*Iztok PREZELJ in Milan TARMAN**

SISTEM VAROVANJA TAJNIH PODATKOV V REPUBLIKI SLOVENIJI V LUČI DEMOKRATIČNEGA ZAGOTAVLJANJA NACIONALNE VARNOSTI**

Povzetek. *Grožnja nezakonitega odtekanja tajnih podatkov zahteva oblikovanje učinkovitega sistema varovanja tajnih podatkov v vsaki sodobni državi. Varovanje tajnih podatkov zahteva celovit pristop, ki presega ozko sistemsko razmišljanje. Članek v tem smislu opredeljuje koncept celovitega sistema varovanja tajnih podatkov, ki obsega zakonodajne in institucionalne elemente, kriterije za določanje tajnih podatkov, kriterije za dostopanje do tajnih podatkov, časovno omejenost tajnosti in postopke za umik tajnosti, mehanizme za zaščito virov, ki razkrijejo kazniva dejanja itd. Proučitev obstoja teh elementov v Sloveniji kaže, da je država sistemsko dokaj celovito uredila področje varovanja tajnih podatkov, vendar pa se sooča še z nekaterimi perečimi izzivi.*

Ključni pojmi: *nacionalna varnost, tajni podatki, sistem varovanja tajnih podatkov, obveščevalna dejavnost, odtekanje tajnih podatkov, dostop, varnostno preverjanje, žvižgači*

Uvod

Javnost dela ter pravica dostopa do podatkov in informacij državnih organov je splošno sprejeto načelo v sleherni demokratični družbi. Demokratična država dolgoročno ne more učinkovito delovati brez zaupanja javnosti in posledične legitimnosti. Hkrati pa mora sleherna država zagotavljati nacionalno varnost, kar pomeni suverenost na svojem ozemlju, varnost prebivalstva in ključnih družbenih institucij (državne institucije, kritična infrastruktura ipd.). V ta namen država uporablja tudi tajne podatke, ki so pomembni zato, ker bi njihovo razkritje nepooblaščenim osebam ali širši javnosti lahko ogrozilo varnost zgoraj navedenih prvin. Sodobne države so izpostavljene širokemu spektru ogrožanja, v katerem igra odtekanje tajnih podatkov zelo specifično vlogo. Poleg tega obstaja ogrožanje s strani tujih

* *Dr. Iztok Prezelj, izredni profesor na Fakulteti za družbene vede Univerze v Ljubljani; mag. Milan Tarman, sekretar v Uradu Vlade Republike Slovenije za varovanje tajnih podatkov.*

** *Pregledni znanstveni članek.*

obveščevalnih služb, ki se namerno in sistematično fokusirajo na pridobivanje tajnih podatkov drugih držav, ki zanje predstavljajo obveščevalne tarče. Glavni cilj obveščevalnih služb je pridobiti tajne podatke, informacije in dokumente ciljne države oziroma organizacije ter jih uporabiti v korist svojih nacionalnih interesov. Pri tem uporabljajo predvsem metode, kot sta HUMINT (pridobivanje tajnih podatkov s pomočjo človeških virov – vohunov in informatorjev) in TECHINT (pridobivanje tajnih podatkov s pomočjo tehničnega spremljanja komunikacij in drugih vrst signalov).

Zaradi grožnje nezakonitega odtekanja tajnih podatkov so države v okviru svojih sistemov nacionalne varnosti razvile tudi podsistem varovanja tajnih podatkov. Poleg tega pa nezakonite obveščevalne namere v zvezi s pridobivanjem tajnih podatkov spremljajo tudi protiobveščevalni organi (glej Shulsky in Schmitt, 2003: 9; Lowenthal, 2003: 113). Še več, sodobna praksa v državah članicah zveze NATO je pokazala, da ne samo sovražne države, temveč tudi prijateljske države intenzivno pridobivajo tajne podatke druga od druge. To pomeni, da države lahko intenzivno prijateljsko sodelujejo, hkrati pa zbirajo tajne podatke in s tem ogrožajo varnost in interese druga druge (primer ameriškega prisluškovanja mobilnemu telefonu nemške kanclerke Angele Merkel).[1] Sistemska ureditev področja varovanja tajnih podatkov je potrebna tudi zaradi tipičnih preteklih težav na tem področju. Moynihan (1997: 59–66) je denimo poudarjal, da se je razvila prekomerna kultura tajnosti (angl. *culture of secrecy*), ki se nanaša na prekomerno označevanje tajnosti v prekomernem času (angl. *overclassification of information*), kar je posledično onemogočilo prosto izmenjavo idej in informacij. Po drugi strani pa je v literaturi je mogoče najti tudi ravno nasprotna poročila o podcenjevanju potrebe po tajnosti (angl. *underclassification*), ki se včasih pojavlja v zvezi z raziskovalnimi rezultati določenih projektov, ki jih raziskovalci objavijo, ipd. (glej Shulsky in Schmitt, 2003).

Nujnost sistemskega pristopa k ureditvi varovanja tajnih podatkov je torej neizpodbitna, vprašanje pa je, kako sodobne države sistemsko to področje uredijo. Vprašanje je tudi, katere elemente zajema sodobni sistem varovanja tajnih podatkov. Razumljivo je, da načelo javnosti dela ter dostopnosti do podatkov in informacij državnih organov in nosilcev javnih pooblastil ne more veljati absolutno in neomejeno. V zvezi s tem je najpomembnejše vprašanje, v katerih primerih, na kakšen način in pod katerimi pogoji je dopustno določene podatke in informacije odtegniti javnosti. Določeni podatki in informacije, ki nastanejo oziroma obstajajo v državnih organih, se morajo zaradi zavarovanja določenih državnih interesov in

[1] *Kissinger je že davno tega ugotavljal, da prijateljske obveščevalne agencije ne obstajajo, in navajal primere, kako je Izrael vohunil proti ZDA, ZDA proti Franciji in Kitajska proti ZDA v času, ko so te države bile strateške partnerke (glej Lowenthal, 2003: 113).*

koristi določiti kot tajni, s čimer se njihova dostopnost bistveno omeji. Za varovanje tajnosti mora država vzpostaviti instrumente, ki ščitijo zasebnost države pred javnostjo in dejanskim ali potencialnim nasprotnikom. Ob tem, ko se državi dopusti zaščita tajnosti, pa je treba zagotoviti tudi dovolj močne vzvode, ki onemogočajo in otežujejo zlorabo tega instituta.

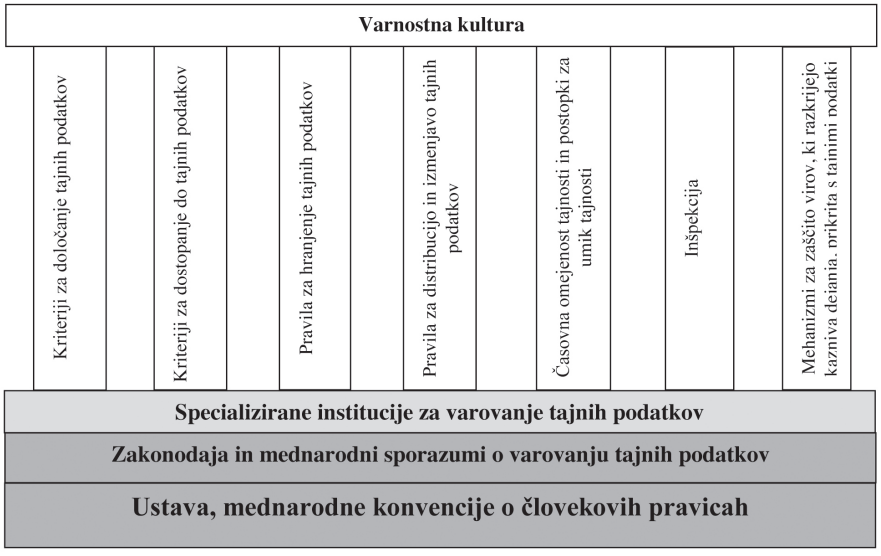
Cilj tega članka je opredeliti temeljne elemente celovite ureditve varovanja tajnih podatkov v sodobni državi in hkrati proučiti, kako je to področje urejeno v Republiki Sloveniji. Avtorja zagovarjava tezo, da je Slovenija kot mlada država sistemsko dokaj celovito uredila področje varovanja tajnih podatkov, vendar pa se sooča še z nekaterimi resnimi izzivi. Besedilo se najprej osredotoča na opredelitev temeljnih elementov celovite ureditve varovanja tajnih podatkov, nato pa sledi analiza urejenosti po posameznih elementih v Republiki Sloveniji. Na koncu avtorja izpostavljava temeljne sistemske izzive v zvezi z vsakim elementom in podajava predloge za izboljšanje ureditve v prihodnosti.

Celovita ureditev varovanja tajnih podatkov v sodobni državi

Označevanje podatkov za tajne, način dostopanja do njih in ravnanja z njimi morajo potekati po natančno določenih in transparentnih pravilih. Tajni podatek ima svoj pričakovani življenjski cikel (nastanek, uporaba ob hkratni zaščiti, prenehanje ali umik stopnje tajnosti), kar pomeni, da mora sistem varovanja tajnih podatkov celovito zajemati različne mehanizme. Celovitost je pomembna zato, da demokratična država nadzira vse vidike in postopke določanja, ravnanja in umikanja (deklasificiranja) tajnih podatkov ob hkratni demokratični odgovornosti svoji javnosti. Celovitost ureditve sistema varovanja tajnih podatkov torej pomeni, da varovanje temelji na ustavnih osnovah in temeljnih mednarodnih deklaracijah o človekovih pravicah. Državna tajnost se mora uporabljati tudi v podporo varovanja človekovih pravic, saj je država namenjena ljudem in ne sama sebi oziroma peščici ljudi. Sistem varovanja tajnih podatkov mora temeljiti na posebnem zakonu, ki ureja to področje. Celovitost pristopa na tem področju je razvidna ravno iz tega zakona. Za proces varovanja tajnih podatkov v sodobni državi morajo skrbeti odgovorne posebne institucije: nacionalni organ za varovanje tajnih podatkov, ki ima nadresorni pomen, in pa posamezni resorni organi, ki skrbijo za varovanje tajnih podatkov na svojem področju. Poleg tega morajo skrbeti za varovanje teh podatkov vse osebe in institucije, ki take podatke tudi posedujejo. To pomeni, da v širšem institucionalnem smislu sistem varovanja tajnih podatkov vključuje omrežje številnih državnih organov in tudi nedržavnih organizacij. Sistem varovanja tajnih podatkov mora določati natančne kriterije za določanje tajnih podatkov, ki morajo vsebovati tudi jasno utemeljitev razlogov za označitev s stopnjo

tajnosti. Obstajati morajo natančna pravila za dostopanje do tajnih podatkov (npr. varnostno preverjanje, pravica do védenja itd.) in tudi pravila za hranjenje tajnih podatkov. Dostopanje do tajnih podatkov je v tesni povezavi z natančno določenimi pravili za njihovo distribucijo in izmenjavo v okviru posamezne države ali pa v mednarodnem okviru, bodisi bilateralno ali pa multilateralno. Kot posledico pritiska demokratične javnosti je treba videti nujnost obstoja časovne omejitve tajnosti in postopkov za umik tajnosti. S temi postopki se konča življenjski cikel tajnega podatka, kar je zelo pomembno za demokratično družbo, poleg tega pa tudi za seznanjenost in učenje o načinu delovanja države ter o njeni preteklosti. Vsak podsistem v okviru sistema nacionalne varnosti mora biti izpostavljen različnim oblikam nadzora. Za učinkovitost delovanja sistema varovanja tajnih podatkov je ključen inšpekcijski nadzor, ki ugotavlja odklone od predvidene zaščite in nalaga popravke kot sistemski korekcijski mehanizem. Teorija in praksa s področja varovanja tajnih podatkov sta pokazali, da se pri zagotavljanju nacionalne varnosti in ravnanju s tajnimi podatki vendarle lahko dogajajo nepravilnosti in nezakonitosti. Iz tega razloga je smotrno vključiti v širši okvir sistema varovanja tajnih podatkov tudi mehanizme zaščite virov, ki razkrijejo kazniva dejanja, prikrita s tajnimi podatki (t. i. žvižgači). Za delovanje vseh naštetih elementov in mehanizmov je odgovoren človek, ki lahko ravna bolj ali manj odgovorno. Njegovo ravnanje je v tem smislu odvisno od stopnje varnostne kulture, ki je prav tako eden od temeljnih elementov sodobnega sistema varovanja tajnih podatkov.

Slika 1: SODOBNI SISTEM VAROVANJA TAJNIH PODATKOV



Naj poudarimo, da model zaradi omejitve prostora vsebuje samo ključne in splošne elemente sistema varovanja tajnih podatkov.

Zakonodajni in institucionalni vidiki sistema varovanja tajnih podatkov

Področja, ki pomembno ali celo usodno zadevajo varstvo človekovih pravic (vključno s pravico države, da zagotovi svoj obstoj), je treba nujno urediti z ustreznim in konsistentnim pravnim redom (Anžič, 2001: 48). V tem smislu je tudi nujno, da se sistem določanja tajnosti omeji z zakoni (Moynihan, 1997: 64–65). V Sloveniji je pravica, da vsakdo lahko pridobi informacijo javnega značaja, ustavna kategorija, saj Ustava Republike Slovenije v 39. členu določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. Zakon o določanju, ravnanju in dostopu do tajnih podatkov predstavlja torej en vidik uresničitve ustavne pravice do obveščenosti. V tem primeru gre za uresničitev ustavne obveznosti, da mora zakon določiti razloge, zaradi katerih se lahko odreče dostop do informacij javnega značaja (Rovšek, 2001: 35). V tem smislu je Državni zbor Republike Slovenije leta 2001 sprejel Zakon o tajnih podatkih, ki je predstavljal začetek sistemskega urejanja varovanja tajnih podatkov v Republiki Sloveniji kot demokratični državi. Danes velja Zakon o tajnih podatkih (ZTP) iz leta 2006, s kasnejšimi spremembami in dopolnitvami v letih 2010 in 2011, ko je bil ustrezno nadgrajen ob upoštevanju mednarodnih standardov. Zakon o tajnih podatkih (2006) določa skupne osnove enotnega sistema določanja varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov RS, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ter prenehanja tajnosti takšnih podatkov. Zakon zavezuje vsako osebo, državne organe, organe lokalnih skupnosti, gospodarske družbe itd., ki se seznanijo z vsebino tajnega podatka, da so odgovorni za njegovo varovanje in ohranitev njegove tajnosti (1. člen). Dolžnost varovanja tajnih podatkov pa ne preneha, ko te osebe prenehajo z delom ali funkcijo (8. člen). Uredba o varovanju tajnih podatkov (2005) pa konkretneje določa sistem fizičnih, organizacijskih in tehničnih postopkov in ukrepov pri varovanju tajnih podatkov. Na informacijskem področju je bila dodatno sprejeta še Uredba o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih (2007), ki je vzpostavila sistem minimalnih fizičnih, organizacijskih in tehničnih standardov, postopkov in ukrepov za varovanje tajnih podatkov.

Sistem varovanja tajnih podatkov je sestavni del sistema nacionalne varnosti v Republiki Sloveniji. Resolucija o strategiji nacionalne varnosti Republike Slovenije (2010), ki je temeljni razvojno-usmerjevalni dokument na

področju nacionalne varnosti, sicer ne omenja neposredno nalog sistema varovanja tajnih podatkov, poudarja pa pomen tajnih podatkov na področju nacionalne varnosti. V zvezi z dejavnostjo tujih obveščevalnih služb resolucija omenja krepitev klasičnega obveščevalnega delovanja nekaterih tujih držav proti Republiki Sloveniji zaradi njene aktivnejše vloge v okviru mednarodne skupnosti, zlasti v Evropski uniji in Natu. Resolucija izpostavlja, da pri tem izstopa interes za pridobitev vseh vrst tajnih podatkov ter zanimanje za slovenske diplomatske in gospodarske aktivnosti v mednarodnem okolju. Poleg tega pa tudi omenja možnost še agresivnejšega delovanja tujih obveščevalnih in varnostnih služb proti predstavnikom RS v tujini (poglavje 4.2.6). V poglavju o odzivanju na tujo obveščevalno dejavnost resolucija tudi omenja sodelovanje med našimi obveščevalnimi službami in odgovornimi nosilci na področju varovanja tajnih podatkov RS v zvezi z ukrepi proti tuji obveščevalni dejavnosti (poglavje 5.3.6).

Z institucionalnega vidika je pomembno, da izvajanje zakona o tajnih podatkih v RS ter z njim povezanih predpisov in mednarodnih pogodb spremlja nacionalni varnostni organ, ki ga v Sloveniji predstavlja Urad Vlade za varovanje tajnih podatkov. Urad 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 itd. (Zakon o tajnih podatkih, 2006: 43.a člen) V ministrstvih, organih in nedržavnih organizacijah pa za varovanje tajnih podatkov skrbijo specializirana telesa ali posamezniki.

Kriteriji za določanje tajnih podatkov

Tajni podatki sleherni državi omogočajo, da z oznako tajnosti varuje svoje vitalne interese in tako zadosti svoji nacionalni varnosti. V tem smislu je zelo pomembno, da so kriteriji za določitev tajnosti jasni in enostavni. Ti kriteriji se skozi zgodovino očitno spreminjajo. Če denimo pogledamo vojaško področje, lahko ugotovimo, da po koncu hladne vojne določeni podatki tipično niso več tajni: gre denimo za lokacije vojaških objektov in enot, obrambni proračun, število vojakov po enotah, število orožij, kot so glavni bojni tanki, bojna letala, topovi ipd., namen in izvedba večjih vojaških vaj itd. (glej Vienna Document 2011 on CSBM, 2011). Še vedno pa so lahko tajni: raven usposobljenosti vojaških posadk, kakovost vzdrževanja orožja, proizvodnja novih tipov oborožitvenih sistemov itd. Splošni kriterij za označitev tajnosti pri podatkih je po Moynihanu (1997: 64–65) demonstrativna potreba po zaščiti podatkov v imenu nacionalne varnosti, vendar pa je treba

to potrebo ohranjati na minimumu. V primeru dvoma, ali podatki potrebujejo zaščito, se jih ne sme označiti za tajne. Clark (2004: 97–98) v zvezi s tem poudarja, da na obveščevalnem področju obstajajo različne logike pri zaščiti podatkov. Običajno se obveščevalni produkt označi z nižjo stopnjo tajnosti (ker njegovo razkritje razkrije samo njega) kot denimo obveščevalni viri in metode. Najvišjo stopnjo zaščite se načeloma nameni podatkom o virih, ker bi njihovo razkritje lahko povzročilo zaprtje ali smrt določenih oseb. Tudi podatki COMINT (še posebej kripto telekomunikacije) so zelo zaščiteni, medtem ko podatki IMINT ne potrebujejo velike zaščite, ker je dokaj jasno, kaj se da dobiti in kako. Podatki OSINT pa ne potrebujejo nobene zaščite, razen tega, kaj natančno so tarče in katere medije se spremlja (druge obveščevalne službe lahko namreč podtaknejo zgodbe v določene medije).

V Sloveniji 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 varnostnih razlogov zavarovati pred nepoklicanimi osebami. Tajni dokument se lahko nanaša na napisan, narisan, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugačen zapis tajnega podatka (Zakon o tajnih podatkih, 2006: 2. člen). Ključni kriterij za določitev tajnosti in njene stopnje je v Sloveniji vezan na potencialno škodo v primeru razkritja. Za tajnega se tako lahko določi podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale ali bi očitno lahko nastale škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, in se nanaša na:

1. javno varnost;
2. obrambo;
3. zunanje zadeve;
4. obveščevalno in varnostno dejavnost državnih organov Republike Slovenije;
5. sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije;
6. znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije (Zakon o tajnih podatkih, 2006: 5. člen).

Tajni podatki se glede na možne škodljive posledice za varnost države ali za njene politične ali gospodarske koristi razvrščajo po naslednjih stopnjah:[2]

[2] *Za primerjavo si poglejmo, kako so tajni podatki označevani v zvezi NATO:*

– *COSMIC TOP SECRET: nepooblaščeno razkritje bi povzročilo izjemno resno škodo zvezi NATO;*

1. "STROGO TAJNO", ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo;
2. "TAJNO", ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije;
3. "ZAUPNO", ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije;
4. "INTERNO", ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa (n. d.: 13. člen).[3]

Predpisi o tajnih podatkih opredeljujejo tudi materialna in formalna merila tajnosti. Po ZTP je namreč tajen le tisti podatek, ki kumulativno izpolnjuje materialno in formalno merilo tajnosti. Materialno merilo tajnosti podatka se opira na sámo vsebino podatka in določa, da se lahko podatek določi za tajnega le takrat, če je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi lahko nastale ali bi očitno nastale škodljive posledice za varnost države ali za njene politične in gospodarske koristi, ter se obenem nanaša izključno na že zgoraj navedena področja. Materialno merilo torej vključuje dva vidika – prvi je v tem, da bi z razkritjem podatka lahko nastala ali bi očitno nastala določena škoda, drugi pa v povezavi škode s taksativno naštetimi interesnimi področji države. Oba materialna elementa se zrcalita v formalnem merilu tajnega podatka. Podatek je upravičeno označen kot tajen le, če so izpolnjeni trije formalni elementi. Prvi tak element je, da lahko podatek za tajnega določi le za to pooblaščena oseba. Načeloma je to po ZTP predstojnik organa ali oseba na najvišjih delovnih mestih in položajih, s čimer je zagotovljeno, da odločitve o tajnosti sprejemajo osebe, ki imajo dovolj informacij in znanja, da lahko ocenijo pomen morebitnih škodljivih posledic ob razkritju tajnega podatka. ZTP predpisuje tudi način in postopek določanja tajnosti, katerega bistvo je v izdelavi pisne ocene o tem, kateri podatek se dejansko stopnjuje, razloge za stopnjevanje in možne škodljive posledice, ki bi lahko nastale z razkritjem podatka. Pisna ocena je obvezna in dejansko določa objekt varstva, torej interes, ki bi bil z razkritjem nepooblaščeni osebi ogrožen. Pisna ocena se hrani kot priloga dokumenta pri organu, ki je podatku določil stopnjo tajnosti. Prav ta pisna ocena možnih škodljivih posledic omogoča tudi naknadno preverjanje in ugotavljanje

– *NATO SECRET: nepooblaščeno razkritje bi povzročilo resno škodo zvezi NATO;*
– *NATO CONFIDENTIAL: nepooblaščeno razkritje bi bilo škodljivo zvezi NATO;*
– *NATO RESTRICTED: nepooblaščeno razkritje bi bilo škodljivo interesom in učinkovitosti zveze NATO (Brezovšek in Črnčec, 2010: 108–109).*

[3] *Vsi pisni dokumenti morajo imeti označeno stopnjo tajnosti v glavi in nogi, poleg tega pa tudi številko izvoda dokumenta ipd. (Uredba o varovanju tajnih podatkov, 2005).*

razlogov in okoliščin za odločitev, da se podatek določi za tajnega. Tretji element formalnega merila pa temelji na pravilni oznaki, saj je tajen samo tisti podatek, ki je ustrezno označen kot tajen.

Kriteriji za dostopanje do tajnih podatkov

Eden od ključnih kriterijev za dostopanje do tajnih podatkov je potreba po védenju (angl. *need to know*), ki jo ima posameznik ali organizacija za opravljanje svojih nalog. To določi, kdor je odgovoren za posamezen tajni podatek in njegovo razpošiljanje (Shulsky in Schmitt, 2003). Drugi kriterij za dostopanje do tajnih podatkov je varnostna preverjenost posameznikov. Pri tem gre za ugotavljanje volje po ohranjanju zaupnih podatkov in tveganj v zvezi s tem. Kandidati odgovarjajo na posebne vprašalnike, čemur sledi preverjanje odgovorov, podatkovnih baz, opravljanje intervjujev s prijatelji, znanci, sosedi, sošolci itd. (prav tam). Za pridobitev dovoljenja se opravlja tudi vpoglede v razne nacionalne baze podatkov o kaznovanosti, izobrazbi, finančnem stanju itd. Intervjuji se lahko osredotočajo na zbiranje podatkov o sedanjih in preteklih aktivnostih, družinskem ozadju, financah (zadolženost), uživanju drog, alkohola, mentalni neuravnovešenosti, kompromitirajočem seksualnem vedenju itd. (Lerner in Wilmoth Lerner, 2004: 61). Pri tem preverjanju je pomembno tudi ugotoviti, da preverjane osebe niso dovzetne za izsiljevanje (Lownethal, 2003).

V Sloveniji morajo biti vse osebe, ki dostopajo do tajnih podatkov zaradi opravljanja nalog ali funkcije na svojem delovnem mestu, ustrezno varnostno preverjene (razen nekaterih zakonsko določenih izjem ter za stopnjo "interno", kjer zadošča osnovno usposabljanje in podpis izjave o varovanju tajnih podatkov) (Zakon o tajnih podatkih, 2006). To pomeni, da se v postopku varnostnega preverjanja osebe preveri njena lojalnost, zanesljivost in verodostojnost, in sicer z namenom, da se ji izda ali da zadrži dovoljenje za dostop do tajnih podatkov. V postopku varnostnega preverjanja se obravnavajo vidiki, ki zadevajo osebnostni značaj, in okoliščine, ki bi lahko povzročile nastanek potencialnih varnostnih problemov. Za različne stopnje tajnosti obstajajo različne ravni varnostnega preverjanja: osnovno varnostno preverjanje, razširjeno varnostno preverjanje in razširjeno varnostno preverjanje z varnostnim poizvedovanjem. Preverjanje se opravi na osnovi vprašalnikov, ki jih kandidati izpolnijo. V primeru varnostnega zadržka se posameznikom dovoljenje za dostop do tajnih podatkov ne izda.

Informacijski sistemi, ki vsebujejo tajne podatke, morajo v skladu z Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (2007) prav tako pridobiti varnostno dovoljenje za delovanje. Ključne sestavine takih sistemov so strežniki, usmerjevalniki in delilniki prometa, oprema za upravljanje in nadzor, aktivna oprema za prenos podatkov v

nešifrirani obliki, oprema za šifrirno zaščito podatkov, varnostne pregrade, oprema za odkrivanje in zaščito pred vdori, oprema za izdelavo varnostnih kopij. Informacijski sistemi lahko delujejo na tri varnostne načine glede na nadzor dostopa do tajnih podatkov: neselektiven, selektiven in dvojno selektiven način. Ti sistemi so tudi občutljivi na poskuse odtujevanja tajnih podatkov, kar se označuje kot kritični informacijski varnostni dogodek.

Praksa ogrožanja tajnih podatkov kaže, da samó varnostno preverjanje in posedovanje ustreznega dovoljenja ne predstavlja nujno stoodstotnega zagotovila za varstvo tajnih podatkov. Evidentno nedavno deviacijo kljub predhodnemu varnostnemu preverjanju in posedovanju ustreznega dovoljenja predstavlja primer Estonca Hermana Simma, ki je posredoval Rusiji številne tajne podatke zveze NATO. Simm je na estonskem obrambnem ministrstvu delal od leta 1995 in je bil do leta 2006 vodja varnostnega oddelka na ministrstvu, kar pomeni, da je imel dostop do najstrožje zaupnih dokumentov. Prijeli so ga septembra leta 2008 in mu nato začeli soditi v popolni tajnosti. Po pričevanju preiskovalcev je 61-letni Simm delal za rusko obveščevalno službo (SVR) in se z njenimi člani tri- do štirikrat na leto srečeval v različnih evropskih državah, kjer jim je večinoma predajal tajne dokumente zveze NATO. Sodišče ga je obsodilo na 12-letno zaporno kazen in plačilo denarne odškodnine. Gre za največji vohunski škandal v Estoniji po koncu hladne vojne in primer je v estonski javnosti povzročil kar nekaj razburjenja, še posebno ker je Simm Estonec in ne pripadnik ruske manjšine, ki šteje četrtino prebivalstva v tej baltski državi. Zveza NATO je v povezavi s tem vohunskim škandalom v letu 2009 odredila izgon dveh ruskih diplomatov iz Bruslja. S tem je sprožila oster odziv Moskve, ki je dejanje označila za "veliko provokacijo" (glej Schmid in Ulrich, 2010; Former Estonian High Government Official Suspected in Treason, 2008).

Zgoraj navedeni kriteriji za dostopanje do tajnih podatkov pa imajo tudi izjemo. Po ZTP (2006: 3. člen) lahko do tajnih podatkov brez dovoljenja za dostop dostopajo natančno določene kategorije oseb: predsednik republike, predsednik vlade, poslanec, državni svetnik, župan in občinski svetnik, minister in predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade, varuh človekovih pravic in njegov namestnik, guverner, namestnik in viceguverner centralne banke, član računskega sodišča, sodnik, predsednik in član državne revizijske komisije, državni tožilec, generalni državni pravobranilec in informacijski pooblaščenec. Prav tako ima dostop do tajnih podatkov tudi Komisija DZ za nadzor nad delom obveščevalnih in varnostnih služb (4. člen). Te osebe dobijo dovoljenje z začetkom funkcije oziroma opravljanja dela in podpisom izjave, da so seznanjene s tem zakonom in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ter da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.

Pravila za hranjenje tajnih podatkov

Pri varovanju tajnih podatkov se posebna pozornost posveča shranjevanju teh podatkov. Slovenska Uredba o varovanju tajnih podatkov (2005: 10. člen) določa območja, v katerih se lahko obravnavajo tajni podatki. Tajni podatki stopnje "interno" se lahko obravnavajo kar v upravnem območju, medtem ko se tajni podatki stopnje tajnosti "zaupno" ali višje stopnje lahko obravnavajo in hranijo samo v določenem vidno označenem prostoru, ki ga imenujemo varnostno območje I. ali II. stopnje. Varnostno območje I. stopnje je označen prostor, v katerem se lahko obravnavajo tajni podatki stopnje "zaupno" ali višje stopnje tajnosti tako, da že sam vstop v varnostno območje pomeni dostop do teh podatkov. V tem varnostnem območju se izvajajo najmanj naslednji varnostni postopki in ukrepi:

- sistem vhodnega nadzora, ki zagotavlja popoln nadzor nad vstopom oziroma izstopom oseb in vozil z ustreznim dovoljenjem;
- vodenje razvida tajnih podatkov, s katerimi se oseba seznani že ob samem vstopu v varnostno območje;
- prepoved vnosa kakršnihkoli mehanskih, elektronskih in magnetno-optičnih sestavnih delov, s katerimi bi bilo mogoče nepooblaščeno posneti, odnesti ali prenesti tajne podatke;
- neposredno in neprekinjeno fizično varovanje varnostnega območja;
- ob nadomestitvi fizičnega varovanja s sistemom tehničnega varovanja mora ta sistem zagotavljati celovit nadzor varnostnega območja, ki mora biti nadzorovano iz nadzornega centra, itd.

Varnostno območje II. stopnje pa je označen prostor, v katerem se tajni podatki stopnje "zaupno" ali višje stopnje obravnavajo tako, da sam vstop in gibanje v tem območju še ne omogočata dostopa do teh podatkov. V tem varnostnem območju se izvajajo manj restriktivni ukrepi kot v primeru varnostnega območja I. stopnje.

Tajni podatki se morajo hraniti v pisarniških ali protivlomnih omarah (podatki stopnje "interno") in v blagajnah, ki morajo ustrezati najmanj protivlomni stopnji II (stopnji "zaupno" in "tajno") ter stopnji III (stopnja "strogo tajno"). Število oseb, ki ima dostop do elektronskih ali mehanskih ključev, naj bi bilo čim manjše (Uredba o varovanju tajnih podatkov, 2005: 19. člen). Poleg tega se varnostna območja ščitijo tudi protiprisluškovalno.

Tajni podatki in objekti, kjer se nahajajo, se praviloma varujejo s kombinacijo tehničnih in fizičnih ukrepov. Pri tehničnem varovanju gre za uporabo protivlomnih sistemov (npr. varovalne ograje, protivlomna vrata, varovalne rešetke, protivlomne omare, cestne zapore itd.), sistemov za nadzor gibanja (npr. identifikacijski sistemi za preverjanje gesel, biometričnih podatkov itd.), sistemov videonadzora (kamere) in alarmnih sistemov za

javljanje nepooblaščene prisotnosti, odkrivanje in javljanje požarov. Fizično varovanje pa vključuje varnostno osebje, ki opravlja kontrolo dostopa, obhode po objektih, reagiranje ob alarmih, varovanje prenosa tajnih dokumentov (Grabušnik, 2007).

Pravila za distribucijo in izmenjavo tajnih podatkov (nacionalno in s tujino)

Po 11. septembru se poleg potrebe po védenju vedno bolj uveljavlja potreba po delitvi informacij med akterji, odgovornimi za varnost (angl. *need to share*). Po Zakonu o tajnih podatkih (2006: 31.a člen) imajo v Sloveniji pravico dostopa do tajnih podatkov samo tiste osebe, ki imajo dovoljenje in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog (angl. *need to know*). Tajnih podatkov nihče ne sme dobiti prej ali v večjem obsegu, kot je potrebno. Po 34. in 35. členu pa se tajni podatki lahko pošiljajo drugim organom, ki morajo ravno tako ravnati po tem zakonu. Za organizacije je pomembno, da imajo varnostno dovoljenje, kar pomeni, da izpolnjujejo fizične, organizacijske in tehnične pogoje za varovanje tajnih podatkov, da do teh podatkov dostopajo le osebe z varnostnim dovoljenjem, da imajo odgovorno osebo za ravnanje s tajnimi podatki, da varujejo prostore s tajnimi podatki in komunikacije, po katerih se prenašajo tajni podatki, da imajo kontrolo dostopov do teh podatkov ipd. Po 39. členu organi ne smejo posredovati ali prenašati tajnih podatkov po nezaščitenih komunikacijskih sredstvih.

Člen 37 pa dodatno zahteva, da morajo pooblaščene osebe organov in organizacij imeti ažuren pregled nad distribucijo tajnih podatkov izven njihovih sistemov. Uredba o varovanju tajnih podatkov (2005: členi 21–24) določa načine prenosa in pošiljanja tajnih podatkov. Taki podatki se v soodvisnosti od stopnje tajnega podatka lahko pošiljajo v dveh ovojnicah, zaklenjenih kovčkih, škatlah ali torbah. Podatke prenašajo posebej usposobljene kurirske službe. Uredba prav tako določa pravila za razmnoževanje tajnih podatkov, ki mora biti ravno tako evidentirano, vse kopije pa tudi primerno označene (členi 25–26).

Za potrebe mednarodne izmenjave tajnih podatkov prav tako obstajajo natančno določena pravila. Izdelava pravne podlage in s tem povezanega sistema varovanja tajnih podatkov EU je bila prvi korak, obenem pa tudi pogoj za članstvo Slovenije v EU. Republika Slovenija je poleg usklajevanja teh pravil za uspešen vstop v EU leta 2004 kasneje izvedla tudi postopek usklajevanja in sprejemanja sporazuma med državami članicami o varovanju tajnih podatkov, ki se izmenjujejo v interesu EU. V letu 2011 je bil tako sprejet Zakon o ratifikaciji Sporazuma med državami članicami Evropske unije o varovanju tajnih podatkov, ki se izmenjujejo v interesu Evropske

unije. Določila sporazuma dajejo primeren okvir za varovanje nacionalnih tajnih podatkov, izmenjanih med državami članicami v interesu EU, če države članice med seboj nimajo sklenjenih dvostranskih sporazumov, obenem pa vidno in jasno vključujejo obveze, da se za tajne podatke, ki jih EU prejme od tretjih držav in mednarodnih organizacij, zagotovi ustrezna raven varovanja v državah članicah, če jim tajne podatke predložita Svet Evrope ali Evropska komisija. Seveda pa je glavni namen sporazuma obveza držav članic, da sprejmejo vse ustrezne ukrepe za zagotovitev primernega varovanja tajnih podatkov, ki jim jih predložijo Svet Evrope in Evropska komisija ter agencije EU (Zakon o ratifikaciji sporazuma med državami članicami Evropske unije, 2011).[4] Sporazum nima prednosti pred nacionalnimi zakoni in predpisi držav članic glede varovanja njihovih tajnih podatkov, dostopa javnosti do dokumentov ali varstva osebnih podatkov, niti ne vključuje usklajevanja ali približevanja zakonodaje ali predpisov na tem področju.

Pomembni za meddržavno sodelovanje sta tudi pomoč pri varnostnem preverjanju in izmenjava podatkov o dovoljenjih za dostop do tajnih podatkov. Usklajevanje in opredelitve ter stališča do posameznih vprašanj, ki se nanašajo na varovanje tajnih podatkov EU, se poleg agencij (npr. Europol, Eurojust) lahko dotikajo tudi drugih ključnih delov EU (npr. Evropskega parlamenta), lahko pa se nanašajo na posamezne projekte (npr. Projekt Galileo, FP7) ali druga področja delovanja EU (kritična infrastruktura, nabavni postopki).

Predpisi o varovanju tajnih podatkov v Republiki Sloveniji so usklajeni tudi s predpisi zveze NATO. Tajni podatki NATA ohranjajo stopnjo tajnosti podatkov, pogodbenice pa storijo vse potrebno, da jih varujejo primerno stopnji tajnosti. Zakon določa, da pogodbenice vzpostavijo in izvajajo enotne minimalne varnostne standarde, ki zagotavljajo enotno skupno raven varovanja tajnih podatkov, in da tajnih podatkov ne uporabljajo v druge namene kakor samo v tiste, ki so določeni v Severnoatlantski pogodbi, sklepih in resolucijah, nanašajočih se na to pogodbo. Države tajnih podatkov ne razkrivajo stranem, ki niso članice zveze NATO, brez soglasja lastnika podatkov

[4] *Za EU tajni podatki pomenijo vse podatke ali material v kakršnikoli obliki, katerih nepooblaščeno razkritje bi lahko v različni meri škodovalo interesom Evropske unije ali eni ali več državam članicam, in imajo eno od naslednjih oznak stopnje tajnosti EU:*

- *"TRES SECRET UE/EU TOP SECRET" za podatke in material, katerih nepooblaščeno razkritje bi lahko imelo izjemno težke posledice za vitalne interese Evropske unije ali ene ali več držav članic;*
- *"SECRET UE/EU SECRET" za podatke in material, katerih nepooblaščeno razkritje bi lahko resno škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic;*
- *"CONFIDENTIEL UE/EU CONFIDENTIAL" za podatke in material, katerih nepooblaščeno razkritje bi lahko škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic;*
- *"RESTREINT UE/EU RESTRICTED" za podatke in material, katerih nepooblaščeno razkritje bi lahko bilo škodljivo za interese Evropske unije ali ene ali več držav članic (Zakon o ratifikaciji sporazuma med državami članicami EU, 2011: 2. člen).*

(Zakon o ratifikaciji sporazuma med pogodbenicami Severnoatlantske pogodbe o varnosti podatkov, 2004).

Časovna omejitev tajnosti in postopki za umik tajnosti

Thompson (1999: 184) ugotavlja, da časovna omejenost tajnosti predstavlja pomemben korak k demokratični odgovornosti. Moynihan (1997: 65) poudarja, da je treba avtomatično omejiti čas veljavnosti tajnosti (na 10 ali 30 let), potem pa morajo varnostne agencije na osnovi ocen tveganj utemeljiti, kateri podatki morajo še ostati tajni. "Demokratični sistem tajnosti" naj bi vseboval avtomatsko deklasifikacijo tajnih podatkov po preteku dveh do treh let (Ellsberg, 2010: 798) ali pa vsaj po dvajsetih letih (Melanson, 2001).

V slovenskem Zakonu o tajnih podatkih (2006: 15. člen) je končanje tajnosti določeno s tem, da pooblaščena oseba tajnost podatka pisno prekliče, ko ni več pogojev za tajnost. O preklicu mora obvestiti vse, ki so imeli dostop do takih podatkov. Sicer pa po 18. členu tajnost podatka lahko preneha na določen datum, z nastopom določenega dogodka, s potekom določenega časa ali z zgoraj omenjenim preklicem tajnosti. Če ni določeno drugače, tajnost preneha s potekom časa, ki je določen v zakonu, ki ureja arhivsko gradivo in arhive (to v Sloveniji postane dostopno za uporabo praviloma 40 let po nastanku, razen v primerih izjem po Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih, 2006/2014). Pooblaščene osebe morajo vsako leto (za strogo tajne podatke) ali na tri leta (za ostale tajne podatke) ocenjevati, ali še obstaja potreba po njihovi tajnosti.

Tajnost podatkov pa se lahko prekliče tudi v situaciji, ko bi bil javni interes za razkritje tajnega podatka močnejši od javnega interesa za omejitev dostopa do podatka zaradi njegove tajnosti. O tem odloča vlada (Zakon o tajnih podatkih, 2006: 21.a člen).

Uredba o varovanju tajnih podatkov (2005: 30. člen) dodatno določa še postopke za uničenje tajnih podatkov, kjer je treba podatke uničiti v evidentiranem veččlanskem postopku na način, s katerim se zagotovi njihova nerazpoznavnost in neobnovljivost.

Inšpekcije kot sistemski korekcijski mehanizem

Nadzor nad izpolnjevanjem predpisov v nacionalnovarnostnem sistemu opravljajo različne inšpekcije (glej Grizold, 1999). Za učinkovitost delovanja sistema varovanja tajnih podatkov je poleg notranjega nadzora nad varovanjem pomemben tudi inšpekcijski nadzor, ki ugotavlja odklone od predvidene zaščite in nalaga popravke (kot sistemski korekcijski mehanizem). Inšpektorat za notranje zadeve in na obrambnem področju Inšpektorat za

obrambo preverjata sistem določanja, označevanja, varovanja in dostopa do tajnih podatkov. Inšpektorji morajo imeti dovoljenje za dostop do strogo tajnih podatkov, vendar nimajo pravice zahtevati vpogleda v vsebino tajnih podatkov. Inšpektorji imajo v primeru nepravilnosti pravico in dolžnost odrediti rok za odpravo pomanjkljivosti oziroma nepravilnosti, zahtevati pisna pojasnila, podati ovadbo zaradi kaznivih dejanj, predlagati uvedbo disciplinskega postopka ipd. Pristojni inšpektorat o svojih ugotovitvah poroča letno nacionalnemu varnostnemu organu (Zakon o tajnih podatkih, 2006: 42. člen). Inšpekcijski nadzor nad varovanjem tajnih podatkov EU in NATA opravljajo inšpektorji teh mednarodnih organizacij.

Mehanizmi zaščite virov, ki razkrijejo prikrita kazniva dejanja

Anonimni viri ali razvpiti žvižgači so osebe z dostopom do tajnih podatkov, ki so v preteklosti večkrat razkrivali tajne podatke. To so počeli iz različnih razlogov, med katerimi igra pomembno vlogo želja razkriti javnosti določene nezakonitosti delovanja varnostnega sistema. Problematično je namreč, če se želi nezakonite ukrepe javnosti prikriti z označevanjem ukrepov za tajne. Ellsberg (2010: 798) poudarja, da je pri oblikovanju demokratičnega sistema tajnosti (angl. *democratic secrecy system*) treba oblikovati zakonska določila o zaščiti žvižgačev in zagotoviti njihovo imunost pred pregonom v primeru javnega razkritja domnevnih ali dejanskih kaznivih dejanj. Prav tako predlaga, da bi morale biti laži s strani civilnih ali vojaških oseb na zaslišanjih v parlamentu kriminalizirane. Elwotrthyjeva (1998: 8) pa celo priporoča oblikovanje učinkovitega sistema spodbujanja in zaščite žvižgačev, saj naj bi se s tem v različnih proračunih veliko prihranilo.

V Sloveniji Zakon o tajnih podatkih (2006: 6. člen) določa, da podatek, ki mu je bila tajnost določena zato, da bi se prikrilo storjeno kaznivo dejanje, prekoračitev ali zloraba pooblastil ali prikrilo kakšno drugo nezakonito dejanje ali ravnanje, ni tajen. Kazenski zakonik RS v 260. členu določa kaznivost za izdajo tajnih podatkov. Člen, ki je veljal v začetku leta 2015, določa kazenske sankcije za uradno ali drugo osebo, ki v nasprotju s svojimi dolžnostmi varovanja tajnih podatkov sporoči ali izroči komu tajne podatke ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke, zato da jih izroči nepoklicani osebi (prvi odstavek 260. člena). Prav tako določa kazen za tiste, ki protipravno pridejo do tajnih podatkov, da bi jih neupravičeno uporabili, in tiste, ki take podatke brez dovoljenja javno objavijo (drugi odstavek 260. člena), npr. novinarje. Ministrstvo za pravosodje je v začetku leta 2015 predlagalo spremembo Kazenskega zakonika z namenom izključitve kaznivosti razkritja tajnih podatkov zaradi prevladujočega javnega interesa in povečanja zaščite svobode izražanja (v bistvu gre za delno oziroma omejeno izključitev kaznivosti). Novi predlog dodaja varovalko za

t. i. ilegalne tajnosti z določilom, da se "oseba, ki izpolni znake kaznivega dejanja iz prvega odstavka tega člena, ne kaznuje, če gre za podatek, ki razkriva očitno protipraven poseg države v človekove pravice ali temeljne svoboščine, očitne zlorabe oblasti ali pooblastil ali druge hude nepravilnosti pri izvrševanju oblasti, javnih pooblastil ali opravljanju javne službe, dejanje pa ni storjeno iz koristoljubnosti in ne ogroža življenja ljudi oziroma nima hudih ali nepopravljivih škodljivih posledic za varnost ali zakonsko varovane interese Republike Slovenije. Poleg tega se po tem predlogu ne kaznuje, kdor tajni podatek javno objavi, pridobi, posreduje ali poseduje z namenom razkritja, če glede na okoliščine primera javni interes po razkritju tajnega podatka prevlada nad javnim interesom po ohranitvi njegove tajnosti, in če z dejanjem ni neposredno ogroženo življenje ene ali več oseb" (Predlog Zakona o spremembah in dopolnitvah kazenskega zakonika – medresorsko usklajevanje, 2015). V obeh primerih dopolnil gre za izjeme in presojo o prevladi javnega interesa po razkritju tajnega podatka nad javnim interesom po ohranitvi njegove tajnosti (razmerje med svobodo izražanja oziroma tiska in potrebo po varstvu tajnosti). S tem bi se izključil kazenski pregon novinarjev in drugih oseb (npr. urednikov), ki bi v javnem interesu razkrile kazniva dejanja. Pri tem pa je treba poudariti, da je bila podobna varovalka že vgrajena v slovenski sistem varovanja tajnih podatkov v obdobju 1999–2008, poleg tega pa tudi, da tuje države večinoma nimajo takšnih varovalk.

Varnostna kultura in varovanje tajnih podatkov

Med možne vire ogrožanja tajnih podatkov štejemo tudi zaposlene, torej osebe z dostopom do tajnih podatkov. V tem smislu je pomembna varnostna kultura, ki se kot del splošne kulture posameznikov in organizacij nanaša na preventivno dejavnost v zvezi z varovanjem tajnih podatkov. Nanaša se na del organizacijske kulture, ki povzema in izgrajuje tiste vrednote posameznika, ki so bistvenega pomena za varovanje tajnih podatkov (Hartman, 2007: 90). Po Stajiču (v Hartman, 2007: 65) se varnostna kultura nanaša na zavest o nepogrešljivosti neprekinjenega, samoiniciativnega in zavestnega izvajanja varnosti. Hartman (2007: 65–67) povzema in dopolnjuje naslednja načela pri varnostni kulturi: načelo zakonitosti (varovanje tajnih podatkov skladno z zakonodajo), načelo odgovornosti (sposobnost, da posamezniki sami prepoznajo grožnje in nanje samoiniciativno odgovorijo), načelo neprekinjenosti (stalno izvajanje varovanja) in načelo pravočasnosti (pravočasna preventivna dejavnost proti virom ogrožanja). Pri varovanju tajnih podatkov je zaželeno celostno obravnavanje tehničnih, organizacijskih in človeških vidikov. Po mnenju nekaterih kar 80 % vseh varnostnih dogodkov, povezanih z varovanjem tajnih podatkov, povzroči človek (Hartman, 2007: 64).

Varnostno kulturo v Sloveniji je težko objektivno oceniti. Na splošno bi lahko rekli, da posamezniki z dostopom do tajnih podatkov dobro opravljajo svoje naloge varovanja, vendar pa se pojavljajo tudi nekatere težave (npr. občasne afere, kjer so v ozadju objavljeni tajni dokumenti), ki navajajo strokovno skupnost, da si prizadeva za zvišanje te kulture. Še posebej pomembno je izvajati dobre izobraževalne programe na tem področju.

Sklep

V uvodu je bilo zastavljeno vprašanje, v katerih primerih, na kakšen način in pod kakšnimi pogoji je dopustno določene podatke in informacije s področja nacionalne varnosti v sodobni liberalnodemokratični državi odtegniti javnosti. Besedilo je na primeru Slovenije pokazalo, da je iz varnostnih razlogov mogoče povsem legalno prikriti javnosti določene podatke, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države. Ključni kriterij za določitev tajnosti je v Sloveniji vezan na potencialno škodo v primeru razkritja. Za tajnega se tako lahko določi le podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale ali bi očitno lahko nastale škodljive posledice za varnost države ali za njene politične ali gospodarske koristi. Za ohranjanje upravičenosti ohranjanja tajnih podatkov pa mora sodobni sistem varovanja tajnih podatkov poskrbeti še za transparentne kriterije za dostopanje do tajnih podatkov, natančna pravila za hranjenje tajnih podatkov in tudi pravila za distribucijo tajnih podatkov. Večina tajnih podatkov mora biti časovno omejena, zato da se lahko javnost na določeni točki seznani s prikritimi dejstvi in morda tudi razlogi za prikritost. Ker pa je praksa po svetu pokazala na možnost zlorabe zgoraj opisanih mehanizmov, je treba zagotoviti tudi obstoj pravnih mehanizmov za zaščito virov, ki bi razkrili kazniva dejanja, prikrita s tajnimi podatki. Le s pomočjo v besedilu proučenih mehanizmov lahko sodobni sistem nacionalne varnosti ohranja svojo legitimnost pred javnostjo, ki jo mora varovati.

Popolna zaščita tajnih podatkov verjetno ni mogoča v nobeni državi, vendar pa se lahko s primernim sistemskim pristopom približamo visoki stopnji zaščite in varovanja. Analiza obstoja in razvitosti sistemskih mehanizmov varovanja tajnih podatkov v Sloveniji je pokazala, da imamo razvite mehanizme, ki odražajo celovitost pristopa na tem področju. Tudi po mnenju mednarodnih inšpekcij iz EU in NATA je aktualni sistem varovanja tajnih podatkov v Republiki Sloveniji primerno urejen in implementiran. Podana so bila sicer določena priporočila za izboljšave, ki so bila v veliki meri implementirana in ki naše države ne zavezujejo k spremembam področnega zakona. Kljub temu lahko izpostaviva številne izzive pri varovanju tajnih podatkov v Sloveniji. V nadaljevanju podajava za vsak izziv tudi osnovno priporočilo za izboljšanje stanja.

Zakonodajni in institucionalni vidiki sistema varovanja tajnih podatkov. Izziv na tem področju je, da stalno prihaja do številnih bolj ali manj celovitih pobud s predlogi sprememb zakonodaje. V zvezi s tem priporočava, da se vsaka taka pobuda presoja z vidika celovitosti urejenosti področja varovanja tajnih podatkov, pri čemer je treba pobudo povezati z ugotovitvami inšpekcijskih organov, tujimi dobrimi praksami, človekovimi pravicami, ugotovitvami medinstitucionalne razprave in tudi dejanske javne razprave.

Kriteriji za določanje tajnih podatkov. Glavni izziv na tem področju je racionalno in na predpisih temelječe določanje stopenj tajnih podatkov. Za premoščanje tega izziva bo potrebno stalno izobraževanje pooblaščenih oseb za določanje stopenj tajnosti in pogostejše uporabljanje možnosti prenehanja tajnosti po preteku določenega časa.

Kriteriji za dostopanje do tajnih podatkov. Izziv na tem področju se pojavlja pri osebah, ki lahko dostopajo do tajnih podatkov brez dovoljenja. Zanimivo je, da se na tem področju pojavljajo določene pobude (predvsem v okviru inšpekcijskih nadzorov EU in NATA ter bilateralnega sodelovanja) za spremembe v smeri zmanjšanja tovrstnih izjem. Za premoščanje tega izziva predlagava stalno usposabljanje oseb, ki lahko dostopajo do tajnih podatkov brez dovoljenja, in pa javni razmislek o možnosti pridobitve varnostnega dovoljenja.

Pravila za hranjenje tajnih podatkov. Temeljni izziv na tem področju je v konfliktu med nujnostjo nadgradnje ukrepov ter preveliko rigidnostjo podzakonskih predpisov in pravil o hrambi tajnih podatkov. V zvezi s tem priporočava spremembo teh predpisov v smeri večje vloge ocene tveganja, kar bi povečalo zmožnosti ocenjevalcev, da bolj kombinirajo različne varnostne ukrepe in s tem zmanjšajo stroške vlaganja v določene segmente varnostne opreme.

Pravila za distribucijo in izmenjavo tajnih podatkov (nacionalno in s tujino). Temeljni izziv na tem področju je hitrost izmenjave tajnih podatkov med različnimi varnostnimi organi doma in v tujini. V zvezi s tem priporočava, da se sprejmejo ukrepi za pospešitev izmenjave tajnih (in obveščevalnih) podatkov zlasti na področjih, kot je terorizem, kjer je časovna komponenta ključnega pomena.

Časovna omejitev tajnosti in postopki za umik tajnosti. Izziv v Sloveniji na tem področju je redno pregledovanje tajnih podatkov in uporaba postopka po 21.a členu zakona (ki dovoljuje preklic tajnosti v situaciji, ko bi bil javni interes za razkritje tajnega podatka močnejši od javnega interesa za omejitev dostopa do podatka zaradi njegove tajnosti). V zvezi s tem priporočava dosledno pregledovanje in evalvacijo upravičenosti tajnosti ter pogostejšo uporabo možnosti po 21.a členu zakona s strani zainteresiranih z ustrezno pobudo.

Inšpekcije kot sistemski korekcijski mehanizem. Glavni izziv na tem

področju se nanaša na premajhno pozornost že ugotovljenim pomanjkljivostim pri drugih inšpiciranih subjektih: v Sloveniji se ne učimo dovolj na napakah drugih. Zato meniva, da je treba okrepiti povezanost ugotovljenih pomanjkljivosti in nepravilnosti ter priporočil inšpekcij s procesi varnostnega ozaveščanja in izobraževanja.

Mehanizmi zaščite virov, ki razkrijejo kazniva dejanja, prikrita s tajnimi podatki. Temeljni izziv na tem področju je v vprašljivi zmožnosti žvižgača, da samostojno oceni, ali gre za dejansko razkrivanje kaznivega dejanja in ali lahko razkriva pod enakimi pogoji tudi tajne podatke EU in NATA. V zvezi s tem priporočava, da se opravi ustrezne premisleke glede žvižgaštva, glede morebitne distinkcije med nacionalnimi tajnimi podatki ter tajnimi podatki EU in NATA ter glede precedenčne sodne prakse v Republiki Sloveniji v zvezi z upoštevanjem načela sorazmernosti v tovrstnih primerih.

Varnostna kultura in varovanje tajnih podatkov. Temeljni izziv v Sloveniji v zvezi s tem je necelovit pristop k spodbujanju varnostne kulture. V tem smislu je pomembno okrepiti sodelovanje državnih organov, izobraževalnih institucij, združenj in društev novinarjev ter ostalih zainteresiranih na področju izobraževanja.

Zgoraj navedene ugotovitve omogočajo potrditev v uvodu zastavljene teze, da je Slovenija kot mlada država sistemsko dokaj celovito uredila področje varovanja tajnih podatkov, vendar pa se sooča še z nekaterimi resnimi izzivi. Tem izzivom bo treba nameniti precej pozornosti, če želimo dodatno izboljšati varovanje tajnih podatkov v Sloveniji ob sorazmernem upoštevanju pravice, da lahko vsakdo pridobi podatek ali informacijo javnega značaja. Smer razreševanja izzivov pa je bila podana s priporočili v tem članku.

LITERATURA

Anžič, Andrej (2001): Tajnost kot družbeni fenomen – varnostni vidiki. V Igor Belič (ur.), Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, 48. Ljubljana: Ministrstvo za notranje zadeve RS.

Brezovšek, Marjan in Damir Črnčec (2010): Demokratična uprava in tajnost podatkov. Ljubljana: FDV.

Clark, Robert (2004): Intelligence Analysis: A Target-Centric Approach. Washington D.C.: CQ Press.

Ellsberg, Daniel (2010): Secrecy and National Security Whistleblowing. Social Research 77 (3): 773–804.

Elworthy, Scilla (1998): Balancing the Need for Secrecy with the Need for Accountability. RUSI Journal 143 (1): 5–8.

Lerner, Lee K. in Brenda Wilmoth Lerner (ur.) (2004): Encyclopaedia of Espionage, Intelligence and Security – vol. 3. New York: Thomson – Gale.

Former Estonian High Government Official Suspected in Treason, 2008, Baltic Business News, 22. 9. Dostopno preko www.balticbusinessnews.com, 18. 11. 2008.

Uredba o varovanju tajnih podatkov (2005), Uradni list RS št. 74/2005, 5. 8.

Grabušnik, Jožef (2007): Tehnično in fizično varovanje na obrambnem področju. Specialistično delo. Ljubljana: FDV.

Grizold, Anton (1999): Obrambni sistem Republike Slovenije. Ljubljana: Visoka policijsko-varnostna šola.

Hartman, Ervin (2007): Varovanje tajnih podatkov in varnostna kultura na obrambnem področju: protiobveščevalno-varnostni vidik. Specialistično delo. Ljubljana: FDV.

Lowenthal, Mark (2003): Intelligence: from Secrets to Policy. Washington D.C.: CQ Press.

Melanson, Philip H. (2001): Secrecy Wars: National Security, Privacy, and the Public's Right to Know. Herndon: Brassey's.

Moynihan, Daniel Patrick (1997): The Culture of Secrecy. Public Interest 128: 55–72.

Predlog Zakona o spremembah in dopolnitvah kazenskega zakonika – medresorsko usklajevanje (2015), 19. 3., št. 007-96/2015, Ljubljana: Ministrstvo za pravosodje.

Resolucija o strategiji nacionalne varnosti Republike Slovenije (2010), Uradni list RS, št. 27/2010, 2. 4.

Rovšek, Jernej (2001): Dostopnost informacij javnega značaja in dopustnost omejitev z vidika ustave in varstva človekovih pravic. V Igor Belič (ur.), Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih, 35. Ljubljana: Ministrstvo za notranje zadeve RS.

Schmid, Fidelius in Andreas Ulrich (2010): Betrayer and Betrayed: New Documents Reveal Truth on NATO's 'Most Damaging' Spy. Spiegel Online. Dostopno preko http://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-693315.html, 30. 4. 2015.

Shulsky, Abram in Gary Schmitt (2003): Silent Warfare: Understanding the World of Intelligence. Washington D.C.: Brassey's Inc.

Thompson, Dennis F. (1999): Democratic Secrecy. Political Science Quarterly 114 (2): 181–193.

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (2007), Uradni list RS št. 48/2007, 1. 6.

Ustava Republike Slovenije (1991/2013), prečiščeno besedilo (vključno s spremembami, sprejetimi leta 2013), Uradni list RS, št. 33/91-I.

Vienna Document 2011 on CSBM (2011), 30. 11. Vienna: OSCE.

Zakon o ratifikaciji Sporazuma med državami članicami Evropske unije, ki so se sestale v okviru Sveta, o varovanju tajnih podatkov, ki se izmenjujejo v interesu EU (2011), Uradni list RS št. 93/11, 18. 11.

Zakon o ratifikaciji Sporazuma med pogodbenicami Severnoatlanske pogodbe o varnosti podatkov (2004), Uradni List RS št. 83/2004, 29. 7.

Zakon o tajnih podatkih (2006), Uradni list RS št. 50/2006, 16. 5., ter spremembe in dopolnitve.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (2006/2014), Uradni list RS št. 30/06 in 51/14.