tožbo proti Sloveniji in Rotisu za razveljavitev pogodbe ter zaprosila za vpogled v ponudbo Rotisa, kar jim je bilo zavrnjeno. Po odzivu Odbora za obrambo DZ RS je bila narejena ocena ponudbe, ki je potrdila ugodnost ponudbe, vendar je že nakazala nekatera odprta vprašanja. Ta so se pojavila dovolj hitro, da je DZ spet pozval k obravnavi, saj je časopis Dnevnik objavil članek, v katerem razkriva, da se je cena za Patrie podražila za tretjino in da se bo dobava oklepnikov zavlekla. Po zadnji ministrski zamenjavi so se stvari pričele še bolj odvijati, ko je ministrica odkrito spregovorila o tem, da smo oklepnike Patria preplačali, ali drugače, za denar, ki smo ga plačali, nismo dobili obljubljenega.

Tako tudi v aferi Patria lahko zasledimo izkoriščanje stopnje tajnosti, in sicer za to, da se prikrijejo informacije v zvezi z nabavo oklepnikov Slovenske vojske. Nejasnosti, ki so se pojavljale v zvezi s tem, pa so precej povečala zanimanje javnosti. Ugotovitve tega sem zasledila tudi v intervjuju, ko je g. Praprotnik izjavil, da *»stopnja ogrožanja prej ni bila takšna, da bi opravičevala oznako na dokumentih Patrie.*[37]*«* Ko pa je interes tega, da ostanejo dokumenti tajni, prenehal, se je javnost z nastalo situacijo lahko seznanila. Največji motiv za razkritje dokumentov, ki so jih odgovorni skrivali pod stopnjo tajnosti, v primeru afere Patria, je bil interes javnosti, vse bolj pa tudi skrivanje nepravilnosti v tej zadevi.

Ponovno lahko opozorimo torej na zlorabo postopka klasifikacije tajnih podatkov, poleg tega pa je ponovno zaslediti nejasnost glede točke uhajanja v postopku obravnavanja le-teh. Mogoče je, da je prišlo do uhajanja na najbolj izpostavljenih točkah obravnavanja tajnih podatkov in sicer razmnoževanju in hranjenju. Glede na vire ni mogoče identificirati tako

[37] Glej prilogo C, intervju s Praprotnikom, vprašanje 7.

oseb kot tudi samega načina uhajanja podatkov v javnost oz. medijem. Ključna manjkajoča komponenta je ponovno sledljivost.

»*V demokraciji je razumljivo, da namesto iskanja odgovora na ključno vprašanje - ali je bilo podkupovanje ali ne - bo zdaj prišlo do medsebojnega obtoževanja, ki ne vem, komu koristi". "Razčiščevanju te zadeve vsekakor ne*!« (Uredništvo Mladine, 2008)

Dogajanja, kot npr. objava in navedbe finske televizije o provizijah in podkupninah ter posledično preplačanih oklepnikih, gotovo so razkritja informacij javnosti. Koliko so povezana z razkritjem tajnih podatkov, vedo odgovorni sami. Primer pa je povezan tudi s takratnim političnim dogajanjem v Sloveniji, saj je afera malo pred državnozborskimi volitvami 2008 dosegla višek. Finski novinar je javno obtožil, da je Patria podkupila Janeza Janšo, predsednika Vlade RS in nekatere druge visoke uradnike ter, da so sklenili orožarski posel z njimi. S tega vidika so mediji afero Patria poimenovali tudi kot politično ali orožarsko afero, ki je kreirala komunikacijo predvolilne propagande. Podobno ugotavlja tudi Praprotnik[38], ki pravi, da »ko pride do razkritja neupravičeno označenih tajnih podatkov, se lahko tistim, ki državo vodijo, pripiše odgovornost in s tem ustrezne konsekvence, ki jih brez razkritja ne bi bilo.«

Primer afere Patria na eni strani pokaže na bistveno stvar politike in nas opozori na dejstvo, da je lahko tajnost ter s tem povezano prikrivanje tajnih podatkov na nek način zakrivanje odgovornosti vladajočih do volivcev na političnem parketu in javnosti na splošno. V primeru, ko gre za poskus prikrivanja nepravilnosti in njegovo objavo, se izvaja nadzor nad oblastjo. Na drugi stani pa oblast sama z nezakonitim označevanje lahko poskuša ta nadzor omejiti. Še ena bistvena ugotovitev, ki se je pokazala v primeru afere Patria, je politična diskreditacija, predvsem preko manipuliranja z raznimi informacijami o tajnih dokumentih v času predvolilnega boja in posledično s slabšim oz. boljšim rezultatom na volitvah.

5.2 SINTEZA UGOTOVITEV IZ PRIMEROV

V Tabeli 5.1. sem želela povzeti skupne elemente, ki se, oz. se ne pojavljajo v predstavljenih primerih. Skupna točka vsem primerom je predvsem nejasnost glede tega, na kateri stopnji

[38] Glej prilogo C, intervju s Praprotnikom, vprašanje 11.

obravnavanja tajnih podatkov prihaja do uhajanja. Najverjetneje lahko popolnoma izključimo prve štiri stopnje obravnavanja tajnih podatkov, ki so sprejem, evidentiranje, dodeljevanje in posredovanje tajnih podatkov. Tako je najbolj verjetno, da prihaja do uhajanja na stopnji bodisi pri razmnoževanju, uničenju nosilcev ali hranjenju tajnih podatkov. Predvsem je bistvena manjkajoča komponenta v teh primerih jasna sledljivost rokovanja s tajnimi podatki v teh stopnjah, s katero bi lahko točneje identificirali tako stopnjo kot tudi vpletene v ta proces. Še en element, ki ga je mogoče v teh primerih zaslediti, pa je problematika klasifikacije. Na eni strani se klasifikacija zlorablja za prikrivanje občutljivih podatkov, hkrati pa je na drugi strani tako po vsebini kot tudi po okoliščinah preveč prepuščena samovoljnemu in samostojnemu dodeljevanju stopenj tajnosti.

TABELA 5.1: Primerjava ugotovitev analiziranih primerov

PRIMER/ UGOTOVITVE	Sava	Sova	Washingtonska depeša	Patria
TOČKA UHAJANJA*	razmnoževanje, uničevanje, hranjenje	razmnoževanje in hranjenje	brez oz. klasifikacija	klasifikacija ter razmnoževanje in hranjenje
ZLORABA TAJNOSTI**	DA	NE	NE	DA
MOTIVI ZA IZDAJO	politični	politični[1]	nejasno	politični
POLITIČNI KONTEKST	državnozborske volitve 2000, pristopna pogajanja za NATO	utrjevanje pozicije[2]	predsedovanje EU	državnozborske volitve 2008
IDENTIFICIRANI OSUMLJENCI	DA	NE	NE	NE
SODNI EPILOG	NE[3]	NE	NE	NE

*Na kateri točki obravnavanja tajnih podatkov je prišlo do možne odtujitve.
**V smislu prikrivanja spornih podatkov pod stopnjo tajnosti.
[1] V osnovi ni šlo za uhajanje tajnih podatkov, temveč za samovoljni dostop s strani Vlade.
[2] Ni povsem jasno, kaj se je dogajalo, saj so bili izraženi številni dvomi glede delovanja komisije za nadzor SOVE.
3 Zaradi neupravičene oznake so bili osumljenci izdaje tajnega podatka v predkazenskem postopku oproščeni, sankcije proti tistim, ki so podatek tako označili, pa niso znane.

5.3 INDIVIDUALNI POGLEDI NA VAROVANJE IN ODTEKANJE TAJNIH PODATKOV

Z individualnimi pogledi treh predstavnikov različnih sistemov ali, bolje rečeno, preko intervjujev z njimi, lahko bolje ovrednotimo sistem in s tem pridobimo merodajnejše podatke za analizo delovanja in implementacije sistema. Z g. mag. Tarmanom sem naredila intervju na podlagi dejstva, da je najvišji predstavnik sistema, oz. je predstavnik sistema varovanja tajnih podatkov v okviru vladajoče pozicije. To dejstvo se mi zdi zelo pomembno, še posebej, če bomo na drugi stani z njegovim mnenjem primerjali mnenja predstavnika prakse (g. Gregorja Klemenčiča) in predstavnika medijev (g. Roka Praprotnika – oba intervjuja sta povzeta nadalje).

Za pridobitev podatkov sem uporabila strukturiran intervju s polzaprtimi vprašanji. Vprašanja so zasledovala naslednje teme:

- vloge intervjuvancev v odnosu do sistema varovanja tajnih podatkov
- motivi za razkrivanje tajnih podatkov
- vpliv ZTP na ureditev področja v RS in uhajanje tajnih podatkov
- vpliv politike in političnega dogajanja na uhajanje in varovanje tajnih podatkov v RS
- vpliv posameznika v sistemu varovanja tajnih podatkov v RS
- pomen in razumevanje varnostne kulture v RS

5.3.1 Intervju z direktorjem Urada Vlade RS za varovanje tajnih podatkov

Mag. Milan Tarman je direktor UVTP. Po 3. členu Sklepa o ustanovitvi, nalogah in organizaciji UVTP, direktorja »imenuje in razrešuje vlada na predlog generalnega sekretarja vlade. Za svoje delo in delo urada je odgovoren vladi in generalnemu sekretarju vlade«.

»Akt o notranji organizaciji in sistemizaciji delovnih mest v Uradu izda na predlog direktorja Urada in po predhodnem soglasju Vlade RS generalni sekretar Vlade najkasneje v 30 dneh po uveljavitvi tega sklepa.« (4. člen)

Z g. mag. Tarmanom sem naredila intervju na podlagi dejstva, da je najvišji predstavnik sistema, oz. je predstavnik sistema varovanja tajnih podatkov v okviru vladajoče pozicije. To dejstvo se mi zdi zelo pomembno, še posebej, če bomo na drugi stani z njegovim mnenjem primerjali mnenja predstavnika prakse (g. Gregorja Klemeniča) in predstavnika medijev (g. Roka Praprotnika). Na tak način lahko bolje ovrednotimo sistem, ker s tem pridobimo merodajnejše podatke za analizo delovanj in implementacije sistema.

V začetku intervjuja je g. Tarman predstavil zgodovino, naloge ter delo urada po zakonskih določilih in skladno z njimi tudi različne projekte, ki pokrivajo tako področje mednarodnega sodelovanja kot delo na področju varovanja tajnih podatkov v Sloveniji. Nekaj tega je bilo že omenjeno[39], lahko pa dodamo še pogled g. Tarmana na prednostne naloge urada oz. ključne dosežke v mandatu 2004-2008. Kot ugotavlja g. Tarman, je Urad v tem obdobju okrepil sodelovanje na podlagi medresorskih skupin (ministrstva, službe, uradi…) ter v okviru področja varovanja tajnih podatkov okrepil odnose na mednarodni ravni. Velik prispevek k varnostni kulturi je urad dodal s pripravami gradiv s področja dela in z uspešno predstavitvijo na Odboru za državno ureditev in javne zadeve, Vladi RS ter za potrebe bilateralnih sporazumov na Odboru za zunanjo politiko DZ.

Zaključim lahko, da se preko znanja in izobraževanja ter v primeru Urada - sodelovanje z univerzami in z ustvarjanjem »socialnega kapitala«[40] med državami, lahko nadejamo tudi dobrih rezultatov in zavedanja varnostne kulture posameznikov v RS. Tudi g. Tarman se pridružuje mnenju, da je posameznik ključni člen v sistemu varovanja tajnih podatkov in pravi, da sta prav ozaveščanje posameznikov in organizacij ter krepitev varnostne kulture ključnega pomena. Vlogo UVTP-ja pa v skladu s tem vidi v vlogi dajanja nasvetov tistim, ki jih rabijo in v odprtosti za vse.

V intervjuju je g. Tarman izrazil tudi mnenje, da je posameznik ključni člen v sistemu varovanja tajnih podatkov, predvsem pa tudi njegovo delovno okolje in organizacijska klima. Navedel je tudi pomembno dejstvo, da mora vsak posameznik, ne glede na obseg vkljuenosti v delo s tajnimi podatki, biti sposoben te ustrezno obravnavati. Če je soočen s pomisleki, je

[39] V poglavju o NSA

[40] Socialni pomeni, da gre za neke relacije med ljudmi, beseda kapital pa nakazuje a to, da imajo relacije vrednostno izraženo komponento. Drugače lahko socialni kapital opredelimo kot vir, ki pospešuje aktivnosti med ljudmi, oz. gre za pogostost in pomembnost stikov, na katere se posameznik lahko zanese z namenom izboljšanja svojega položaja. Socialni kapital temelji na socialnih vezeh. Socialne vezi se razvijajo med posamezniki, organizacijami in družbami, ki se medsebojno povezujejo zaradi svojih ali širših kolektivnih koristi. (http://www.daimonion.si/socialni-kapital-in-linkedin.php)

UVTP organ, ki mu primerno svetuje in ga vodi ob takih nalogah. Ob tem je naštel tudi nekaj primerov motivov uhajanja tajnih podatkov, od malomarnosti preko naklepa pa do tega, da je vrednost tajnih podatkov odvisna od posameznih področij (primer: vojaški-NATO, strateški-EU …). Kjer obstajajo motivi, pa mora obstajati tudi pozornost ne samo v smislu izobraževanja v skladu z ravnanjem tajnih podatkov, ampak nenazadnje tudi opozarjanje na konsekvence in kompetentnost.

UVTP je pod vodstvom g. mag. Milana Tarmana ustrezno normativno urejen, hkrati pa po njegovih lastnih besedah celo presega normative mednarodnih standardov. Kot ugotavlja, je sistem v letih od vzpostavitve bil ustrezno implementiran. Poudarja pa, da praksa narekuje določene nove in dopolnjene predpise, čemur UVTP z upoštevanjem »dobrih praks« članic NATO in EU ažurno sledi. Standardi normativne ureditve v RS so strožji, kot jih narekujejo minimalni, praksa pa mogoče že na nekaterih področjih kaže na potrebo po bolj pragmatični ureditvi, posebej na področjih fizične in industrijske varnosti[41]

5.3.2 Intervju z v.d. vodje Službe za tajne podatke, CR/PR EU in PR/NATO na Ministrstvu za zunanje zadeve

G. Gregor Klemenčič je v.d. vodje Službe za tajne podatke, CR/PR EU in PR/NATO[42] na Ministrstvu za zunanje zadeve. Mnenja g. Klemenčiča bodo odsevala predvsem pogled na praktični vidik varovanja tajnih podatkov na MZZ, v primerjavi z mnenjem predstavnika sistema varovanja tajnih podatkov mag. g Tarmanom in predstavnikom medijev g. Praprotnikom.

Glavne naloge ZTP, ki jih je g. Klemenčič omenil[43] so vodenje centralnega podregistra EU in podregistra NATO tajnih podatkov v skladu z varnostno politiko EU in NATO ter obravnavanje nacionalnih tajnih podatkov, izvajanje postopkov varnostnih preverjanj, urejevanje dovoljenj za dostop do nacionalnih, EU in NATO tajnih podatkov, izvajanje

[41] Fizična varnost je pomemben element celotnega sistema varovanja tajnih podatkov. Njen glavni cilj je odvrniti, preprečiti in/ali odkriti nepooblaščene dostope do tajnih podatkov. Fizična varnost je sestavljena iz različnih postopkov in ukrepov varovanja; organizacijskih, varnostno-tehničnih in mehanskih ter postopkov in ukrepov fizičnega varovanja. Industrijska varnost pomeni uporabo varnostnih ukrepov in postopkov za preprečevanje, odkrivanje in povrnitev izgube ali prenehanje ogrožanja tajnih dokumentov, s katerimi razpolaga izvajalec ali podizvajalec med pogajanji pred dodelitvijo in med izvajanjem tajnega naročila oziroma tajnega podnaročila.
[42] Centralni podregister EU in podregister NATO;
[43] Omenila bom samo najpomembnejše.

usposabljanja s področja tajnih podatkov, izvajanje notranjih nadzorov s področja tajnih podatkov in nenazadnje sodelovanje v medresorskih delovnih skupinah.

Poudariti bi želela strinjanje g. Klemenčiča in g. mag. Tarmana, ki sta oba mnenja, da so varnostni standardi v RS bistveno previsoki, s tem da je g. Klemenčič nadaljeval z opozorilom, da so pa pri samem implementiranju nekateri vidiki bili neustrezno ovrednoteni. Predvsem so to vidiki organizacijsko-tehnične narave, kar je vidno v pomanjkanju kadra in sredstev. Uravnavanje s sledečim, bi bil velik doprinos k izvajanju celovitejše zakonodaje na področju varovanja tajnih podatkov, ki se nanaša na vse uslužbence MZZ. Vsak izmed njih je dolžan s svojim odgovornim ravnanjem obravnavati tajne podatke v skladu z zakonom. Sicer g. Klemenčič poudarja, da imajo na MZZ uslužbenci redna usposabljanja s področja tajnih podatkov in možnost pridobitve gradiv ter v skladu s tem ZTP prispeva tudi k višjemu nivoju varnostne kulture v RS.

Podobno se izvaja izpolnjevanje zakonodaje tudi v tujini na DKP[44]. Še pred nastopom dela diplomata, mora posameznik opraviti dodatna usposabljanja s področja tajnih podatkov. Od tam naprej ZTP predvsem pomaga pri implementaciji v obliki depeš, izdelovanju delovodnikov, pri svetovanju nabave rezalcev za uničenje[45] tajnih podatkov, vzpostavitvi varnostnih območij ter izdaja druge notranje akte, s katerimi se ureja obravnavanje tajnih dokumentov. ZTP izvaja tudi nadzore na DKP, skladno in na podlagi Uredbe o notranjih nadzorih ZTP, ki je bila s strani ministra za zunanje zadeve določena s sklepom.

Glede tematike uhajanja tajnih podatkov je g. Klemenčič mnenja, da je še zmeraj najpogostejši politični motiv. Navedel je še, da po ugotovitvah prakse tudi področje gospodarstva ne zaostaja. Sicer g. Klemenčič dodaja, da se z dobrim sistemom varovanja hitreje sanira ali odpravi posledice, ne more pa se preprečiti kršitev. Prav kršitve pa bi morale biti v RS obravnavane preko komisije, ki deluje na nacionalnem varnostnem organu. Po podatkih, ki jih ima g. Klemenčič, namreč v RS še nobena oseba ni izgubila dovoljenja za dostop do tajnih podatkov, oz. ji ni bilo dovoljenje preklicano.

[44] Diplomatska-konzularna predstavništva
[45] Poglej točko 4.2.6. Uničenje nosilcev tajnih podatkov!

Še zmeraj pa je posameznik tisti, pri katerem se »varnost začne in konča, vmes med začetkom in koncem pa je sistem, ki je lahko boljši ali slabši.«[46] Kot ugotavlja g. Klemenčič, sta zanesljivost in lojalnost posameznika organu in tudi državi najpomembnejša faktorja za zavedanje in pojmovanje varnosti ter posledično tudi spoštovanje standardov varovanja tajnih podatkov.

V intervjuju je bilo izraženo tudi opažanje, da drugi sektorji in službe MZZ ne pripisujejo ZTP vrednosti in pomena, saj delovanje te službe prej jemljejo kot nevšečno. Pravi pomen ZTP se priznava le ob težavah in v kritičnih situacijah. Ta ugotovitev je zelo verjeten pokazatelj varnostne kulture v organih javne uprave ki kaže, kakšen je odnos do obravnavanja tajnih podatkov v RS.

Ugotovljeno je tudi bilo, da bi centralizacija obravnavanja tajnih podatkov v smislu enega centralnega registra , enega delovodnika, vhodnih in izhodnih tajnih podatkov (kreiranih in prejetih) in tudi centralni arhiv tajnih podatkov, veliko pripomogli k učinkovitejšemu sistemu varovanja tajnih podatkov v RS. Dvojnost varovanja, kot smo jo zasledili že v primerih javno objavljenih tajnih podatkov, ki je lahko tudi v korist državljanom, bi s tem dobila nek epilog za resnejši pristop. Kot zadnjo ugotovitev bi mogoče še navedla, da zaznave javnega vpliva tega, da je uhajanje tajnih podatkov politično motivirano, zaenkrat še ni in mogoče bomo čez nekaj časa lahko naredili tudi statistiko le tega.

5.3.3 Intervju z novinarjem časopisa Dnevnik

Kot zadnjega bi želela omeniti intervju z g. Rokom Praprotnikom, ki predstavlja kritično javnost v RS. G. Praprotnik je zaposlen kot novinar v časopisni hiši Dnevnik. Intervju z g. Praprotnikom sem opravila predvsem zato, ker se v svojem delu ukvarja skoraj izključno z objavo vsebin člankov o razkritih tajnih podatkih, ki so predmet raziskovanja mojega diplomskega dela.

V začetku g. Praprotnik opozori na dejstvo, da kot novinar gleda na ustreznost normativne ureditve tajnih podatkov drugače, kot bi moral gledati na njo posameznik, ki varuje tajne podatke, kajti, po njegovem mnenju, mu varovanje tajnih podatkov brez ustreznega razloga

[46] Glej prilogo 3, intervju z Gregorjem Klemenčičem!

prepreči dostop do teh podatkov ter s tem tudi prikrajša javnost za pravico do svobode informiranja. Če pa gledamo na ustreznost sistema normativne ureditve z vidika tistih, ki varujejo podatke, pa g. Praprotnik povzema, da je ta ureditev preveč ustrezna, saj omogoča, da se »varujejo« podatki tudi, ko ni razloga za takšno dejanje. Dodaja, da se navkljub uveljavitvi kriterijev po ZTP, le ti še vedno zlorabljajo za neutemeljeno označevanje.

Tudi g. Praprotnik se pridružuje mnenju g. Tarmana in g. Klemenčiča in pravi, da je posameznik najpomembnejši člen v sistemu varovanja tajnih podatkov. Nadaljuje s primerom, da v sistemu, ki funkcionira po točno določenem varovanju prostora[47], ni mogoče, da podatki v fizični obliki zapustijo prostor, vendar je že sam stik posameznikov z informacijami tudi merodajen za varovanje tajnih podatkov. Podobno problematiko sem zasledila v že omenjenem primeru SOVE, kjer ni jasno, kdo in na kakšen način je pregledoval podatke.

Kot ugotavlja g. Praprotnik, je uhajanje tajnih podatkov lahko politično motivirano, navaja pa še druge možne motive, kot so koristoljubje, resnicoljubje in osebno obračunavanje. Po njegovem, uhajanje tajnih podatkov tako ni nujno vezano na predvolilno obdobje, oz. ni jasnih indicev za to, da bi frekvenca takih dogodkov bila v tem času večja.

Pojmovanje varnostne kulture se lahko tudi razdeli na tiste, ki se ukvarjajo z varovanjem tajnih podatkov v državnih organih in na druge osebe, ki dostop do tajnih podatkov pridobijo na osnovi funkcije (funkcionarji, poslanci …). Prvi razpolagajo z visokim nivojem varnostne kulture in ustreznim strokovnim znanjem, pri drugih pa nastane problem glede pristojnosti, ki jih pridobijo že s samo izvolitvijo. Problem je namreč prav pomanjkanje ustrezne usposobljenosti ter takojšen dostop do tajnih podatkov brez preverjanja temveč le z zasedbo funkcije. Kot ugotavlja g. Praprotnik, se varnostna kultura najbolje oblikuje preko izobraževanja in z zavedanjem o odgovornem ravnanju in pomembnosti o nacionalni in posameznikovi varnosti. Z ugotovitvami glede varnostne kulture še nadaljuje in izpostavi pomembno dejstvo, da razkrivanje tajnih podatkov ni nujno del »negativne« varnostne kulture, temveč lahko koristi temu, da je javnost obveščena o morebitnih nepravilnostih in nezakonitostih.

[47]» Primer MORS (monitor brez priključka za USB, brez printerja….)« intervju s Praprotnikom, priloga 3, vprašanje 9.

5.4 PRIMERJAVA POGLEDOV

Če povzamemo in strnemo mnenja intervjuvancev glede navedenih tematik intervjuja lahko ugotovimo naslednje: implementacija ZTP je po njihovem mnenju ustrezna, čeprav prihaja do organizacijskega primanjkljaja (kadri, sredstva) za učinkovito izvajanje. Ugotovili smo tudi, da normativna ureditev odstopa od mednarodnih standardov, vendar ne enostransko, temveč tako v pozitivni smeri, kjer ti standardi višajo nivo varovanja, kot tudi v negativni smeri, kjer naj bi bili ti standardi preveč zahtevni za ustrezno izvajanje v praksi. Vsi intervjuvanci vidijo posameznika in njegovo delovanje kot temelj sistema za varovanje tajnih podatkov. Uhajanje tajnih podatkov iz tega sistema pa po njihovem večinoma izvira iz različnih motivov (gospodarski, politični in osebni), za katerimi se skrivajo politični interesi, vezani na politično dogajanje. Pomen varnostne kulture je tudi bistven faktor pri varovanju tajnih podatkov. Dodatno pa naj bi k temu prispevala še organizacijska kultura znotraj vsakega organa in občutek pripadnosti oz. lojalnosti do državnih institucij. V Tabeli 5.2. sem strnila navedene poglede intervjuvancev glede bistvenih tematik raziskovanja v diplomskem delu.

TABELA 5.2: Primerjava pogledov intervjuvancev

INTERVJUJI/ POGLEDI NA	direktor UVTP	v.d. vodje Službe za tajne podatke MZZ	novinar časnika Dnevnik
MOTIVI ZA RAZKRIVANJE TAJNIH PODATKOV	malomarnost, naklepno delovanje, vojaški, strateški, gospodarski	niso nikoli naključni, politični in gospodarski	gospodarski, politični, osebni in moralni (resnicoljubje)
IMPLEMENTACIJA ZTP	ustrezna in pozitivna	neustrezna[1]	ustrezna[2]
VPLIV POLITIKE IN POLITIČNEGA DOGAJANJA	brez odgovora	uhajanje tudi zaradi političnih interesov, povezava s političnim dogajanjem	uhajanje tudi zaradi političnih interesov, povezava s političnim dogajanjem
VPLIV POSAMEZNIKA	ključni člen pri varovanju tajnih podatkov	posameznik in njegovo pojmovanje varnosti	ključni člen pri varovanju tajnih podatkov
POMEN VARNOSTNE KULTURE	visok, dopolnjuje ga organizacijska kultura	visok, enako pomembna je tudi lojalnost do organa	visok[3]
ODSTOPANJE OD NATO IN EU STANDARDOV	DA[4]	DA[5]	Brez odgovora

[1] Pomanjkanje kadrov in sredstev za ustrezno implementacijo
[2] Po njegovem mnenju pa je ZTP zastavljen tako, da omogoča zlorabe prikrivanja tajnih podatkov.
[3] Varnostna kultura je problematična, kadar politična funkcija omogoča dostop do tajnih podatkov.
[4] V začetni fazi je koristno imeti strožje standarde od minimalnih.
[5] Slovenski standardi so previsoki za implementacijo.

6 ZAKLJUČEK

Varovanje tajnih podatkov je v današnjem času resen izziv tako za posameznika, družbo in državo. Cilji in motivi na področju varovanja pa so lahko različni. Način obravnave in raziskave te tematike, ki sem ga uporabila za pridobivanje relevantnih podatkov, pa je prikazal tudi zanimiva nasprotja varovanja tajnih podatkov.

Uhajanje tajnih podatkov v RS je večinoma politično motivirano in tako sem pri raziskovanju primerov uhajanja tajnih podatkov poskušala upoštevati tudi takrat aktualno politično dogajanje. V vsakem od primerov je bilo zaznati večja politična trenja, kot npr. napetosti med takratnim premierom Janezom Janšo in predsednikom države dr. Janezom Drnovškom, kadrovanje oz. kadrovske menjave na Sovi, verjetni predvolilni pritisk na vlado v primeru Patria itd. Po analizi primerov sem prišla do ugotovitve, da ni samo uhajanje tajnih podatkov politično motivirano, temveč je v nekaterih primerih takšno tudi njihovo označevanje. Še posebej je to motiv za prikrivanje raznih nezakonitosti in nepravilnosti vladajoče pozicije, katere moč za označevanje podatkov izhaja, oz. je podeljena na podlagi njihove funkcije. Moj naslednji sklep bi bil tudi navezava na politično moč vladajoče pozicije, kajti lahko trdimo, da uhajanje tajnih podatkov na nek način pritiska na vladajočo pozicijo in s tem zahteva odgovor in ravnanje, hkrati pa se pozicija z inštitutom tajnosti tudi poskuša pred tem zavarovati. Po navedenem lahko zaključim, da vendarle ni jasnih pokazateljev, da je uhajanje tajnih podatkov v predvolilnem obdobju najpogostejše, bodisi na to posebej vezano. Kot je to omenil sogovornik v intervjuju, bi za to bile potrebne daljnosežne analize. Jasno pa je, da je večina takih dogodkov politično motiviranih in izvira iz političnih napetosti oz. trenj z različnimi ozadji oz. interesi (gospodarski, vojaški in strateški). Poleg tega pa so bili identificirani tudi drugi potencialni motivi za uhajanje tajnih podatkov, kot so koristoljubje, resnicoljubje in osebno obračunavanje.

Varovanje in uhajanje tajnih podatkov obdaja široko področje nejasnosti. Tako v svojem raziskovanju nisem mogla jasno določiti točke pri obravnavanju tajnih podatkov, za katero bi bilo mogoče reči, da omogoča odtujitev tajnih podatkov. Verjetne točke za to so predvsem razmnoževanje, uničevanje nosilcev in način hranjenja tajnih podatkov. Hkrati je popolnoma nejasno, kako ti podatki lahko zapustijo varovana območja brez jasnih zapisov o njihovem premeščanju, dupliciranju itd. S tem je vsakršna identifikacija prenašalcev, pa tudi drugih

akterjev, ki so povezani s tem, praktično nemogoča. Četudi morda do identifikacije pride, je zaradi nejasnosti nemogoč ali pa vsaj javnosti neznan pravni izid takega delovanja. Iz tega lahko sklepamo, da je ena največjih pomanjkljivosti varovanja tajnih podatkov sledljivost dokumentov kot tudi posameznikov, ki prihajajo in odhajajo iz varovanih območij.

Varnostna kultura poglavitno vpliva na učinkovito obravnavanje in varovanje tajnih podatkov. Njena odsotnost oz. nezadostnost vsekakor zmanjšuje to učinkovitost in povečuje možnost uhajanja tajnih podatkov. Nivo varnostne kulture je vsekakor odvisen od organizacijske kulture, lojalnosti, pa tudi osebnega odnosa do pomena tajnosti za državne interese. Primer tega podaja Praprotnik, ko govori o tem da so se javnosti prosto podajali tajni podatki (Anton Rop, vsebina prisluškovanj pogovorov Janša- Sanader). Varnostna kultura se najbolje oblikuje preko izobraževanja, na raznih usposabljanjih, seminarjih itd. Odkrili smo tudi, da v oziru na varnostno kulturo razkrivanje tajnih podatkov ni nujno del negativne varnostne kulture, temveč lahko služi tudi kot informiranje javnosti o zlorabi legitimno pridobljene moči o čemer pričajo navedeni primeri. Lahko smo se prepričali tudi, da je nivo varnostne kulture v organih javne uprave nizek, zaradi tega, ker se tajni podatki in področje varovanja le-teh neustrezno pojmujejo in zaznavajo oz. imajo veljavo le takrat, ko varovanje zataji. Ker so premalo poudarjene posledice za kršitve v skladu z varovanjem tajnih podatkov in posledice uhajanja tajnih podatkov, je posledično tudi nižja raven varnostne kulture. V tem kontekstu bi mogoče bil zelo dobrodošel sistem za vzdrževanje in preverjanje varnostne kulture ter percepcije varovanja tajnih podatkov, ki bi nadgrajeval tako varnostno kulturo kot tudi učinkovitost varovanja tajnih podatkov.

Tako osveščen posameznik je namreč temelj za učinkovito obravnavo in varovanje tajnih podatkov. Predstavlja ključni člen stabilnosti tega sistema, saj je od njegovega odnosa, usposobljenosti in moralnosti v veliki meri odvisno ali bo sistem deloval ali ne. Kot smo lahko zasledili ima tudi posameznik velik pomen in avtonomijo v sistemu, saj odloča o tem, ali tajni podatek označiti s stopnjo tajnosti ali ne. Posledica tega je dopuščanje uhajanja zaradi neurejenosti zakonodajnih standardov pa tudi kriterijev. Kot rečeno pa ga pri tej izrabi sistema vodijo številni motivi. Za stabilno delovanje sistema za varovanje pa bi bil potreben neodvisen in večstopenjski nadzor. Napredek pri nadzoru kot tudi pri izboljšanju sledljivosti bi lahko dosegli z uporabo sodobnih in prihajajočih informacijskih tehnologij, na katere pa se trenutno sistem varovanja premalo zanaša, npr. pregledovanje z biometrijo.

Na področju varovanja tajnih podatkov je v prihodnje potrebno vzpodbuditi boljše sistemsko organizirano delovanje s ciljem večje centralizacije in racionalizacije, ki bo imela za posledico večji napredek in boljšo povezavo med posamezniki, organi in institucijami ter večjo varnost tajnih podatkov. Enakovredna vzpostavitev vseh delov sistema varovanja tajnih podatkov v vseh državnih organih, vztrajno posodabljanje, načrtno usposabljanje ter jasna sledljivost so ključ za uspešno in učinkovito delovanje sistema varovanja tajnih podatkih na nacionalni ravni.

7 LITERATURA

1. Almond, Gabriel A. in Sidney Verba. 1963. *The civic culture: political attitudes and democracy in five nations.* Princeton: Princeton University press.
2. *Amsterdamska pogodba*. Dostopno prek: http://evropa.gov.si/pravni-red/pogodbe/ (22. november 2008).
3. Anžič, Andrej. 1996. *Vloga varnostnih služb v sodobnih parlamentarnih sistemih-nadzorstvo*. Ljubljana: Enotnost.
4. --- 1997. *Varnostni sistem Republike Slovenije*. Ljubljana:Uradni list RS.
5. --- 2000. Tajnost: vrednota in zlo. *Teorija in praksa* 37(5): 849- 863.
6. Anžič, Andrej in Franc Trbovšek. 2003. Varnostno preverjanje v NATO po novih standardih: (povzetek). V *Dnevi varstvoslovja / (Četrti Slovenski dnevi varstvoslovja, Bled, 5. do 7. junij 2003),* ur. Milan Pagon in Iztok Podbregar, 118-128. Ljubljana: Visoka policijsko-varnostna šola.
7. Bernhard, Vesna R. 2008. Afera uhajanje dokumentov z MZZ: Diplomatsko depešo je lahko bralo več sto zaposlenih na MZZ. *Dnevnik*, 13. februar. Dostopno prek: http://www.dnevnik.si/novice/slovenija/298502 (15. december 2008).
8. Bohinc, Rado. 2001. Uvodni nagovor. V *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih*, ur. Igor Belič, 5-8. Ljubljana: Ministrstvo za notranje zadeve RS.?
9. Bohinc, Rado in Rajko Pirnat. 2005. *Osebe javnega prava : javni zavodi, javna podjetja, javne agencije, javni skladi.* Ljubljana: GV Založba.
10. Brezovšek, Marjan in Damir Črnčec. 2007. *Demokratična uprava in tajnost podatkov*. Ljubljana:Fakulteta za družbene vede.
11. Bučar, Bojko, Zlatko Šabič, Milan Brglez in Monika Kalin-Golob, ur. 2002. *Navodila za pisanje: seminarske naloge in diplomska dela*. Ljubljana: Fakulteta za družbene vede.
12. Bukovec, Tomaž. 2007. Storilci, ki to sploh niso bili. *Dnevnik*, 5.junij. Dostopno prek: http://www.dnevnik.si/tiskane_izdaje/nedeljski/249813 (30. november 2008).
13. Buzan, Barry. 1991. *People, states and fear: an agenda for international security studies in the post-cold war era.* New York: Harvester Weatsheaf.
14. Buzan, Barry, Ole Waever in Jaap de Wilde. 1998. *Security: a new framework for analysis.* Boulder, London: Lynne Rienner.

15. Caharijas, Domen. 2007. Sovi puščajo kri po kapljicah. *Dnevnik*, 26. maj. Dostopno prek: http://www.dnevnik.si/tiskane_izdaje/objektiv/247757 (25. november 2008).
16. Čaleta, Denis. 2003. *Trend razvoja slovensko obveščevalno-varnostne skupnosti po vstopu v EU in NATO*. 4. Slovenski dnevi varstvoslovja. Ljubljana: Visoka policijsko varnostna šola.
17. --- 2004. Konceptualne spremembe na področju varovanja tajnih podatkov v Republiki Sloveniji. V *Zbornik prispevkov [Elektronski vir] / Dnevi varstvoslovja / (5. slovenski dnevi varstvoslovja, Bled, 3.-5. junij 2004),* ur. Branko Lobnikar, 48-57. Ljubljana: Fakulteta za policijsko- varnostne vede.
18. Černetič, Metod in Liliana Brožič. 2003. Potrebe po novih znanjih- varovanje tajnih podatkov v Evropski uniji in zvezi NATO. *Organizacija* 36 (8): 575-582.
19. Črnčec, Damir. 2003. *Tajnost podatkov: varnostno preverjanje in obveščevalno-varnostne službe: magistrsko delo*. Ljubljana: Fakulteta za družbene vede.
20. *Declaration of Western European Union on role of Western European Union and its relations with European Union and with the Atlantic Allienc* (22. julij 1997). Dostopno prek: http://www.weu.int/documents/970722en.pdf (20. november 2008).
21. *Declaration on enhanced cooperation between the European Union and the Western European Union (*22.julij 1997). Dostopno prek: http://eurlex.europa.eu/sl/treaties/dat/11997E/htm/11997E.html#0125020019 (20. november 2008).
22. *Deklaracija o zunanji politiki Republike Slovenije*. Ur. l. RS 108/1999 (27. december 1999).
23. (ds), (STA, pn). 2008. Beograjska Politika se odziva na izjave o objavi dokumentov. *Dnevnik,* 21. januar. Dostopno prek: http://www.dnevnik.si/novice/eu/295197/ (10. december 2008).
24. Dvoršak, Andrej in Bojan Radulj. 2005. Katalogizacija in klasifikacija: prikaz sistematičnega urejanja podatkovnih zbirk-evidenc na podlagi uveljavljenih standardov, ki omogočajo kompatibilnost in izmenljivost podatkov. V *Zbornik prispevkov [Elektronski vir] / 6. slovenski dnevi varstvoslovja, Bled, 2.-4. junij 2005*, ur. Branko Lobnikar, 1-16. Ljubljana: Fakulteta za policijsko-varnostne vede.
25. Grizold, Anton, ur. 1998. *Perspektive sodobne varnosti: Iz obramboslovnih raziskav II.* Ljubljana: Fakulteta za družbene vede.
26. --- 1999. *Evropska varnost.* Ljubljana: Fakulteta za družbene vede.

27. Grizold, Anton, Ljubica Jelušič in Tomo Korošec, ur. 1991. *Demilitarizacija Slovenije in nacionalna varnost: zbornik*. Ljubljana: Znanstveno in publicistično središče.
28. Hartman, Ervin. 2007. *Varovanje tajnih podatkov in varnostna kultura na obrambnem področju : protiobveščevalno-varnostni vidik: specialistično delo*. Ljubljana: Fakulteta za družbene vede.
29. Jazbec, Milan. 2002. *Diplomacija in varnost: razvoj in približevanje procesov*. Ljubljana: Vitrum.
30. Južnič, Stane. 1989. *Politična kultura*. Maribor: Obzorja.
31. Kavčič, Bogdan. 1991. *Sodobna teorija organizacije*. Ljubljana: Državna založba Slovenije.
32. Klemenčič, Gregor. 2009. Intervju z avtorjem. Ljubljana, 5. januar.
33. Kline, Miro, Marko Polič in Vlasta Zabukovec. 1998. *Javnost in nesreče: obveščanje, opozarjanje, vplivanje.* Ljubljana: Znanstveni institut Filozofske fakultete.
34. K. N. S. in M. E. 2000. Nova afera na obrambnem ministrstvu. *24ur*, 14. junij. Dostopno prek: http://24ur.com/novice/slovenija/nova-afera-na-obrambnem-ministrstvu.html (30. november 2008).
35. Kolenc, Janez. 1993. *Politična kultura Slovencev: raziskovanje odnosa med civilno družbo in državo.* Ljubljana: Karantanija.
36. Korošec, Sabina. 2006. *Varnostno preverjanje v Republiki Sloveniji: Diplomsko delo.* Ljubljana: Fakulteta za družbene vede.
37. Kozlevčar, Marjan. 2007. *Organizacijske in administrativne ovire pri delu s tajnimi podatk: magistrsko delo.* Univerza v Ljubljani: Fakulteta za upravo.
38. *Kronologija pristopnih pogajanja zveze NATO.* Dostopno prek: http://nato.gov.si/slo/slovenija-nato/kronologija/ (20. november 2008).
39. Lukšič, Igor. 2006. *Politična kultura: političnost morale*. Ljubljana: Fakulteta za družbene vede.
40. *Markle Foundation, Adressing Critical Public Needs for Help and National Security in the Information Age.* Dostopno prek: http://www.markle.org/ (10. oktober 2008).
41. Mekina, Igor in Meta Roglič. 2008. MZZ bo zaradi objave internega dokumenta sprožilo interno preiskavo in poostrilo varnost. *Dnevnik*, 25. januar. Dostopno prek: http://www.dnevnik.si/novice/eu/294858 (10. december 2008).
42. Mitar, Miran. 2008. *Primerjava izbranih pristopov za ocenjevanje varnosti sodobne družbe.* Ljubljana: Fakulteta za varnostne vede.

43. *Nato Security Committtee, Directive on Personal Security*. Document AC/35-D/2000, North Atlantic Council.
44. *Navodilo za izvajanje posebnih ukrepov za varovanje dokumentov in drugih zapisov, ki so določeni kot obramba- državna skrivnost oziroma vojaška ali uradna skrivnost s stopnjo »strogo zaupno« (NIPUUD)*. Ur. l. RS 38/1993 (25. julij 1993).
45. *Odlok o varnostnih ukrepih (OVUOP*). Ur. l. RS 49/1992 (25. oktober 1992).
46. Praprotnik, Rok. 2007. Dolgi politični prsti v bazah najbolj zaupnih podatkov. *Dnevnik,* 21. marec. Dostopno prek: http://www.dnevnik.si/novice/aktualne_zgodbe/235581 (30. november 2008).
47. --- 2007. Afera SOVA: Janševi ljudje so bili tajno v SOVI okoli 35 ur. *Dnevnik*, 27. marec. Dostopno prek: http://www.dnevnik.si/novice/slovenija/236576 (30. november 2008).
48. --- 2007. Vrh Sove se je otresel politike. *Dnevnik*, 18. december. Dostopno prek: http://www.dnevnik.si/novice/slovenija/287860 (21. december 2008).
49. --- 2008. Obletnica Dnevnikovega razkritja: Po letu dni afera Sova še vedno brez epiloga. *Dnevnik*, 21. marec. Dostopno prek: http://www.dnevnik.si/novice/slovenija/306840/ (30. november 2008).
50. Praprotnik, Rok. 2008. Intervju z avtorjem. Ljubljana, 9. december.
51. Prezelj, Iztok, ur. 2007. *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*. Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.
52. *Resolucija o strategiji nacionalne varnosti Republike Slovenije*. Ur. l. RS 56/2001 (06. julij 2001).
53. Rovšek, Jernej. 2001. Dostopnost informacij javnega značaja in dopustnost omejitev z vidika ustave in varstva človekovih pravic. V *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih,* ur. Igor Belič, 35-42. Ljubljana: Ministrstvo za notranje zadeve RS. ?
54. *Security Whithin the Nort Atlantic Treaty Organiastion (NATO.* Document C-M (2002) 49.
55. *Security Regulations of the Council of the European Union.* (2001/264/EC), L 101 (19. marec 2001). Sklep sveta EU z dne 19.03.2001 o sprejetju predpisov Sveta Skupnosti o varovanju tajnosti.
56. *Sklepu o ustanovitvi, nalogah in organizaciji Urada RS za varovanja tajnih podatkov*. Ur. l. RS 6/2002 (25. januar 2002).

57. Splichal, Slavko in France Vreg. 1986. *Množično komuniciranje in razvoj demokracije*. Ljubljana: Komunist.
58. Splichal, Slavko. 1997. *Javno mnenje: teoretski razvoj in spori v XX. stoletju*. Ljubljana: Fakulteta za družbene vede.
59. Škerlep, Andrej. 2002. Javnost, javno mnenje in diskurzivna racionalnost. *Družboslovne razprave* 18 (41): 153-169.
60. Štamcar, Miha. 2000. Odkar je zavladala Bajukova vlada, je Slovenija postala država afer. *Mladina*, 35. Dostopno prek: http://www.mladina.si/tednik/200035/clanek/afere/ (30. november 2008).
61. Tarman, Milan. 2008. Intervju z avtorjem. Ljubljana, 5. december.
62. *TV Slovenija, Studio City. 2008. Kučan: Imamo tradicijo uhajanja tajnih podatkov.* Dostopno prek: http://www.rtvslo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=1&c_id=163780 (10. december 2008).
63. *Uredba o upravnem poslovanju.* Ur. l. RS 20/2005 (4. marec 2005).
64. *Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov*. Ur. l. RS 71/2006 (7. julij 2006) in Ur. l. RS 138/2006 (28. december 2006).
65. *Uredba o varovanju tajnih podatkov.* Ur.l. RS 74/2005- UPB (20. avgust 2005).
66. *Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih*. Ur. l. RS 48/2007 (1. junij 2007).
67. Uredništvo Mladine. 2008. Za Kučana ključno, ali so v afero Patria vmešane tudi državne institucije. *Mladina,* 3. september. Dostopno prek: http://www.mladina.si/dnevnik/03-09-2008-za_kucana_kljucno__ali_so_v_afero_patria_vmesane_tudi_drzavne_institucije/ (17. december 2008).
68. *Ustava Republike Slovenije (URS).* Ur.l. RS/I 33/1991. (23.12.2991). Objavljena dne 28.12. 1991, začela veljati 23. decembra 1991, z dnem razglasitve.
69. *Varnostni sporazum med Vlado Republike Slovenije in Vlado ZDA glede varnostnih ukrepov pri varovanju zaupnih vojaških podatkov.* Ur. l. RS 57/1996, Mednarodne pogodbe 15/1996 (8. maj 1996).
70. Vršec, Milan 2003. Ocena ogroženosti in varnostnih tveganj kot ena od ključnih podlag za varnostno politiko in varnostni sistem. V *Dnevi varstvoslovja (Elektronski vir) / (Četrti Slovenski dnevi varstvoslovja, Bled, 5. do 7. junij 2003),* ur. Milan Pagon in Iztok Podbregar, 21. Ljubljana: Visoka policijsko-varnostna šola.

71. *Zakon o dostopu do informacij javnega značaja (ZDIJZ)*. Ur.l. RS 24/2003 (22. marec 2003).
72. *Zakon o obrambi in zaščiti (ZOZ)*. Ur.l. RS 15/1991 in 18/1991 popravek. (14. april 1991).
73. *Zakon o ratifikaciji Varnostnega sporazuma med Republiko Slovenijo in Organizacijo Severnoatlantskega pakta* (MVSOSP*)*. Ur. l. RS 23/1997 (13. julij 1994).
74. *Zakon o ratifikaciji Varnostnega sporazuma med Vlado Republike Slovenije in Zahodnoevropsko unijo* (MVSZU). Ur. l. RS št. 20/1999 (24. julij 1998).
75. *Zakon o tajnih podatkih (ZTP)*. Ur. l. RS 50/2006- UPB2 (16. maj 2006).
76. Zgaga, Blaž. 2008. O Patria, ti si kakor zdravje! *Mladina*, 8. avgust. Dostopno prek: http://www.mladina.si/dnevnik/08-08-2008-o_patria__ti_si_kakor_zdravje_/ (17. december 2008).
77. Žirovnik, Janez. 2005. Dostop do tajnih podatkov v zvezi NATO in EU ter v izbranih tujih zakonodajah. V *Zbornik prispevkov* [Elektronski vir] / 6. slovenski dnevi varstvoslovja, Bled, 2.-4. junij, ur. Branko Lobnikar, 1-15. Ljubljana: Fakulteta za policijsko-varnostne vede.
78. Žurga, Gordana. 2001. *Kakovost državne uprave: pristopi in rešitve*. Ljubljana: Fakulteta za družbene vede.
79. --- 2004. *Projektni menedžment kot del menedžmenta v javni upravi*. Ljubljana: Fakulteta za družbene vede.

8 Seznam prilog

Priloga A: Intervju z g. mag. Milanom Tarmanom
Priloga B: Intervju z g. Gregorjem Klemenčičem
Priloga C: Intervju z g. Rokom Praprotnikom
Priloga Č: Zgoščenka z zvočnim zapisom intervjujev z g. Gregorjem Klemenčičem in g. Rokom Praprotnikom (WAV datoteke)[48]:

1. datoteka – INTERVJU1.wav (intervju z g. Gregorjem Klemenčičem)
2. datoteka – INTERVJU2.wav (intervju z g. Rokom Praprotnikom)

[48] G. mag. Milan Tarman se za zvočno snemanje intervjuja ni odločil.

Priloga A: Intervju z g. mag. Milanom Tarmanom!

Ljubljana, UVTP; 05.12.2008

1. ***Lahko na kratko predstavite zgodovino UVTP?***

Od l. 2002; 43. člen zakona pravi: Izvajanje ZTP in drugih predpisov, sprejetih na njegovi podlagi ter mednarodnih pogodb, ki jih je sklenila RS, spremlja in usklajuje nacionalni varnostni organ, razen če mednarodna pogodba ne določa drugače. Naloge nacionalnega varnostnega organa opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov;Uradni list RS, št. 6/2002 z dne 25.01.2002;
S tem sklepom se ustanovi Urad Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljnjem besedilu: Urad) in se v skladu z zakonom določijo strokovne naloge Urada in njegova organizacija.

2. ***Na katerih področjih UVTP opravlja dela in naloge?***

V skladu z organizacijo in sistemizacijo se naloge UVTP izvajajo v skladu z določili Zakona o tajnih podatkih (Uradni list RS, št. 50/06-prečiščeno besedilo), v nadaljevanju: ZTP) in njegovih podzakonskih aktov ter v skladu z določili Sklepa o ustanovitvi, nalogah in organizaciji UVTP (Uradni list RS, št. 6/02).

UVTP:

- spremlja in usklajuje stanje na področju obravnavanja in varovanja tajnih podatkov,
- predlaga ukrepe za izboljšanje varovanja tajnih podatkov, skrbi za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja tajnih podatkov v organih in organizacijah,
- koordinira delovanje organov, pristojnih za varnostno preverjanje,
- pripravlja predloge predpisov s področja tajnih podatkov za vlado,
- daje mnenja o skladnosti splošnih aktov organov in organizacij z ZTP na področju obravnavanja in varovanja tajnih podatkov in

- opravlja druge naloge, določene z ZTP in s predpisi, sprejetimi na njegovi podlagi.

UVTP na področju mednarodne dejavnosti:

- skrbi za izvrševanje mednarodnih pogodb in sprejetih mednarodnih obveznosti, ki jih je v zvezi z obravnavanjem in varovanjem tajnih podatkov sklenila ali sprejela Republika Slovenija,
- na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij ter
- usklajuje dejavnosti za zagotavljanje varnosti nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov na območju Republike Slovenije.

UVTP za namene izvrševanja pristojnosti in nalog po ZTP, drugih predpisih in obvezujočih mednarodnih pogodbah vodi in obdeluje naslednje evidence:

- dovoljenja za dostop do tajnih podatkov,
- dovoljenja fizičnim osebam za dostop do tujih tajnih podatkov,
- izdana varnostna dovoljenja organizacijam,
- izdana varnostna dovoljenja organizacijam za dostop do tujih tajnih podatkov,
- začasni dostopi do tajnih podatkov.

UVTP v zvezi z izvrševanjem mednarodnih pogodb in sprejetih mednarodnih obveznosti opravlja zlasti naslednje naloge:

- izdaja in preklicuje dovoljenja fizičnim osebam za dostop do tujih tajnih podatkov,
- izdaja in preklicuje varnostna dovoljenja organizacijam za dostop do tujih tajnih podatkov,
- izdaja in preklicuje varnostna dovoljenja za sisteme in naprave za prenos, hranjenje in obdelavo tujih tajnih podatkov v skladu s sprejetimi mednarodnimi pogodbami,
- potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa ali organizacije tujim državam in mednarodnim organizacijam,
- izdaja navodila za ravnanje s tajnimi podatki tuje države ali mednarodne organizacije,
- nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države ali mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni nemudoma izvršiti,

- od pristojnega inšpektorata zahteva izvedbo inšpekcijskega nadzora pri določenem organu ali organizaciji in
- izmenjuje podatke z nacionalnimi varnostnimi organi tujih držav in z mednarodnimi organizacijami.

Temeljni procesi v UVTP so medsebojno povezane aktivnosti, ki zagotavljajo izvajanje nalog UVTP z naslednjimi cilji:

- strokovno, učinkovito in racionalno izvajanje nalog, ki so opredeljene v aktu o organizaciji in sistemizaciji ter
- realizacija vsakoletnega programa dela v obdobju l. 2004-2008.

Pri uresničevanju letnih programov UVTP v obdobju 2004 – 2008 velja kot ključne izpostaviti naslednje dosežke, in sicer, da smo:

- okrepili medresorsko sodelovanje z intenziviranjem dela medresorskih delovnih skupin ter okrepili bilateralno in multilateralno sodelovanje s pristojnimi organi drugih držav na področju varovanja tajnih podatkov,
- pripravili vsa načrtovana gradiva s področja dela in jih uspešno predstavili na Odboru za državno ureditev in javne zadeve Vladi Republike Slovenije ter za potrebe bilateralnih sporazumov na Odboru za zunanjo politiko Državnega zbora,
- uspešno predstavljali urad kot »National Security Authority« Republike Slovenije v delovnih telesih Evropske unije, Evropske komisije in zveze NATO.

V okviru UVTP delujejo naslednje komisije, ki jih vodijo oziroma koordinirajo njihovo delo uslužbenci UVTP:

- komisija za presojanje upravičenosti prevladujočega javnega interesa v zvezi z razkritjem podatkov, ki so določeni kot tajni (21.a člen Zakona o tajnih podatkih),
- komisija za informacijsko varnost, (15. člen Uredbe varovanju tajnih podatkov v komunikacijskih in informacijskih sistemih),
- medresorska komisija za industrijsko varnost,
- medresorska projektna skupina za oblikovanje šablonskih rešitev v registrih in podregistrih tajnih podatkov,
- delovna skupina organov, pristojnih za varnostno preverjanje.

3. ***S sprejetjem Zakona o tajnih podatkih je bil uzakonjen enotni sistem določanja, dostopanja, varovanja in prenehanja tajnih podatkov. S tem se je RS pridružila državam, ki imajo področje varovanja tajnih podatkov urejeno po mednarodnih standardih. Ali so bili ti standardi ustrezno implementirani v RS?***

Da.
Urad Vlade za varovanje tajnih podatkov je normativno ustrezno uredil področje varovanja tajnih podatkov. Sprejeti so:

Zakon o tajnih podatkih (Ur. l. RS, št. 50/06, UPB2),
Uredba o varovanju tajnih podatkov (Ur. l. RS, št. 74/05),
Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji (Ur. l. RS, št. 70/07),
Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS, št. 48/07),
Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Ur. l. RS, št. 71/06),
Uredba o spremembah Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Ur. l. RS, št. 138/06),
Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja (Ur. l. RS, št. 94/06),
Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Ur. l. RS, št. 94/06),
Uredba o obliki in uporabi znaka Urada Vlade RS za varovanje tajnih podatkov (Ur. l. RS, št. 1/08).

UVTP ima sprejete vse akte, ki urejajo področje varovanja tajnih podatkov. Za potrebe implementacije predpisov bomo glede na potrebe prakse kot rezultate medresorskega dela izdajali ustrezna navodila.

Trenutno pripravljamo bilateralne Sporazume o izmenjavi tajnih podatkov, katerih trenutno stanje je opisano v točki 16. oz. v prilogi št. 5. – Poročilo o mednarodni dejavnosti.

4. ***Kako bi komentirali kritiko, da na nekaterih področjih preveč odstopamo od minimalnih standardov varnostne politike NATA in sklepa sveta EU?***

Ne bi rekel, da preveč odstopamo in tudi glede na mednarodne izkušnje je v začetni fazi vzpostavljanja sistema obravnave in varovanja tajnih podatkov celo koristno imeti nekoliko strožje standarde.

Je pa res, da z več prakse prihaja do potrebe po reviziji določenega dela predpisov v tem smislu, kar na podlagi pobud v medresorskem delu proučujemo in bomo na podlagi teh dogovorov in usklajevanj (ter z upoštevanjem »dobrih praks« dolgoletnih članic NATO in EU) poslali v predpisano proceduro določene amandmaje.

Držimo se načela botom-up, se pravi, višje ko gremo, bolj tresoča mora biti roka. Zagovarjamo dejstvo, da višji ko so standardi, boljša je zaščita.

5. ***Na kakšen način sodelujete z drugimi državnimi in vladnimi službami? In kakšen pomen Vam pripisujejo? Se vam zdi, da se obrnejo na Vas za nasvete, navodila…?***

Sodelovanje je na zelo visokem nivoju. Seveda pa ena naših ključnih nalog ostaja še nadaljnje spodbujanje in promocije varnostne kulture v vseh organih in organizacijah, ki se s tajnimi podatki srečujejo.

Kot primer lahko navedem tudi letošnji uspešno izveden projekt poziva glede sprejemnih točk in odgovornih oseb za prejem tajnih podatkov. Dopis z naslovom Tajni podatki – sprejemna točka in osebe št. 02230-5/2008/1 je bil dne 23. 4. 2008 poslan na naslov vseh organov (ministrstva, vladne službe, organi v sestavi, upravne enote, občine, pravosodni organi: sodišča, tožilstva) ter tistih organizacij, ki imajo izdano varnostno potrdilo. Urad Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljevanju UVTP) je prejel 246 odgovorov. Dopisu so se najbolj številčno odzvale upravne enote, in sicer 93%, najmanj številčno pa občine, in sicer 28%.

Veliko naslovnikov je ob pošiljanju podatkov tudi zaprosilo za našo strokovno pomoč pri urejanju upravnega ali varnostnega območja oz. za dodatna pojasnila Sklepa o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja.

Nadalje še lahko omenim srečanja strokovnjakov na mesečnih sestankih in ad hoc skupine, katere veliko pripomorejo k povečanju pomena urada na področju varovanja tajnih podatkov.

USMERJENOST K UPORABNIKU, ODPRTOST ZA POMOČ IN NASVETE. Tajnih podatkov se ni treba bati, treba jih je le ustrezno obravnavati in varovati!

6. ***Ali se varovanje tajnih podatkov v praksi in normativna ureditev varovanja le-teh v RS razlikujeta? Če se, kje je to najbolj vidno in s kakšnimi težavami se soočate v skladu s tem?***

Dolžni smo slediti veljavni normativni ureditvi in v okviru naših pristojnosti napotujemo na to tudi ostale. Praksa je v določenih primerih že pokazala potrebo po bolj pragmatični ureditvi normativne ureditve v smislu približevanju minimalnim standardom varnostne politike NATA in sklepa sveta EU. Vidno predvsem na področju fizične in industrijske varnosti. Kot že omenjeno, na podlagi pobud v medresorskem delu navedeno proučujemo in bomo na podlagi teh dogovorov in usklajevanj (ter z upoštevanjem »dobrih praks« dolgoletnih članic NATO in EU) poslali v predpisano proceduro določene amandmaje.

7. ***Po pregledu predpisov, ki veljajo na področju varovanja tajnih podatkov lahko ugotovimo, da varnost še vedno sloni na posamezniku kot ključnem členu v sistemu varovanja tajnih podatkov. Prosim za komentar.***

Se strinjam. Prav zato je ozaveščanje in krepitev varnostne kulture tako pomembno. Vlogo UVTP pa vidim prav tem smislu in v smislu, da smo odprti kot urad in kadarkoli na voljo za nasvete.
Projekt »usposabljanje usposobljevalcev« (poleg rednih usposabljanj) po ministrstvih – npr. CIP - pravosodje tekoči projekt.
Tudi primeri iz tujine (npr. VB, Estonija) kažejo, da je pri varovanju tako občutljivih kot tajnih podatkov ključen »človeški faktor«.

8. ***Kakšni so po Vaše najpogostejši razlogi, zaradi katerih prihaja do uhajanja tajnih podatkov? So to splet naključnih okoliščin, nezadosten varnostni sistem, zavestno ali nesrečno oz. nerodno delovanje posameznikov? In nadalje, kaj mislite na katerih področjih in kakšne vrste podatki so najbolj zaželeni?***

Različni: od malomarnosti do naklepa. Največkrat človeški faktor.
Vojaški – NATO, strateški EU, gospodarski interesi, sicer odvisno od države in tudi od njene geostrateške lege.

9. ***Na kakšen način po Vašem mnenju UVTP prispeva k višjemu nivoju varnostne kulture v RS?***

Že nekaj primerov je bilo navedenih tekom intervjuja; sicer pa usposabljanje ter tesno sodelovanje z vsemi v državi (tudi univerzami oz. fakultetami) in prenos usmeritev, novosti, prakse ter izkušenj NATO, EU, multi. in bilaterala. Tudi na način ustvarjanja socialnega kapitala med državami.

MEDNARODNI ANGAŽMA UVTP -. krepitev zaupanja, pomembnosti ustreznega obravnavanja in varovanja TP tudi v RS.

10. ***A menite, da so odnosi med zaposlenimi, nadrejenimi in podrejenimi, občutek pripadnosti organizaciji in lojalnost pomembni faktorji, ki prispevajo k (ne)uhajanju tajnih podatkov oz. čim manjšemu uhajanju?***

Vsekakor. Pomemben visok nivo organizacijske kulture in klime v organu ali organizaciji!

Tudi tisti, ki mu to ne predstavlja vsakodnevnega dela, mora v primeru, ko se sreča s tajnimi podatki le-tega obravnavati in varovati na ustrezen način – če je kakšen pomislek ali dvom glede tega, pa se še vedno lahko k nam obrne po nasvet.

Sicer pa posvečanje pozornosti tudi z ravni predstojnikov, krepitev odgovornosti in nenazadnje opozarjanje na posledice.

NSA kot varnostni organ ima inšpekcijsko vlogo, UVTP pa je posvetovalni in svetovalni organ.

Priloga B: Intervju z g. Gregorjem Klemenčičem!

Ljubljana, MZZ; 05.01.2009;

1. ***Lahko, prosim, predstavite glavne naloge Službe za tajne podatke, na Ministrstvu za zunanje zadeve?***

Glavne naloge naše službe so: vodenje centralnega podregistra EU in podregistra NATO tajnih podatkov v skladu z varnostno politiko EU in NATO ter obravnavanje nacionalnih tajnih podatkov; pod obravnavanje sodi distribucija, signiranje, hranjenje, uničevanje, arhiviranje, evidentiranje, kopiranje in sledenje. Izvajanje postopkov varnostnih preverjanj, urejevanje dovoljenj za dostop do nacionalnih, EU in NATO tajnih podatkov, izvajanje usposabljanja s področja tajnih podatkov, izvajanje notranjih nadzorov s področja tajnih podatkov, prilagajanje organizacijsko-tehničnih postopkov v našem ministrstvu skladno z nacionalno, EU in NATO zakonodajo. Sodelujemo v medresorskih delovnih skupinah. To bi bila groba predstavitev naših nalog.

2. ***S sprejetjem Zakona o tajnih podatkih je bil uzakonjen enotni sistem določanja, dostopanja, varovanja in prenehanja tajnih podatkov. S tem se je RS pridružila državam, ki imajo področje varovanja tajnih podatkov urejeno po mednarodnih standardih. Ali so biti ti standardi ustrezno implementirani v RS?***

Osebno menim, da ne. Predvsem so bile v postopku vzpostavljanja zakonodaje, organizacijsko-tehnične zadeve neustrezno ovrednotene. Ocenjujem, da bi bilo za celovito izpolnjevanje zakonodaje potrebno v MZZ bistveno več kadra in sredstev, kar pa si država naše velikosti ne more privoščiti, zato bi bilo nujno kar nekaj nepotrebnih zakonskih določil poenostaviti.

3. ***Kako bi komentirali kritiko, da na nekaterih področjih preveč odstopamo od minimalnih standardov varnostne politike NATA in Sklepa Sveta EU?***

Tej kritiki se pridružujem, saj so standardi v RS bistveno previsoki in tako nikoli ne bodo in niso bili implementirani v nacionalni sistem tajnih podatkov.

4. ***Na kakšen način sodelujete s sektorji in službami znotraj MZZ-ja? In kakšen pomen Vam pripisujejo? Se vam zdi, da se obrnejo na Vas za nasvete, navodila…?***

V času vodenja Službe za tajne podatke opažam, da se je vpliv povečal, ne glede na to pa še vedno precejšen del našega ministrstva meni, da smo služba v smislu »nebodigatreba«. Kadar pa pride do težav ali do inšpekcijskih nadzorov, takrat pa služba vedno odigra svojo vlogo in upraviči svoj namen.

5. ***Kako je z implementacijo ZTP na veleposlaništvih RS? Na kakšen način se izvaja nadzor in kdo ga izvaja?***

Vsak uslužbenec je podvržen izpolnjevanju zakonodaje. ZTP pomaga pri implementaciji s tem, da daje DKP navodila v obliki depeš, izdeluje za njih delovodnike, svetuje pri nabavi rezalcev, vzpostavitvi varnostnih območij ter izdaja druge notranje akte, s katerimi se urejuje obravnavanje dokumentov.
Nadzor se je začel izvajati s strani ZTP v letu 2008, ko so bili vzpostavljeni vsi ustrezni pogoji, da se je nadzor lahko pričel. V letu 2009 imamo predvidenih več nadzorov, vsaj enega mesečno. Nadzore izvajamo skladno in na podlagi Uredbe o notranjih nadzorih ZTP, ki je bila s strani ministra za zunanje zadeve določana s sklepom.

6. ***Ali se varovanje tajnih podatkov v praksi in normativna ureditev varovanja na MZZ-ju razlikujeta? Če se kje je to najbolj vidno in s kakšnimi težavami se soočate v skladu s tem?***

Normativna ureditev varovanja tajnih podatkov na MZZ bi pomenila v teoriji, da bi se tako varovanje kot obravnavanje tajnih podatkov uredilo na način, da bi bil vzpostavljen en centralni register za tajne podatke, s tem tudi en delovodnik tajnih podatkov, vhodnih in izhodih (kreiranih in prejetih) tajnih podatkov in tudi centralni arhiv le-teh, se pravi, da bi bili vsi podatki na enem mestu. Finančno kadrovsko in organizacijsko to zaenkrat ni izvedljivo. Veliko zahtev in določb, ki jih zahteva zakonodaja lahko rešimo na en način. npr. z uvedbo centralnega delovodnika tajnih podatkov ne rešimo samo to, da bo enotna preglednost, ampak bo tudi istočasno zagotavljanje sledljivosti, potem uničevanja teh podatkov, arhiviranja, obravnavanja; se pravi, da imamo nek centralni nadzor teh podatkov; kadar pa je to prepuščeno službam in vsaka služba obravnava svoj del tajnih podatkov, takrat pa so ti

podatki podvrženi večjim zakonodajnim nepravilnostim. Kajti če bi se to obravnavalo centralno in bi za to skrbela služba, ki je usposobljena za delo s takimi podatki, bi kršitve lahko s tem eliminirali in jih sploh ne bi bilo.

7. ***Po pregledu predpisov, ki veljajo na področju varovanja tajnih podatkov lahko ugotovimo, da varnost še vedno sloni na posamezniku kot ključnem členu v sistemu varovanja tajnih podatkov. Prosim za komentar.***

Absolutno se strinjam, da se varnost začne in tudi konča pri posamezniku, vmes med začetkom in koncem imamo pa vedno nek sistem, ki pa je lahko boljši ali slabši. Vseeno ocenjujem, da je najpomembnejši del pojmovanje varnosti pri vsakem posamezniku. Tukaj bi mogoče še dodal, da se na nacionalni ravni ta del še premalo izpolnjuje, kajti na koncu, po mojem vedenju, še nobena oseba v Slo ni izgubila dovoljenja za dostop do tajnih podatkov oz. ji ni bilo dovoljenje preklicano, zaradi kršitev s področja tajnih podatkov. Mnenja sem, da bi v RS morali imeti en organ, ki bi izvajal varnostne preveritve in bi imel popolno avtoriteto nad tem, zdaj pa imamo štiri organe, ki izvajajo varnostno preverjanje, kar se mi zdi nesmiselno in popolnoma neučinkovito.

8. ***Kakšni so po Vaše najpogostejši razlogi, zaradi katerih prihaja do uhajanja tajnih podatkov? So to splet naključnih okoliščin, nezadosten varnostni sistem, zavestno ali nesrečno(nerodno) delovanje posameznikov?***

Absolutno ni to splet naključnih okoliščin. Do sedaj, kar je bilo uhajanja, je bilo izključno zaradi nekih političnih interesov. Z dobrim sistemom varovanja tajnih podatkov bi lahko hitreje sanirali, odpravili posledice ter locirali posameznika, ki je ta podatek izdal v javnost. Ne bi pa mogli preprečiti kršitev.

9. ***Ali je zavestno delovanje posameznikov, ki ima za cilj izdajo tajnih podatkov politično motivirano ali jih vodijo tudi drugi motivi? Primer: diskreditacija političnih veljakov, sprememba politične moči med političnimi strankami, osebna korist, preprodaja informacij…itd***

Moje mnenje je, da je še vedno najbolj pogost politični motiv; v primerih Patrie je bil močan motiv tudi interes javnosti…lahko smo videli, da je bilo razkritje dokumentov tudi v korist

državljanov. Menim, da bi to moralo biti urejeno na način, kot ga določa zakonodaja; in sicer, da o tem odloča komisija; komisija deluje na nacionalnem varnostnem organu in v takih primerih, kadar je interes javnosti tako velik, kot smo videli, lahko zaseda in tudi umakne stopnjo tajnosti dokumentov in s tem omogoči vpogled javnosti v vsebine podatkov.

10. ***Pomislite na izdajanje tajnih podatkov. Kaj mislite, na katerih področjih in kakšne vrste podatki so najbolj zaželeni?***

Kot smo do sedaj iz prakse ugotovili, ne samo iz prakse ministrstva, temveč tudi iz prakse države in drugih ministrstev, so sigurno najbolj zaželeni podatki iz področja politike in gospodarstva. Primer Dunajske depeše, Washingtonske depeše, primer Patrie.

11. ***A mislite, da je uhajanje povezano z volitvami?***

Za kakšno resnejšo oceno tega vprašanja bomo morali še počakati kakšno desetletje.

12. ***Na kakšen način po Vašem mnenju MZZ prispeva k višjemu nivoju varnostne kulture v RS? Na kakšen način sooblikuje varnostno identiteto posameznika?***

ZTP izvaja redna usposabljanja s področja tajnih podatkov, skrbimo, da vsi uslužbenci sledijo navodilom, da so seznanjeni z zakonodajo ter imajo možnost pridobitve gradiv. Veliko sodelujemo z nacionalnim varnostnim organom in tudi v medresorskih delovnih skupinah, kjer sooblikujemo varovanje tajnih podatkov ter njihovo obravnavanje.

13. ***A menite, da so odnosi med zaposlenimi, nadrejenimi in podrejenimi, občutek pripadnosti organizaciji in lojalnost pomembni faktorji, ki prispevajo k (ne)uhajanju tajnih podatkov oz. čim manjšemu uhajanju?***

Strinjal bi se, da sta lojalnost in zanesljivost posameznika najpomembnejša faktorja. Se pravi, da je uslužbenec lojalen organu, kjer je zaposlen ter seveda tudi državi. Velikokrat se namreč posamezniki ne zavedajo, kakšno škodo povzročajo s tem, ko razkrijejo kakšen tajni podatek.

Priloga C: Intervju z g. Praprotnik Rokom!

Ljubljana, Dnevnik; 09.12.2008

1. ***Ali menite da je trenutna zakonodaja na področju varovanja tajnih podatkov ustrezna?***

Da. Več kot ustrezna je za tistega, ki varuje podatke, ker mu omogoča izredno, da jih varuje tudi ko ni nobenega zakonitega in utemeljenega razloga. Lahko prepreči meni dostop do podatkov, ki bi sicer po vseh demokratičnih standardih in zdravi pameti morali biti javni oz. omogočeni-njemu kot novinarju. Na ta način ta zakonodaja omogoča, da jo zlorabljajo.

2. ***Kako bi ocenili stopnjo varovanja tajnih podatkov v RS?Ali po Vašem mnenju sistem deluje in zagotavlja pričakovano varnost in zahteve mednarodne skupnosti?***

Hvala bogu, da stopnja varovanja še ni takšna in tudi nikoli ne bo, da tajni podatki ki so nezakonito označeni kot tajni, ker se z njimi poskušajo zakriti nepravilnosti in nezakonitosti, takšni tajni podatki ne ostanejo vedno tajni, ker kot vidite v več primerih (SOVA, PATRIA) pridejo tudi do mene, čeprav so formalno tajni. S pomočjo tega lahko izvajamo nadzor nad oblastjo, brez tega je pa več kot očitno, da oblast poskuša z označevanjem tajnosti ta nadzor omejiti oz. preprečiti.

3. ***Ravnanje z zaupnimi podatki, kot smo jih imenovali v preteklosti (pred ZTP) je bilo relativno urejeno v posameznih organih, vendar brez vnaprej znanih kriterijev, kar je imelo za posledico poplavo zaupnih dokumentov. A mislite, da se je količina javno razkritih tajnih podatkov po letu 2001, ko je bil objavljen ZTP, zmanjšala oz. povečala?***

Nimam statistik o tem. Občutek pa govori, da se je količina javno objavljenih tajnih podatkov zmanjšala, ker ni več vsak navaden toaletni robček označen s tajnostjo. Ker, hvala bogu, so vsaj nekateri kriteriji, ampak, kot sam vidim iz prakse, se ti nekateri kriteriji ne spoštujejo vedno in dajejo oznake tajnosti na zadeve, ki nikakor niso utemeljene.

4. ***Kaj so po Vašem mnenju razlogi za uhajanje oz. razkrivanje tajnih podatkov javnosti?***

Po teoriji je jasno, da so razlogi lahko trije: lahko je koristoljubje, resnicoljubje in osebno obračunavanje (politično obračunavanje). Koristoljubje šteje med gospodarske interese.

5. ***Ali mislite, da je uhajanje tajnih podatkov politično motivirano, in da je frekvenca razkrivanja le-teh v predvolilnem času večja?***

Nisem imel občutka, da je frekvenca v predvolilnem času večja. Lahko pa je politično motivirano, vendar ni to nujno vezano na predvolilno obdobje.

6. ***Kaj Vam predstavlja načelo tajnosti in če ga soočite z njenim naravnim nasprotjem javnosti-oz. načelom publicitete!***

Načelo tajnosti: Če se v mojih člankih znajdejo tajni podatki, to pomeni da sem kot novinar svoje delo opravil, tisti, ki bi pa morali varovati tajne podatke pa svojega dela niso opravili. Absolutno se strinjam s stališčem, da je čim manj tajnih podatkov, čim manj skritih zadev, razen, ko gre za osebne zadeve. Ko pa gre za stvari v javnem sektorju, ki se financirajo z državnim denarjem, čim manj tajnosti, ker tajnost je v nasprotju s svobodo kot takšno, svobodo pretoka informacij, svobodo informiranja. Tajnost posega v to. Sem zagovornik tega, da se tajnost uporablja čim redkeje.

7. ***Ali menite, da je tajnost zakrivanje odgovornosti vladajoče pozicije do volivcev?***

Ja. Primer je Patria. Minister Erjavec je poskušal prikriti stvari, ki niso po nobeni logiki zakonito lahko tajna in jih je označil s stopnjo tajnosti. Ni bilo možno dobiti teh podatkov, dokler je bil on na ministrstvu. Čim je prišla nova ministrica, ki tega interesa več nima, kot ga ima on, je nemudoma vzela oznako tajnosti iz teh podatkov. Torej stopnja ogrožanja ni bila prej takšna, da bi opravičevala to, kar tudi zdaj ni, ni bilo zakonitega razloga, da so bili tajni. Pa niso mogli doseči tega, da bi se oznaka tajnosti umaknila, zaradi tega, ker ima politika takšno moč. No, zdaj pa pada toliko močneje po g. Erjavcu.

8. ***Kako bi ocenili varnostno kulturo ljudi v RS, glede na 1. vrednote, 2. pravila in 3. splošno razumevanje področij, kot so nacionalna varnost, varovanje tajnosti, lojalnost organizaciji, instituciji...?***

Varnostna kultura profesionalcev, ki se s tem ukvarjajo v državnih organih, npr. na obrambnem ministrstvu, na policiji na SOVI, je dobra. Problem so funkcionarji, poslanci, ministri, ki s tem, da zasedejo funkcijo, dobijo bianco dostop do vrste tajnih podatkov, brez preverjanja, brez izobraževanja. Če pogledamo kakšne pristojnosti imajo parlamentarna komisija za nadzor SOVE; oni lahko pogledajo vse, poslušajo tudi prisluhe (Janša, Sanader pogovori-prisluhi)- tu Need to know principa ni, v osnovi pa niso ugotovili kar bi morali, se pravi, da je cela stvar neustavna. Primer: Rop- razlagal Vodušku kaj je zvedel kot predsednik vlade od SOVE, tu ni varnostne kulture.

9. ***Se Vam zdi posameznik pomemben člen v sistemu varovanja tajnih podatkov?***

Posameznik je najbolj pomemben člen. Sicer je sistem pomemben, ki funkcionira po točno določenem varovanju prostora: primer SOVA (monitor, brez priključka za USB, niti printerja), ta sistem omogoča to, da v fizični obliki ne uhajajo podatki iz sistema. V smislu informacij, pa so posamezniki tisti, ki ne varujejo, oz. varujejo podatke. Posameznik je potem tu ključni člen v varovanju tajnosti.

10. ***Prosim, če dopolnite stavek: Varnostna kultura se najboljše oblikuje……..***

…..z odgovornim ravnanjem in z zavedanjem o tem, kaj je pomembno za nacionalno in posameznikovo varnost. To pa pomeni z izobraževanjem.

11. ***Kaj so po Vaše značilnosti pozitivne varnostne kulture in kaj negativne? A bi uvrstili razkrivanje tajnih podatkov k negativni varnostni kulturi?***

Pozitivna varnostna kultura je značilna za posameznike, ki zakonito uporabljajo predpise o tajnih podatkih. Zakonita uporaba represivnih organov in obveščevalnih služb itd. Ne nujno vedno, ker kadar gre za razkrivanje tajnih podatkov v korist temu, da je javnost obveščena o morebitnih nepravilnostih in nezakonitostih, potem je to del pozitivne varnostne kulture. Ker na ta način lahko tistim, ki vodijo državo ali pa sisteme, postavimo ogledala in temu lahko

sledijo neke ustrezne konsekvence. Če bi nezakonitosti ostale tajne, pozitivnih konsekvenc ne bi moglo biti in družba bi tonila v živ pesek- ne bi vedeli, da je v sistemu nekaj skorumpirano, če bi vse ostalo skrito.

12. ***Tajnost v demokratični državi je legitimno sredstvo, s pomočjo katerega se ščitijo vitalni interesi države. Prosim za komentar!***

Ja. Ampak samo v izjemnih primerih.

13. ***Ali bi se strinjali s trditvijo, da je zagotavljanje varnosti v vsakem sistemu, v vse bolj kritičnih okoljih, nov izziv?Prosim za komentar!***

Vsesplošna obsedenost z varnostjo se mi zdi pretirana. Mislim, da ovira normalen razvoj in napredek družbe. Če pa govorimo o varnosti informacij…informacije so bile zmeraj pomembne, danes enako kot včasih, ker pa je pri vsaki zadevi zelo pomembno, da med zajemom informacij in med obdelavo mine čim manj časa, in ker so danes komunikacijske poti izjemno hitre je seveda varovanje informacij zelo pomembno, oz. ima večji pomen, ker od dobiti informacijo do uporabe le-te–nepooblaščene, danes mine zelo malo časa. Samo mobitel omogoča to. Kar pa se tiče ostale varnostni; ocena ogroženosti, državnih institucij, posameznih funkcionarjev ni tako zaskrbljujoča, kot pa je v javnosti izpostavljen pojem varnosti in potreba po varnosti.

14. ***Elementi za vrednotenje prakse bi morali izvirati iz samega zakona! Prosim za komentar?***

Da. Vendar, kaj nam je za narediti, ko tisti, ki zakon uporabljajo in imajo legitimacijo za njega, si ga razlagajo drugače kot mi. Mi argumentirano povemo, zakaj neka stvar ne more biti tajna, in tisti, ki ima moč z recimo izmišljenimi argumenti, ki delujejo kvazi strokovno, prepriča celo informacijsko pooblaščenko, da mora nekaj biti tajno, recimo zaradi nacionalne varnosti, npr. informacija, koliko topov je na Patriah kupila RS-ni razloga da je tajna, a je celo informacijska pooblaščenka pokleknila. Elementi za vrednotenje prakse morajo izvirati iz zakona, vendar si zakone razlagamo različno in vsak zakon ima dovolj manevrskega prostora, da ga lahko tisti, ki ga uporablja na področju varovanja tajnih podatkov zlorablja. To se je pokazalo že na večih primerih, hvalabogu, pa je to napredek glede na prejšnji sistem.