*Iztok PREZELJ in Anton GRIZOLD**

RAZMERJE MED TAJNOSTJO IN JAVNOSTJO NACIONALNOVARNOSTNIH PODATKOV V SODOBNI DEMOKRATIČNI DRŽAVI**

Povzetek. *Sodobne demokratične države morajo biti transparentne in odprte do javnosti, vendar pa njihovi sistemi nacionalne varnosti lahko delujejo le na osnovi določene stopnje tajnosti podatkov, katerih razkritje bi lahko ogrozilo varnost in človeška življenja. Namen tega besedila je proučiti konceptualne vidike razmerja med tajnostjo in javnostjo na področju nacionalne varnosti ter analizirati dva ključna primera (Wikileaks in Snowden), ki dobro odražata problematičnost tega razmerja. Članek potrjuje tezo, da sta načeli javnosti in tajnosti v sodobni demokratični državi zelo pomembni, vendar mora v primeru potrebe po tehtanju med njima načeloma prevladati načelo javnosti.*

Ključni pojmi: *tajnost, nacionalna varnost, tajni podatki, javnost, transparentnost, Wikileaks, Snowden*

Uvod

Varnost je v človeški družbi postala potreba, vrednota in kulturnocivilizacijska kategorija, ki se nanaša na človekovo eksistenco in tudi na vprašanje kakovosti življenja. Spekter ogrožanja ljudi, države, družbenega sistema in mednarodne skupnosti je postal izjemno širok, saj vključuje poleg vojaških groženj še številne nevojaške grožnje, kot so kriminal, terorizem, naravne in antropogene nesreče, kibernapadi itd. Sodobne države so za odzivanje na tovrstne grožnje vzpostavile sistem nacionalne varnosti (glej Grizold, 1999). Tajnost se je na področju nacionalne varnosti uveljavila kot nujno potrebna za zaščito države, prebivalstva, suverenosti, državnega ozemlja, kritične infrastrukture ipd. Pojav tajnosti se je vedno povezoval s skrivnostnostjo, mistiko, magijo, močjo in, kot že rečeno, tudi varnostjo. Če ne bi obstajali tehtni razlogi, tajnosti nikoli ne bi bilo. Zdi se, da človeška družba v določenem omejenem obsegu želi in potrebuje tajnost. Po drugi strani pa je načelo javnosti eden od temeljnih postulatov vsake demokratične države.

* *Dr. Iztok Prezelj, izredni profesor na Fakulteti za družbene vede; dr. Anton Grizold, redni profesor na Fakulteti za družbene vede, Univerza v Ljubljani.*

** *Izvirni znanstveni članek.*

Javnost je z družbeno pogodbo pooblastila oblast, da v njenem imenu upravlja z državo. Legitimnost tega upravljanja pa je odvisna od eksplicitnega ali implicitnega pristanka javnosti. Javnost delovanja državnega in v tem okviru nacionalnovarnostnega sistema je tako v civiliziranih družbah izjemno pomembna potreba.

Tajnost je kompleksen pojav, ki vključuje potrebo in pravico države do zasebnosti in do varovanja svojih tajnosti (Brezovšek in Črnčec, 2010: 93, 101). Tako nacionalne države že dolgo označujejo občutljive podatke in informacije (ter dokumente, ki te vsebujejo) kot tajne s predpostavko, da bi njihovo razkritje nepooblaščenim osebam povzročilo škodo nacionalni varnosti. Posledično je dostop do tajnih podatkov dovoljen le osebam, ki so varnostno preverjene (imajo varnostni certifikat) in imajo t. i. "potrebo po védenju" (angl. *need to know*) (glej Shulsky in Schmitt, 2003). Kompleksnost tajnosti pa se izraža med drugim v dejstvu, da v sodobnih organizacijskih strukturah poleg formalne tajnosti obstaja še neformalna tajnost (Costas in Grey, 2014). Moynihan (1997: 57) v tem smislu navaja primere, ko zaradi izredne diplomatske ali varnostne občutljivosti tajni podatki sploh niso bili zapisani. Ugotavlja, da so tajnosti, zajete v papirnih tajnih dokumentih, bolj verjetno razkrite v javnosti na neprimeren in za nacionalne interese škodljiv način. Tak primer je bila denimo predsedniška odločitev v ZDA v času vojn na Balkanu, da ZDA ne bodo nasprotovale tajni pošiljki orožja preko Hrvaške v BIH (zelo verjetno tudi preko Slovenije in z vpletenostjo slovenskih oblasti, op. avt.). Pri konceptu tajnosti pa se je treba zavedati dejstva, da tajnost ni nekaj absolutno neznanega, temveč ravno obratno: gre za znane stvari, ki so osebam z dostopom do tajnih podatkov (posameznik, institucija ali država) zaupane v uporabo in varovanje, hkrati pa se jih ne sme ali noče narediti dostopne širši javnosti (Anžič, 2000: 852).

V sodobnih demokratičnih državah se torej pojavlja problematično razmerje med potrebo po tajnosti določenih informacij zaradi nacionalnovarnostnih razlogov (varovanje človeških življenj, državne ureditve, suverenosti ipd.) in pa potrebo po odprtosti, javnosti in transparentnosti dela organov oblasti (vključno z nacionalnovarnostnimi organi). Po eni strani morajo demokratične države delovati javnosti na očeh z visoko stopnjo transparentnosti, po drugi strani pa demokratična javnost pričakuje visoko stopnjo varnosti, ki pa je očitno ni mogoče zagotavljati brez določene stopnje tajnosti. V ta namen so države v okviru nacionalnovarnostnih sistemov oblikovale podsisteme za varovanje tajnih podatkov. Države, ki dobro varujejo tajne podatke, so v mednarodni skupnosti sprejete kot zaupanja vredni partnerji. Namen tega besedila je proučiti konceptualne vidike razmerja med tajnostjo in javnostjo na področju nacionalne varnosti ter analizirati dva primera iz prakse, ki dobro odražata problematičnost tega razmerja (Wikileaks in Snowden). Avtorja zagovarjava tezo, da sta načeli tajnosti in

javnosti v sodobni demokratični državi zelo pomembni, vendar mora v primeru potrebe po tehtanju med njima načeloma prevladati načelo javnosti. Načelo tajnosti lahko prevlada le v primerih, ko razkritje tajnih podatkov dejansko lahko povzroči ogrožanje človeških življenj in vitalnih funkcij družbe oziroma države. Prevlado načela tajnosti je potrebno presojati od primera do primera.

Proučevanja koncepta tajnosti in javnosti se je treba lotiti pazljivo, saj gre za dokaj kompleksno razmerje. V zgodovinskem kontekstu se je namreč izkazalo, da je odločitev glede tega, kaj bi moralo biti tajno (skrito) ali javno (odprto ali dostopno), stvar perspektive akterjev, ki so to presojali (Vermeir, 2012: 176). Tudi Anžič (1997) opozarja, da so multidisciplinarni pristopi, kot so sociologija, politologija, obramboslovje, pravo in psihologija, pojem tajnosti predvsem zapletali.

Struktura tega besedila je naslednja: prvo poglavje obravnava razmerje med načeloma tajnosti in javnosti. Drugo poglavje obravnava eno od ključnih težav pri uravnavanju tega razmerja, to je težavo prekomernega označevanja podatkov z visokimi stopnjami tajnosti. V tretjem poglavju pa bomo sintetično prikazali problematičnost obravnavanega razmerja na dveh praktičnih in zelo povednih primerih.

Razmerje med načeloma tajnosti in javnosti (transparentnosti) v demokratični državi

Potrebi po tajnosti na področju nacionalne varnosti in po javnosti oziroma transparentnosti države sta jasni in v literaturi dobro utemeljeni. Tajnost se razume kot odraz potrebe države po zasebnosti in intimi, demokratična država pa svojo legitimnost gradi na dejstvu, da je pravna in socialna država, ki temelji na vladavini ljudstva (Brezovšek in Črnčec, 2010: 92–93). Temeljni problem tega razmerja je, da se v literaturi večinoma interpretira kot konfliktno (glej npr. Melanson, 2001) ali dihotomno razmerje med nevidnostjo in vidnostjo oblasti (Brezovšek in Črnčec, 2010: 94). Pomembno je poudariti, da javnost namreč hkrati pričakuje oboje: javnost delovanja državnih organov in pa učinkovito zagotavljanje nacionalne varnosti. Razmerje se dodatno zapleta tudi zaradi problema dualnosti nacionalne varnosti, saj prizadevanja za varnost prebivalstva lahko hkrati tudi ogrožajo individualno varnost (glej Grizold, 1999). Tako je tudi za pojem tajnosti mogoče identificirati svojevrstno dualnost: po eni strani je fenomen tajnosti vrednota, po drugi strani pa vir "zla", če pride do odliva informacij, s katerimi se lahko ogrozijo interesi posameznikov, institucij in države (Anžič, 2000: 854).

Thompson (1999) ugotavlja, da se omenjeno razmerje večinoma prikazuje kot konflikt med tajnostjo in demokracijo. Gre za problem tajnosti v demokraciji, kar v bistvu predstavlja konflikt vrednot. Konflikt se v osnovi

nanaša na dilemo odgovornosti: demokracija zahteva publiciteto, nekatere demokratične politike pa vendarle zahtevajo tajnost. Državne politike in procesi morajo biti javni, s čimer se zagotavlja konsenz vladanih, odgovornost uradnikov itd., vendar pa nekaterih politik sploh ne bi mogli izvajati ali pa jih učinkovito izvajati, če bi jih naredili javne. Tu gre tudi za politike, ki bi jih javnost gotovo odobrila, če bi imela priložnost: npr. operacija proti narkokartelu mora biti tajna, sicer bi bila ogrožena (Thompson, 1999: 181). Thompson (1999: 183–186) se nadalje sprašuje, kaj lahko v demokratični državi naredimo v zvezi s to dilemo. Avtor ponuja tri možnosti. Prva vključuje opustitev politike, ki je tajna (še posebej, če je javnost v demokratičnem procesu ne bi odobrila). Druga možnost je opustitev demokratične odgovornosti, kar v demokraciji ni zaželeno. Pravo rešitev pa vidi v tretji možnosti, kjer se kompromisno nekoliko zmanjša tajnost, da se zagotovi minimum oz. določena stopnja demokratične odgovornosti. To pomeni, da se zagotovi ravno toliko publicitete, da lahko javnost presodi, ali je bilo vzpostavljeno pravo ravnotežje. Torej je v demokraciji tajnost upravičljiva le pod posebnimi pogoji: če je predmet oziroma subjekt demokratične odgovornosti oziroma če je upravičena v procesu, ki ni tajen. To pomeni, da tajnost prvega reda (angl. *first-order secrecy*) zahteva publiciteto drugega reda (angl. *second-order publicity*) o odločitvi, da bo neka politika ali proces tajen. Enostavneje povedano, odločitev, da bo neka politika tajna, mora biti javna. Thompson (1999: 185) priznava, da to ne deluje vedno. Problematični so primeri, ko že splošno publiciranje politike ali prakse lahko spodnese to politiko ali prakso. V tem primeru publiciteta drugega reda uniči tajnost prvega reda. Njegov sklep je, da demokratična odgovornost zahteva publiciteto, vendar pa nekatere politike in procesi vendarle zahtevajo tajnost.

Vermeir (2012) v svoji zgodovinski analizi razmerja med tajnostjo in odprtostjo prav tako poudarja, da sta bila pojma večinoma predstavljana kot nasprotna. Tajnost se je pojmovala enostavno kot pomanjkanje odprtosti (če nekaj ni odprto, potem je tajno), podobno kot pojmujemo temo kot pomanjkanje svetlobe. Vendar pa Vermeir ugotavlja, da je realnost bolj kompleksna, saj sta zgodovinsko gledano pojma celo neločljivo povezana. Z vidika razmerja med njima je pomembno, kateri je izhodiščni pojem oziroma način razmišljanja: tajnost ali odprtost. Vermeir navaja, da je bila v času Georgea Busha tajnost privilegirana, ker je dokazno breme padlo na posameznike, ki so zahtevali umik tajnosti. Po njegovem mnenju pa bi v prihodnosti moralo prevladovati načelo odprtosti in transparentnosti.

Florinijeva (1998) ugotavlja, da zagovorniki nacionalne suverenosti večinoma poudarjajo pomen skrivanja informacij, medtem ko zagovorniki transparentnosti menijo, da ta predstavlja rešitev za vse. Tajnost in transparentnost sta tudi po njenem mnenju nasprotna pojma. Tajnost se nanaša na namerno skrivanje aktivnosti, medtem ko se transparentnost nanaša na

namerno razkrivanje teh aktivnosti. Transparentnost in tajnost sta izbiri in tudi idealni stanji (oz. dva konca kontinuuma). Avtorica izpostavlja trend premika od poudarjanja tajnosti (suverenosti itd.) k transparentnosti. Ta trend je posledica demokratizacije (kjer je konsenz vladanih ključen; konsenz nima smisla, če vladani nimajo informacij), globalizacije (svet se je skrčil in konsenz mora sprejeti vedno večje število skupin in ljudi) ter tehnološkega razvoja (ki po eni strani omogoča transparentnost, po drugi strani pa omogoča tudi večjo tajnost) (Florini, 1998: 52). Trend premika k transparentnosti je tako globoka sprememba, da je na nekaterih področjih povzročila upiranje. Nekateri državni uradniki transparentnost dojemajo kot neprijetnost, paralizacijo ali celo kot neposredno grožnjo (Florini, 1998: 51). Vendar pa transparentnost po njenem mnenju ni popolna rešitev. Premik proti transparentnosti in odprtosti mora biti zelo previden. Transparentnost ima namreč naslednje težave:

- v odsotnosti univerzalno sprejetih in kompatibilnih vrednot in norm lahko konflikte še poslabšuje,
- nekatere tajnosti je treba legitimno zaščititi zaradi razlogov nacionalne varnosti in korporativne konkurenčnosti,
- razkrite informacije se lahko zlorabijo in napačno interpretirajo (transparentnost večinoma podaja informacije o védenju in ne o namenih oziroma razlogih za nekaj itd. (Florini, 1998: 60).

Bobbio (1987: 33 v Brezovšek in Črnčec, 2010: 92) govori o nevidni oblasti, ki obstaja v popolnem nasprotju z vidno ali javno oblastjo. V absolutističnih državah je prevladovalo načelo *arcana imperii* (tajnost države), saj so se ključne odločitve sprejemale v ozkem krogu vladajočih. Z oblikovanjem demokratičnih držav je bilo to načelo zamenjano z načelom javnosti, poleg tega pa je bil zastavljen cilj, da bi ideja demokracije onemogočila nevidno oblast, ki obstaja vzporedno z vidno državo. Načelo tajnosti oblasti je bilo torej v demokratičnih državah postopoma zamenjano z načelom javnosti oblasti. Koncept *res privata* pri vodenju države je bil nadomeščen s konceptom *res publica*. Tega so se zavedali tudi kasneje, v času razsvetljenstva, nato v času francoske revolucije in ob nastanku prve generacije človekovih pravic (ko se je načelo javnosti vzpostavilo kot pravica). Vendar pa je dejstvo, da sodobna demokracija ni popolnoma izničila obstoja nevidne oblasti in da si popolne javnosti delovanja ne more privoščiti niti najbolj demokratična država, saj bi s tem postala ranljiva za nedemokratične pritiske, postala bi neuspešna in neučinkovita ter kot takšna sama pomenila največjo grožnjo demokraciji (Brezovšek in Črnčec, 2010: 93).

Galison (2010) je v svoji študiji o ontologiji tajnosti ugotovil, da se je narava tajnosti spreminjala v skokih, ki so predvsem povezani z vojnami. V času prve svetovne vojne je bila tajnost vezana zlasti na nevarnost vohunjenja in

je bila časovno omejena (do konca vojne). V času hladne vojne je prišlo do spremembe v ontologiji tajnosti: jedrske tajnosti so veljale v mirnem času, poleg tega pa niso bile časovno omejene (ker jedrskega orožja nikoli ne moremo razglasiti za zastarelo). Z 11. septembrom in vojno proti terorizmu pa se je zgodil največji preskok, povezan s kritično infrastrukturo in oblikovanjem sive cone v obliki napol tajnih informacij. S terorističnim ogrožanjem se je razširil spekter infrastrukture, ki jo lahko štejemo kot potencialno tarčo (potniški vlaki, nakupovalni centri, stadioni, spomeniki itd.). Države so kritično infrastrukturo definirale kot tisto infrastrukturo, katere nedelovanje ali uničenje bi povzročilo hudo ogrožanje varnosti. Kritična infrastruktura je tako postala referenčni objekt tajnosti, kar ni bila še nikoli poprej. Poleg tega se je število kritičnih sektorjev razširilo (npr. energetika, transport, komunikacije, prehrana, oskrba z vodo itd.), kar vodi v naraščanje informacij o kritični infrastrukturi. Premik v ontologiji tajnosti je predvsem v tem, da so informacije o delovanju in ranljivosti kritične infrastrukture postale tajne (česar pred tem ni bilo) oziroma napol tajne. Po Galisonu (2010: 966) se je po 11. septembru predvsem v zvezi z informacijami o kritični infrastrukturi vzpostavil paratajni svet (angl. *para-secret world*) oziroma siva cona med odprtimi in zaprtimi informacijami. Gre za netajne, vendar občutljive informacije, kar v ZDA ponazarjajo naslednji angleški izrazi: *critical unclassified information*, *controlled unclassified information*, *sensitive security information*, *sensitive homeland security information* itd. V tem smislu pa se lahko večina državnih podatkov opredeli kot potencialno občutljivi, kar postavlja pod vprašaj idejo o odprti državi. Sullivanova (2005) se v zvezi s tem sprašuje, kako se sploh varuje občutljive, vendar netajne informacije.

Elworthyjeva (1998: 5–7) poudarja, da bo vedno obstajala napetost med nacionalnovarnostno potrebo po označevanju stopnje tajnosti podatkov ter potrebo po odgovornosti (*need for accountability*) in diseminaciji informacij v javnosti. Za Veliko Britanijo ugotavlja, da se to ravnotežje nagiba v smer tajnosti in da je odgovornost zaradi pretiranega označevanja podatkov s previsoko stopnjo tajnosti močno oslabljena. Potreba po nacionalni varnosti vodi v nujno klasificiranje določenih podatkov kot tajnih ter nedostopnih javnosti in potencialnim sovražnikom. Vendar pa je nacionalna varnost zelo ohlapno definirana in zato mnogokrat pride do upravičevanja tajnosti, ki sploh ni potrebno. Potreba po odgovornosti oziroma potreba po razkrivanju javnih informacij sta v zadnjem času trend, saj morajo odločevalci delovati v interesu prebivalstva. Javnost mora sodelovati v razpravah, kjer se sprejemajo ključne odločitve, in to vpliva na dejansko ter zaznano legitimnost države/vlade. Na prvi pogled zahteva odgovornost veliko časa in celo denarja, vendar po mnenju Elworthyjeve (1998: 7) ravno konzultiranje, transparentnost proračunov in žvižgači (angl. *whistleblowers*) v končni fazi privedejo do večje stroškovne učinkovitosti, saj prihranijo veliko denarja.

Tudi Aftergood (2010: 839) identificira dva konfliktna interesa, ki ju je bilo vedno težko usklajevati. Interes po vladni tajnosti je po njegovem nekompatibilen z interesom po demokratičnem odločanju. Tajnost po definiciji omejuje dostop do uradnih informacij, s čimer ovira sodelovanje javnosti pri odločanju in državne uradnike odvezuje odgovornosti za njihovo delovanje. Po drugi strani pa obstaja skorajda splošen konsenz, da je določena mera tajnosti upravičljiva in potrebna za zaščito avtoriziranih nacionalnovarnostnih aktivnosti, kot so denimo obveščevalna dejavnost ali vojaške operacije ipd. V zadnjem času se je pojavilo veliko kritikov državnih tajnosti (tudi organizacije, ki se borijo proti državnim tajnostim: npr. openthegovernment.org), ki menijo, da je preveč informacij označenih s stopnjami tajnosti oziroma umaknjenih od javnosti v imenu nacionalne varnosti, kar je po njihovem mnenju pripeljalo do neželenih, celo disfunkcionalnih posledic. Konkreten primer je poročilo preiskovalne komisije v ZDA po 11. septembru, v katerem je poudarjeno, da je prevelika tajnost v sistemu nacionalne varnosti ZDA ovirala horizontalno komuniciranje med agencijami in s tem po nepotrebnem poslabšala pripravljenost na grožnjo terorizma (The 9/11 Commission Report, 2004: 341). Tudi kasnejše analize mrežnega protiterorističnega delovanja so pokazale, da je domet protiterorističnih omrežij še vedno močno determiniran z razmerjem med odprtostjo delovanja različnih protiterorističnih akterjev in njihovo zaprtostjo zaradi tajnosti delovanja. Protiteroristična omrežja so lahko bolj učinkovita samo, če so bolj transparentna (glej Prezelj, 2014: 332).

ZDA predstavljajo verjetno najboljši študijski primer proučevanega razmerja med tajnostjo in javnostjo. So najbolj odprta država na svetu, saj nobena druga država dnevno ne objavlja toliko državnih informacij. Po drugi strani pa so ZDA najbolj tajna država na svetu, saj nobena druga ne proizvede toliko tajnih podatkov na dan. ZDA naj bi na leto proizvedla 3,5 milijona novih tajnosti, kar pomeni približno 10.000 tajnosti na dan (Aftergood, 2010: 841; Thompson, 1999: 181). Problem je v tem, da v ZDA količina tajnih podatkov po 11. septembru narašča. Večina jih je povezana z operacijo v Iraku in Afganistanu ter z bojem proti terorizmu (When Secrecy Hurts Security, 2005). V zvezi s tem trendom je Moynihan (1997: 59–66), nekdanji ameriški senator ter predsednik komisije za zaščito in zmanjšanje državnih tajnosti, ugotavljal, da se je v ZDA, pa tudi drugod razvila "kultura tajnosti" (angl. *culture of secrecy*),[1] ki je zmanjšala oziroma celo ogrozila demokratični proces. Ekstremen primer kulture tajnosti kot izhodišča za razmišljanje o varnosti vidi v ruskem poskusu, da bi jedrsko nesrečo v Černobilu ohranili tajno pred mednarodno javnostjo. Tajnosti po njegovem mnenju

[1] *V zvezi s tajnimi podatki se je vzpostavil sistem tajnosti, ki se vzdržuje s kulturo tajnosti (Ellsberg, 2010: 792).*

ne bo mogoče ukiniti, mogoče pa bo doseči stanje, ko tajnost in kultura tajnosti ne bosta več edina norma na področju nacionalne varnosti v ZDA. Razviti se mora kompetitivna kultura odprtosti (angl. *culture of openness*), ki bo lahko vodila do večje učinkovitosti. Kultura odprtosti je primernejša za informacijsko dobo, saj predpostavlja, da tajnost ni začetna točka razmišljanja o varnosti. Kultura tajnosti pa vodi v prekomerno označevanje tajnosti v prekomernem času (angl. *overclassification of information*), kar posledično upočasnjuje znanstveni in tehnološki napredek ter onemogoča prosto izmenjavo idej in informacij. S tem se tudi onemogoča državo, da bi bila vodilna na določenem področju. Ravno v znanosti se je uveljavilo načelo razširjanja novega in kontroverznega znanja, kar je vodilo k večjemu napredku kot kdajkoli prej. Tehnološke in znanstvene zadeve so lahko tajne, vendar ne za dolgo, saj se bodo prej ali slej tudi drugi spomnili podobnih. Moynihan (1997: 64) sklene, da potrebujemo ravnotežje med možnostjo škodovanja nacionalni varnosti in pravico do obveščenosti javnosti (angl. *right of public to know*), kaj država dela ali ne dela.

Zgornje pregledno poglavje lahko sklenemo s sintetično ugotovitvijo, da sta potrebi po tajnosti in javnosti nujni za obstoj in delovanje sodobne demokratične družbe. V njunem razmerju mora prevladovati potreba in praksa javnosti pred tajnostjo. Vendar ta asimetrija ne sme privesti do izničenja potrebe in prakse tajnosti. Tajnost je še kako pomembna za obstoj in razvoj sodobne demokratične države, če je opredeljena na ustrezen način.

Problem prekomerne uporabe tajnosti pri zagotavljanju nacionalne varnosti

Številni avtorji poudarjajo, da se v praksi preveč podatkov označuje kot tajne in da je preveč tajnih podatkov označenih s previsoko stopnjo tajnosti. Največ razlogov za takšno početje so avtorji našli v Webrovem pojmovanju birokracije. Weber je menil, da je tajnost običajen način delovanja birokracij, da se kultura birokracije ščiti s kulturo tajnosti, da moč v kulturi tajnosti pogosto temelji na zadrževanju informacij oziroma na tajnih informacijah in da ima birokracija interes po moči, ki jo ohranja s tajnostjo (Moynihan, 1997: 61–68; Weinstein, 1998/1999; Brezovšek in Črnčec, 2010: 101). S tem se uradniki tudi izogibajo javni odgovornosti (Shulsky in Schmitt, 2003; Lowenthal, 2003: 58). Poleg tega ne obstaja nobena kazen za prekomerno označevanje tajnosti, kot denimo obstaja za izdajo tajnih informacij (When Secrecy Hurts Security, 2005). V zvezi s tem je na voljo veliko pričanj iz ZDA, kjer so pretekle parlamentarne preiskave in študije pokazale, da je približno med četrtino in polovico informacij še vedno označenih s previsokimi stopnjami tajnosti. Nekdanji pomembni uradnik Pentagona William Florence je ugotavljal, da kakih pet odstotkov tajnih dokumentov dejansko upravičuje

to tajnost, po preteku dveh ali treh let pa morda samo še pol odstotka ali en odstotek dokumentov. Ellsberg (2010: 794) v zvezi s tem meni, da bi skupina neodvisnih strokovnjakov, ki bi ocenjevala velik naključni vzorec tajnih dokumentov, verjetno prišla do zaključka, da po preteku dveh ali treh let manj kot en odstotek dokumentov še zasluži oznako tajnost. Nekdanji ameriški senator Kerry je v devetdesetih letih kot član enega od odborov ugotavljal, da na stotine tajnih dokumentov, ki so jih pregledali, po njegovem mnenju ni imelo nobene tajnostne pomembnosti. Po njegovem mnenju so bili taki dokumenti klasificirani (ali pa so ostali klasificirani) kot tajni zgolj zaradi skrivanja negativnih političnih informacij (Moynihan, 1997: 57). Podsekretar za protiobveščevalno dejavnost in varnost na ameriškem ministrstvu za obrambo pa je ugotavljal, da je verjetno polovica Pentagonovih tajnosti označena s previsoko stopnjo tajnosti (When Secrecy Hurts Security, 2005). FBI in CIA ter druge agencije naj bi uporabljale označevanje dokumentov s stopnjo tajnosti za prikrivanje napak in neprimernega vedenja (Melanson, 2001). Nekdanji predsedujoči združenemu obveščevalnemu odboru v Veliki Britaniji je ugotavljal, da je nenehno gledal dokumente s previsoko določeno stopnjo tajnosti. Njegova razlaga za to so bili dnevni delovni pritiski in občasna želja, da bi se izognili neprijetnostim. Pozval je k intenzivnemu prizadevanju za povečevanje javne dostopnosti do dokumentov (Elworthy, 1998: 7).

Zastavlja se vprašanje, kakšne so posledice prekomerne ali previsoke stopnje tajnosti v sodobnih državah. Ključna posledica je, da države hranijo ogromne količine tajnih podatkov, s čimer so povezani visoki stroški njihovega varovanja. Poleg tega pa to negativno vpliva na taktično in strateško učinkovitost varnostnih agencij, kar se je potrdilo z napadom 11. septembra 2001 (When Secrecy Hurts Security, 2005). Thompson (1999: 191) v tem smislu omenja institucionalno hinavščino (angl. *institutional hypocrisy*), kjer gre za očiten razkorak med dovoljenimi in dejanskimi aktivnostmi. Po Schulskyju in Schmittu (2003) nastajajo zaradi tega posledice za legitimnost ukrepov in varnostnega sistema. Poleg tega pa je prevelika količina tajnosti povzročila paranoiden odnos državljanov do države (Weinstein, 1998/1999), ki se najbolj izraža v številnih teorijah zarote (in celo fantazijah zarote), po katerih agencije, ki bi morale javnost ščititi, to dejansko ogrožajo (Moynihan, 1997: 61).

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 objavljajo raziskovalci, ipd. (glej Shulsky in Schmitt, 2003).

Očitno je torej, da se pravica države do tajnosti v imenu nacionalne varnosti uporablja ter tudi prekomerno uporablja in zlorablja. Zato ni čudno, da takšna koncentracija moči sama povzroča svoj antipol moči v obliki

razkrivanja in objavljanja vsebine tajnih dokumentov. Veliko se lahko naučimo s študijami posameznih ekstremnih primerov iz prakse.

Nekateri primeri iz prakse

V praksi se je pojavilo več primerov, ki vsak posebej izpostavljajo razmerje med potrebo po tajnosti določenih informacij zaradi nacionalnovarnostnih razlogov (varovanje človeških življenj, državne ureditve, suverenosti ipd.) ter potrebo po odprtosti, javnosti in transparentnosti dela organov oblasti. V tem besedilu se bomo osredotočili na dva tuja primera (Wikileaks in Snowden). Oba skupaj kažeta, da se svet tajnosti pri svojem ohranjanju moči sooča s svojevrstnim antipolom moči, ki se izraža skozi omrežje naslednjih akterjev:

- anonimni viri ali razvpiti žvižgači (večinoma inteligentni posamezniki z dostopom do tajnih podatkov),
- mediji, ki prenašajo tajne informacije v javnost in v imenu transparentnosti tudi iščejo tajne informacije, ki bi utegnile odražati nezakonito ali nepravilno delovanje nacionalnovarnostnega sistema, ter
- globalno organizirano omrežje Wikileaks, ki sistematično zbira in objavlja tajne podatke, povezane predvsem z ZDA in posledično z veliko drugimi državami po svetu.

Primer Wikileaks

Kaj je razkril? Wikileaks se je pojavil leta 2010 in takoj pritegnil pozornost globalne javnosti z objavljanjem največje količine tajnih dokumentov v človeški zgodovini. Na svojih spletnih straneh je, med drugim tudi s pomočjo Bradleyja (danes Chelsea) Manninga, nekdanjega obveščevalnega analitika, objavil serije ameriških tajnih dokumentov, med katerimi imajo najvidnejšo vlogo (glej Sledge, 2013):

- objava videoposnetka "Collateral Murder", v katerem ameriški helikopter strelja na skupino neoboroženih civilistov v Iraku, ob čemer vojaki vidno uživajo. Med žrtvami sta bila tudi dva novinarja agencije Reuters. Reuters tega posnetka po uradni poti od Pentagona ni mogel pridobiti;
- objava okrog 400.000 ameriških vojaških tajnih poročil iz Iraka, ki so privedla do zvišanja ocen o žrtvah te vojne;
- objava okrog 75.000 ameriških tajnih dokumentov iz Afganistana, ki so pokazali bistveno bolj temačno sliko vojne, kot jo je poznala javnost;
- objava tajnih dokumentov iz Guantanama, ki so pokazali, da ne obstaja veliko razlogov za pridržanje zapornikov;
- objava tajnih dokumentov o zakulisnem sodelovanju med ZDA in nekaterimi arabskimi diktatorji;

- objava 251.287 tajnih depeš ameriškega zunanjega ministrstva in veleposlaništev z vsega sveta.

Objavljene depeše denimo vključujejo razkritje vohunjenja ZDA za svojimi zavezniki in OZN, razkritje korupcije turškega predsednika, interesnih povezav med Berlusconijem in Putinom, tajnega načrta zveze NATO za zaščito Baltika in Poljske pred Rusijo (Zaščitniški orel) itd. Za Slovenijo je bila denimo razkrita hudo obremenjujoča obveščevalna direktiva, ki določa ameriške prioritete v zvezi z vohunjenjem v naši državi. Razkrito je bilo tudi, da je ameriško jedrsko orožje nameščeno v štirih evropskih državah – v Belgiji, Nemčiji, Turčiji in na Nizozemskem (Phillips, 2010).

Vodja Wikileaksa je Julian Assange, ki je "hektivist" – mešanica političnega aktivista in hekerja. Wikileaks ni klasična organizacija, ampak je v bistvu omrežje posameznikov z enakimi cilji. Tajne podatke Wikileaks objavlja na svojih spletnih straneh in v sodelovanju z nekaterimi močnimi medijskimi hišami, ki pa pri tem sodelovanju igrajo tudi lastno interesno igro.

Motivi za razkrivanje tajnih podatkov. Poslanstvo Wikileaksa je, da ohranja odprtost držav (glej Secret US Embassy Cables, 2010*)* in da poskuša široki javnosti priskrbeti enciklopedijo tega, kako velike obveščevalne, diplomatske in obrambne institucije delujejo, zato da lahko ljudje po vsem svetu načrtujejo svoje poteze v razmerju do teh institucij. Assange tudi meni, da javnosti omogočajo bežen vpogled v *modus operandi* ameriških oblasti, kar daje priložnost manjšim državam. Assangea moti tudi znanje, ki je namerno prikrito in izključeno iz javnega prostora. Meni, da je prikrivanje znanja pogosto povezano z neko krivico in da bi z njegovim razkritjem lahko zmanjšali celotni obseg krivic. Assangeev namen je "biti vohun za ljudi" in Wikileaks je v tem smislu "obveščevalna služba za ljudi". Potrebo po taki službi vidi Assange v dejstvu, da imajo države obveščevalne službe, ki vohunijo za ljudmi in jih nadzirajo. Assange označuje svoje cilje kot metapolitični program. Zaveda se tudi, da je Wilileaks s takimi cilji grožnja oblasti (Assange, 2013). Motiv Manninga, ki je odigral vlogo vira, pa je bil v želji, "da ljudje vidijo resnico, saj brez teh informacij javnost ne bi mogla sprejemati ustreznih odločitev" (Kako je prišlo do razkritja diplomatskih depeš?, 2010).

Posledice v zvezi z razmerjem med tajnostjo in javnostjo. Sam Assange meni, da tovrstna razkritja tajnosti omajejo avtoriteto institucij. "Ko njihova dejanja postanejo dostopna javnosti, se jih ne bojimo več; nenadoma jih uziramo v vsej njihovi bedi in napihnjeni aroganci, pomešani z neumnostjo" (Assange, 2013). Pri analizi posledic je treba najprej pogledati odziv ameriškega političnega in varnostnega sistema na razkritje. Wikileaks je spodkopal avtoriteto ameriškega nacionalnovarnostnega sistema, ki je udaril nazaj. Različni predstavniki ameriških oblasti so javno grozili Wikileaksu, da ga bodo uničili, poleg tega pa so Assangea razglašali za: državnega sovražnika

in grožnjo nacionalni varnosti, vohuna, terorista, kriminalca, ki je podoben Osami bin Ladnu in za katerega je treba doseči smrtno kazen, itd. Wikileaks je celo pridobil zaupne dokumente o tem, kako bodo obveščevalne službe napadale in spodkopavale Wikileaks. Načrti vključujejo tudi metode ustrahovanja virov, pošiljanje lažnih oziroma ponarejenih dokumentov itd. (Assange, 2013). Rusija pa je pozvala k resnemu razmisleku o tem, da bi Assangea predlagali za Nobelovo nagrado (Rusija za Nobelovo nagrado Assangeu, 2010).

Assange še vedno biva na sedežu ekvadorskega veleposlaništva v Veliki Britaniji, ker je za njim razpisana mednarodna tiralica švedskih oblasti zaradi domnevnih posilstev.[2] Bradley (Chelsea) Manning je bil obsojen na 35 let zapora. V sodnem procesu so ga želeli prikazati kot vohuna in psihopata. Po drugi strani pa vojaki strelci iz omenjenega razkritega videoposnetka niso doživeli niti disciplinskih postopkov, saj so delovali v skladu s pravili dejstvovanja.

Javna razprava o primeru Wikileaks kaže razdvojenost: Assangea in Manninga so nekateri označevali za heroja, drugi pa za izdajalca. Postavljalo se je vprašanje, ali so depeše res v interesu javnosti ali pa gre v veliki meri zgolj za neodgovoren ekskluzivizem, ki utegne imeti zelo škodljive posledice. Kritični mediji so se denimo spraševali, kaj bo, če zaradi objav izbruhne vojna med Saudovo Arabijo in Iranom (Bild), Le Figaro pa je menil, da je množično objavljanje tajnih dokumentov znamenje načrtne zlonamernosti in zaskrbljujoč ekshibicionizem ter da si brez minimalne diskretnosti in zaupanja ni mogoče predstavljati prizadevanj za svetovni mir niti reševanja konfliktov (V imenu globalne kritične javnosti, 2010). Predstavniki vlade so govorili o veliki škodi, vendar pa je javno niso želeli konkretizirati. Zagotovo so se poslabšali odnosi med ZDA in partnerji (vključno z zahodnimi partnerji in tudi z Rusijo), zaupanje v ameriški multilateralizem je ohromljeno, nekatere države so intenzivirale protiobveščevalno in tudi obveščevalno dejavnost itd. Po poročanju Rettmana (2010) so nekateri strokovnjaki kot posledico izpostavili, da se vsak tajni dokument zdaj lahko obelodani preko Wikileaksa, tudi papirni dokumenti se lahko poskenirajo in objavijo na internetu.

Primer Snowden

Kaj je razkril? Edward Snowden je bil zaposlen v NSA (National Security Agency), CII (Central Intelligence Agency) in pri pogodbenih podjetjih, ki so delala za NSA. Na svojem delovnem mestu na Havajih je pričel

[2] *Tudi nekdanji informacijski pooblaščenki v RS, Nataši Pirc Musar, se je zdelo absurdno, da je bila za Assangeom razpisana kar mednarodna tiralica zaradi suma storitve posilstva (glej Zaradi suma posilstva mednarodna tiralica? Absurdno!, 2010).*

z zbiranjem tajnih dokumentov o ameriškem nadzorovanju komunikacij v ZDA in tujini, ki ga je izvajala NSA. Shranjeval je dokumente, ki so po njegovem mnenju odražali sporne posege v človekovo zasebnost. Te dokumente je razkril junija 2013, ko sta jih začela objavljati The Guardian in Washington Post. Snowden je razkril tajne podatke o naslednjih programih NSA:

- nediskriminatorno zbiranje metapodatkov o telefonskih klicih in kontaktih od vseh telekomunikacijskih operaterjev v ZDA (na osnovi sodne odločbe), čemur sledi podatkovno rudarjenje in analiza klicnih vzorcev (Greenwald, 2013);
- PRISM pridobiva podatke od Googla, Facebooka, Yahooja, Appla in drugih. Nekateri dokumenti kažejo, da ima NSA neposredni dostop do njihovih strežnikov, kar pa so podjetja zanikala;
- programi za razdiranje internetne enkripcije (npr. internetno bančništvo ipd.), prizadevanje za oslabitev enkripcijskih internetnih standardov, prizadevanje za ohranjanje odprtih stranskih vrat v različne enkripcijske programe (Ball, Borger in Greenwald, 2013);
- dnevno zbiranje SMS-sporočil;
- prisluškovanje optičnim kablom po vsem svetu itd.

Motivi razkrivanja tajnih podatkov. Snowden je po prihodu v izgnanstvo na moskovskem letališču pojasnil svoje motive za izdajo tajnih podatkov. Glavni motiv je bil v tem, da obvesti javnost, kaj se dogaja v njenem imenu in proti njej. Želel je ozavestiti ljudi, da jih ameriška vlada nadzoruje, s čimer krši ustavo in zakone ter njihove pravice. Upal je, da bodo objave sprožile višjo stopnjo zavedanja o nadzoru, ki ga izvaja vlada ZDA. Snowden je tudi pokazal, da se je za ta korak odločil po skrbnem premisleku glede posledic in glede tega, kdaj imajo državljani demokratične države moralno in politično dolžnost kršiti zakon. Pri tem koraku se je odrekel zasebnemu življenju, vključno z dobro plačano službo, v zameno za javno dobro. Najprej je upal, da bo novo ameriško politično vodstvo (predsednik Obama) preklicalo nekatere prakse, ki jih je po 11. septembru uvedel predsednik Bush, vendar se to ni uresničilo. Poleg tega se je o tem pogovarjal s svojimi nadrejenimi, ki pa tudi niso odreagirali, saj v NSA nihče ne dojema teh programov kot problematične (Scheuerman, 2014).

Posledice v zvezi z razmerjem med tajnostjo in javnostjo. ZDA so Snowdnu preklicale potni list in ga uvrstile na seznam prepovedi letenja. Posledično ga ni želela sprejeti nobena država razen Rusije, kamor se je tudi zatekel. Javne razprave o tem so prav tako odrazile razdeljenost. Nekateri so Snowdna označili za heroja, ki je razkril, da programi NSA predstavljajo resno kršitev zakonov ter četrtega in petega amandmaja k ameriški ustavi, poleg tega pa tudi kršitev Univerzalne deklaracije o človekovih pravicah. Veliko predstavnikov vlade in tudi javnosti pa ga je označilo za izdajalca,

žvižgača in vohuna. Nekateri so ga označili za obstranca s talentom za samopromocijo, ki ni naredil tako velike škode. Ameriški predsednik Obama in britanski premier David Cameron sta ugotovila, da je Snowden s svojimi dejanji ljudi izpostavil nevarnosti ter izzval možnost terorističnih napadov (Scheuerman, 2014). Večinoma pa se je govorilo o veliki škodi, ki je javno nihče ni želel ali znal opredeliti.

Objava tajnih dokumentov je povzročila izgubo zaupanja v internetne in telekomunikacijske ponudnike v ZDA. Razkrita je bila tudi laž direktorja NSA Jamesa Clapperja pred ameriškim senatom, ko je dobil vprašanje, ali zbirajo kakršnekoli informacije o Američanih. Clapper je odgovoril, da jih ne zbirajo. Kasneje se je opravičeval, da je njegov odgovor moral biti takšen, ker je bil povprašan o zaupnih informacijah, ter da je pomešal zunanje in notranje delovanje NSA (Papandrea, 2013: 467). Nekdanji ameriški obrambni minister je pozval Snowdna, naj se vrne v ZDA in se sooči s posledicami, če ga resnično zanima razkritje nepravilnosti v NSA (Papandrea, 2013: 484). Britanska obveščevalna služba GCHQ, ki tesno sodeluje z NSA, je po objavi tajnih dokumentov pritisnila na The Guardian. Zahtevali so njihovo uničenje in The Guardian je v izogib tožbam to tudi storil.[3] Afera je vplivala tudi na odnose med ZDA in zavezniki, še posebej Nemčijo, saj se je izkazalo, da je NSA redno prisluškovala telefonskim pogovorom številnih nemških politikov, vključno z Angelo Merkel.

Sklep

V uvodu tega članka smo izpostavili problematično razmerje med načeloma ali potrebama po tajnosti in javnosti v sodobni demokratični državi. Analiza literature o tem razmerju in o problemu prekomernega označevanja s stopnjo tajnosti na področju nacionalne varnosti ter študiji dveh empiričnih primerov so pokazali, da sta obe načeli pomembni za sodobno demokratično državo, vendar mora v primeru potrebe po tehtanju med njima praviloma prevladati načelo javnosti. Izhodišče pri upravljanju sodobne države in sistema nacionalne varnosti mora biti načelo javnosti, medtem ko lahko načelo tajnosti prevlada le v primerih, ko razkritje tajnih podatkov dejansko lahko povzroči ogrožanje človeških življenj in vitalnih funkcij družbe oziroma države. Uporabo načela tajnosti je potrebno presojati od primera do

[3] *Britanska vlada je večkrat zagrozila časopisni hiši The Guardian, da mora vrniti dokumente, ki jih je razkril Snowden. Do medija so prišla sporočila, da bo vlada to dosegla zlepa ali zgrda (po pravni poti). Prav tako je do medija prišlo sporočilo, da mnogi v vladi razmišljajo, da bi The Guardian kar "ukinili". Tako so se v medijski hiši odločili, da pod nadzorom predstavnikov obveščevalne službe uničijo vse računalnike, ki so vsebovali tajne podatke, ki jih je razkril Snowden. Po mnenju novinarjev je bilo to simbolično in nadrealistično dejanje, saj so vsi vedeli (vključno z britansko vlado), da na nerazkritih lokacijah obstajajo še nekatere druge kopije istih tajnih podatkov (Harding, 2014).*

primera, poleg tega pa bi se moral vzpostaviti sistem vsebinskega nadzora glede pravilnosti določitve stopnje tajnosti.

Analiza konceptualnega razmerja in prakse je pokazala na videz paradoksalno situacijo, kjer večina avtorjev pojmuje omenjeno razmerje kot konfliktno, hkrati pa javnost od države pričakuje delovanje na osnovi javnosti in transparentnosti ob hkratnem uspešnem zagotavljanju varnosti, kar vključuje tudi uporabo mehanizmov tajnosti. To pomeni, da je imperativ organiziranega življenja v sodobni družbi in državi uravnoteženo zagotavljanje tako varnosti države kot tudi zaščite osebnih podatkov in svobode ljudi. Bolj konkretno, sodobna politična država je pri zagotavljanju nacionalne varnosti dolžna spoštovati in prakticirati javno in odgovorno delovanje državnih organov. Razreševanje tega (navideznega) konfliktnega razmerja med varnostno vlogo institucionalnega okvira države in javnostjo (oziroma med tajnostjo in demokracijo) pa je v današnjih razmerah kompleksnega ogrožanja zapleteno.

Obravnava dveh konkretnih primerov razkritja tajnih podatkov v javnosti je opozorila na problem prekomerne uporabe instituta tajnosti državnih organov pri zagotavljanju nacionalne varnosti. Javno dostopni (prej tajni) podatki so le potrdili obstoječe bojazni javnosti o delovanju državnih organov pri izvajanju funkcije nacionalne varnosti, prav tako pa so okrepili zavedanje javnosti o potrebi po stalnem javnem nadzoru nad njihovim delovanjem. Tovrstna prekomernost ima tudi negativne implikacije za legitimnost sodobne države.

Obravnava razmerja med javnostjo in tajnostjo v demokratični državi tudi kaže, da vsak pol moči v družbi (v našem primeru tajna država, ki temelji na kulturi tajnosti) avtomatično privede do oblikovanja antipola moči, ki ga v sodobnem svetu predstavljajo omrežje anonimnih virov (v nekaterih primerih so to žvižgači), mediji, ki prenašajo tajne podatke do javnosti, in globalno organizirano omrežje Wikileaks. Assange in Snowden sta postala Robina Hooda sodobne informacijske družbe. Oba sta se obrnila proti ZDA, državi z najmočnejšim sistemom nacionalne varnosti, ki proizvede največ tajnosti na časovno enoto. Oba želita omejiti moč tajne države in njun skupni motiv je obveščanje in zaščita javnosti. Assange se ima celo za vohuna za ljudi. Zanimivo pa je tudi to, da sta oba primera naletela na razdvojen odziv javnosti: za nekatere gre za junaško početje, drugi pa ju označujejo za izdajalca, vohuna in grožnjo nacionalni varnosti.

Kako naj se torej sodobna država sooči s potrebo po zagotavljanju ustreznega razmerja med javnostjo in tajnostjo delovanja? Ključno priporočilo tega besedila je, da mora sodobna država pri zagotavljanju nacionalne varnosti sistemsko urediti obe potrebi in njuno medsebojno razmerje. To pomeni, da mora oblikovati sistem varovanja tajnih podatkov, ki deluje v okviru sistema nacionalne varnosti, poleg tega pa mora delovanje "tajne

države" urediti tako, da bo omogočen stalen javni demokratični nadzor (strokovni, politični in pravni) nad vsakokratno uporabo tajnosti v praksi. Še posebej moteče je, da pretekla škandalozna razkritja tajnih podatkov niso nedvoumno pokazala, kakšno škodo je utrpela nacionalna varnost, država ali družba. Dokazi o škodljivosti razkritij morajo preiti okvire teoretičnih domnev. Le v tem primeru bo civilna družba dejansko razumela nujnost obstoja tajnih podatkov.

LITERATURA IN VIRI

Aftergood, Steven (2010): National Security Secrecy: How the Limits Change. Social Research 77 (3): 839–852.

Anžič, Andrej (1997): Varnostni sistem RS. Ljubljana: Uradni list RS.

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

Ball, James, Julian Borger in Glenn Greenwald (2013): Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security. The Guardian, 6. 9. Dostopno preko http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, 2. 5. 2015.

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

Costas, Jana in Christopher Grey (2014): Bringing Secrecy into the Open. Organization Studies 35 (10): 1421–1447.

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.

Florini, Ann (1998): The End of Secrecy. Foreign Policy 111 (Summer): 50–63.

Galison, Peter (2010): Secrecy in Three Acts. Social Research 77 (3): 941–974.

Greenwald, Glenn (2013): NSA Collecting Phone Records of Millions of Verizon Customers Daily. The Guardian, 6. 6. Dostopno preko http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, 2. 5. 2015.

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

Harding, Luke (2014): Footage Released of Guardian Editors Destroying Snowden Hard Drives. The Guardian, 31. 1. Dostopno preko http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq, 2. 5. 2015.

Kako je prišlo do razkritja diplomatskih depeš? (2010). Delo, 1. 12.: 7.

Krečič, Jela (2013): Julian Assange: Wikileaks smo vohuni za ljudi. Sobotna priloga Dela, 7. 12. Dostopno preko http://www.delo.si/zgodbe/sobotnapriloga/julian-assange-wikileaks-smo-vohuni-za-ljudi.html, 1. 5. 2015.

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.
Papandrea, Mary-Rose (2013): Leaker Traitor Whistleblower Spy: National Security and the First Amendment. Boston Universtiy Law Review 94 (2): 449–544.
Phillips, Leigh (2010): Four European States Host US Nuclear Bombs. EUobserver.com, 29. 11.
Prezelj, Iztok (2014): Inter-organizational Cooperation and Coordination in the Fight against Terrorism: From Undisputable Necessity to Paradoxical Challenges. Comparative Strategy 33 (4): 321–341.
Rettman, Andrew (2010): EU Officials Give First Analysis of Wikileaks Impact. EUobserver.com, 3. 12.
Rusija za Nobelovo nagrado Assangeu (2010). Delo, 10. 12.: 32.
Scheuerman, William E. (2014): Whistleblowing as Civil Disobedience: The Case of Edward Snowden. Philosophy and Social Criticism 40 (7): 609–628.
Secret US Embassy Cables (2010). Dostopno preko www.wikileaks.ch, 6. 12. 2010.
Shulsky, Abram in Gary Schmitt (2003): Silent Warfare: Understanding the World of Intelligence. Washington D.C.: Brasseys Inc.
Sledge Matt (2013): Bradley Manning Uncovered U.S. Torture, Abuse, Soldiers Laughing as They Killed Innocent Civilians. Huffingtonpost.com, 21. 8. Dostopno preko http://www.huffingtonpost.com/2013/08/21/bradley-manning-leaks_n_3788126.html, 2. 12. 2014.
Sullivan, Eileen (2005): Homeland Security Reconsiders Secrecy Policy. Federal Times, 10. 1.: 9.
The 9/11 Commission Report: The Full Final Report of the National Commission on Terrorist Attacks upon the United States (2004). National Commission on Terrorist Attacks Upon the United States, Washington D.C.
Thompson, Dennis F. (1999): Democratic Secrecy. Political Science Quarterly 114 (2): 181–193.
V imenu globalne kritične javnosti (2010). Delo, 1. 12.: 6.
Vermeir, Koen (2012): Openness versus Secrecy? Historical and Historiographical Remarks. British Society for the History of Science 45 (2): 165–188.
Weinstein, Allen (1998/1999): The Cult of Secrecy. The National Interest (Winter): 95–97.
When Secrecy Hurts Security (2005). Defense News, 14. 3.: 95–97.
Zaradi suma posilstva mednarodna tiralica? Absurdno! (2010). Novice 24 ur.com. Dostopno preko http://www.24ur.com/novice/slovenija/zaradi-suma-posilstva-mednarodna-tiralica-absurdno.html, 2. 12. 2014.

analysis of the newspaper part of the Gigafida corpus, a reference corpus of Slovenian (for the period 2000–2009). Among other things, we found that several forms of reference automatism *from a reliable source (we learnt)* have formed part of Slovenian news reporting for almost 150 years and that, in the last decade, two automatisms have mostly been used, i.e. *according to our information* and *according to unofficial information*. Surprisingly, the automatism *rumour has it* is very common as well.

Keywords: journalist, automatism, unnamed source of information, in-depth interviews, corpus, language stylistics

UDK 355.405.1:316.77

Iztok PREZELJ and Anton GRIZOLD: THE RELATIONSHIP BETWEEN THE SECRECY AND TRANSPARENCY OF NATIONAL SECURITY DATA IN A CONTEMPORARY DEMOCRATIC STATE
Teorija in praksa, Ljubljana 2015, Vol. LII, No. 4, pg. 670–686

Contemporary democratic states have to be transparent and open to society, yet their national security systems need to operate based on a certain level of secrecy. The purpose of this text is to analyse the conceptual aspects of the relationship between secrecy and transparency in the field of national security and to study two key cases (WikiLeaks and Snowden) that reflect this relationship well. The paper confirms the argument that the principles of transparency and secrecy are very important in a democratic state, although when there is a need for prioritisation the principle of transparency should prevail.

Keywords: secrecy, national security, secret data, public, transparency, WikiLeaks, Snowden

UDK 355.405.1:355.02(497.4)

Iztok PREZELJ and Milan TARMAN: THE CLASSIFIED INFORMATION PROTECTION SYSTEM IN SLOVENIA FROM THE PERSPECTIVE OF THE DEMOCRATIC PROVISION OF NATIONAL SECURITY
Teorija in praksa, Ljubljana 2015, Vol. LII, No. 4, pg. 687–706

The threat of the illegal disclosure of classified information requires every modern state to create an efficient protection system. Classified information protection demands a comprehensive approach that goes far beyond narrow system thinking. This article defines the concept of a comprehensive