Univerzitet u Beogradu

Terorizam, organizovani kriminal i bezbednost

Master rad

PRAVNI ASPEKTI TAJNOSTI I ZAŠTITE TAJNIH PODATAKA U REPUBLICI SRBIJI

Mentor:

Prof. dr Dragan Simeunović

Student:

Veljko Porobić 189/2016

Beograd, 2017.

PRAVNI ASPEKTI TAJNOSTI I ZAŠTITE TAJNIH PODATAKA U REPUBLICI SRBIJI

Zahvalnica

Zahvaljujem se svom mentoru prof. dr Draganu Simeunoviću na podršci i pomoći u izradi master rada, kao i na znanjima iz oblasti politike i bezbednosti koja sam usvojio od njega.

Zahvalnost dugujem i dr Goranu Matiću koji mi je pomogao u pribavljanju literature i omogućio saradnju sa Kancelarijom Saveta za nacionalnu bezbednost i zaštitu tajnih podataka koja je doprinela da ideje ovog rada budu konkretnije i ozbiljnije.

Sažetak

Tajnost je višedimenzionalan fenomen koj je prisutan u mnogim segmentima čovekovog postojanja. Njena primena u savremenom informacionom društvu i državnoj sferi mora biti pravno regulisana. Između pojedinca, države i društva se razmenom i upotrebom mnoštva podatka stvaraju odnosi koji su rezultat težnje ka ostvarivanju različitih interesa svakog od subjekata. Svaki od interesa, uobličava se i može da se imenuje određenim pravom. Pravo na zaštitu podataka o ličnosti, pravo na slobodan pristup informacijama u posedu organa javne vlasti i pravo da se određeni podaci označe kao tajni i izuzmu od slobodnog pristupa čine trijadu pravne regulative u oblasti podataka i informacija. Cilj svakog pravnog sistema je da propiše norme koje omogućavaju prisustvo i ostvarivanje svakog od ovih interesa u korisnoj meri ali i da se spreče zloupotrebe koje u mogu imati ozbiljne posledice po osnovne postulate demokratskog poretka i nacionalne bezbednosti. Komplementarnost prava koja predstavljaju ove interese, dokazivanje potrebe otklanjanja manjkavosti postojeće regulative i izgradnja posebnih stručnih tela za rad sa tajnim podacima predstavljaju osnovne ideje ovog rada.

Cilj rada odnosi se na naučnu deskripciju i klasifikaciju pravnih i društvenih aspekata fenomena tajnosti. Osim toga, u određenim segmentima, primenjeno je naučno objašnjenje pozitivnopravnih rešenja kojima se uređuje primena tajnosti podataka u Republici Srbiji uz ukazivanje na njihove manjkavosti, pravne praznine i razmatranje mogućih rešenja postojećih nedostataka regulative u ovoj oblasti.

Ključne reči: tajnost, podaci, nacionalna bezbednost, pravni sistem, organi javne vlasti.

Abstract

Confidentiality is a multidimensional phenomenon present in many areas of human life. The way it is used in the modern information society and the state sector should be subject to legal regulation. The exchange and use of the profusion of information among individuals, the state and society create relationships which are the result of efforts to serve the various interests of all parties involved. Each of these interests is shaped by and may be consigned to a particular right. The right to the protection of personal information, the right to free access to information held by public authorities and the right to designate certain information as confidential and exempt from free access make up a triad of legislation in the field of data and information. The goal of any legal system is to prescribe standards which enable the representation and actualization of each of these interests to a useful degree, and to prevent abuses which may have serious consequences for the basic tenets of democratic order and national security. The complementarity of the rights which represent these interests, a demonstration of the need to remedy deficiencies in existing regulations and the formation of special professional bodies to deal with confidential information are the basic ideas of this study.

The aim of this paper is a scientific description and classification of the legal and social aspects of the phenomenon of confidentiality. In addition, in certain areas, a scientific explanation is given of positive legal solutions regulating the confidentiality of data in the Republic of Serbia, with an indication of their deficiencies and legal shortcomings and a consideration of possible solutions for the current lack of regulations in this field.

Keywords: confidentiality, data, national security, legal system, public authorities

Biograija

Veljko Porobić, rođen 22.11.1988. godine u Beogradu. Nakon završene osnovne škole i Treće beogradske gimnazije 2007. godine upisuje Pravni fakultet. Na drugoj godini studija se opredeljuje za pravosudno- upravni smer. Po uspešnom okončanju studija koje je završio sa prosečnom ocenom 8,8 počinje da radi u Auto-moto klubu Novi Beograd (AMSS) na poslovima formiranja novog sektora povezanog sa pravnom strukom i oblastima bezbednosti. Na Fakultetu političkih nauka u Beogradu 2013. godine uspešno pohađa specijalistički program inovacije znanja - Antikorptivne veštine, a naredne godine upisuje master program Terorizam, organizovani kriminal i bezbednost na Univerzitetu u Beogradu. Učesnik je Međunarodnog debatnog turnira (Belgrade open 2013) kao i više seminara o bezbednosti saobraćaja. Govori engleski i francuski jezik i aktivan je član sportskih udruženja.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Student: Veljko Porobić,

Broj indeksa: 189/2016

Student: master akademskih studija Terorizam, organizovani kriminal i bezbednost

Autor master rada pod nazivom: Pravni aspekti tajnosti i zaštite tajnih podataka u Republici Srbiji

Potpisivanjem izjavljujem:

- da je rad isključivo rezultat mog sopstvenog istraživačkog rada;
- da sam rad i mišljenja drugih autora koje sam koristio u ovom radu naznačio ili citirao u skladu sa Uputstvom;
- da su svi radovi i mišljenja drugih autora navedeni u spisku literature/referenci koji su sastavni deo ovog rada i pisani u skladu sa Uputstvom;
- da sam dobio sve dozvole za korišćenje autorskog dela koji se u potpunosti/celosti unose u predati rad i da sam to jasno naveo;
- da sam svestan da je plagijat korišćenje tuđih radova u bilo kom obliku (kao citata, prafraza, slika, tabela, dijagrama, dizajna, planova, fotografija, filma, muzike, formula, veb sajtova, kompjuterskih programa i sl.) bez navođenja autora ili predstavljanje tuđih autorskih dela kao mojih, kažnjivo po zakonu (Zakon o autorskom i srodnim pravima, Službeni glasnik Republike Srbije, br. 104/2009, 99/2011, 119/2012), kao i drugih zakona i odgovarajućih akata Univerziteta u Beogradu;
- da sam da sam svestan da plagijat uključuje i predstavljanje, upotrebu i distribuiranje rada predavača ili drugih studenata kao sopstvenih;
- da sam svestan posledica koje kod dokazanog plagijata mogu prouzrokovati na predati master rad i moj status;
- da je elektronska verzija master rada identična štampanom primerku i pristajem na njegovo objavljivanje pod uslovima propisanim aktima Univerziteta.

Beograd, 15.01.2017.

Potpis studenta _____

S A D R Ž A J

UVOD 2
1. TAJNI PODACI I POTREBA PRAVNE REGULATIVE 4
2. POJAM TAJNOG PODATKA/INFORMACIJE 10
2.1. Podatak/informacija 10
2.2. Pojam tajnosti 13
3. (ZLO)UPOTREBA TAJNIH PODATAKA 17
4. TAJNI PODATAK U DEMOKRATSKOM OKRUŽENJU 23
5. TRANZICIJA TAJNOSTI 28
5.1. Dilema otvaranja tajnih dosijea. 32
6. JAVNOST PROTIV TAJNOSTI, SLUČAJ SRBIJA 37
6.1. Tripartitni test 41
7. ZAKON O TAJNOSTI PODATAKA REPUBLIKE SRBIJE- OTVORENA PITANJA.. 46
7.1. Podatak koji se može odrediti kao tajni. 50
7.2. Ko i kako stvara tajne podatke? 55
7.3. Pristup tajnim podacima 61
7.4. Nadzor i kontrola nad primenom zakona 66
8. KANCELARIJA SAVETA ZA NACIONALNU BEZBEDNOST I ZAŠTITU TAJNIH PODATAKA 70
9. ZAKLJUČAK 75
LITERATURA 77

Popis korišćenih skraćenica

EU- European Union

GPS- Global Positioning System

INFOSEC- Information Security

IPAP- Individual Partnership Action Plan

ISO- International Organization for Standardization

NATO- North Atlantic Treaty Organization

NCSA- National Syber Security Authority

NDA- National Distribution Authority

NDR- Nemačka Demokratska Republika

NSA- National Security Agency

NSA- National Security Authority

SAA- Security Accreditation Authority

SAD- Sjedinjene Američke Države

SFRJ- Socijalistička Federativna Republika Jugoslavija

SRJ- Savezna Republika Jugoslavija

SSSR- Savez Sovjetskih Socijalističkih Republika

TEMPEST- Telecomunications Electronics Material Protected from Emanating Spurious Transmissions

USA FOI ACT- United States Freedom of Information Act

USA PATRIOT ACT- Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorisn Act of 2001.

UVOD

Tajnost je višedimenzionalan fenomen sa kojim se čovek susreće od ranog detinjstva. Ona je pre svega društvena pojava, jer je društvo okvir u kome se ona ostvaruje i vrši svoju funkciju. U dodiru sa sferom politike i političkog, ova pojava dobija novu dimenziju koja se odslikava kroz susretanje naizgled suprotstavljenih interesa, zaštićenih pravnim normama, u pravnom i bezbednosnom okviru jedne države. Propisivanjem pravnih normi vrši se direktan uticaj na usmereavanje različitih interesa u društvu. Od kvaliteta normi zavisi kako će biti rešen susret i preklapanje različitih interesa, odnosno njihov sukob u jednom pravnom sistemu.

Država označavanjem određenih podataka i informacija kao tajnih vrši svoje pravo, koje za cilj ima zaštitu njenih vitalnih interesa, iskazanih kroz pojam nacionalne bezbednosti. Sa druge strane, vršenjem ovog prava država ograničava druga prava koja sama garantuje ustavom i potpisanim međunarodnim pravnim aktima. Ovakav susret prava na slobodan pristup informacijama u posedu organa javne vlasti i potrebe zaštite vitalnih interesa države, oličene u pravu da se određeni podaci izuzmu od uvida (što je omogućeno sistemom zaštite tajnih podataka) stvara specifičan pravni problem procene pretežnosti interesa koji zahteva duboku pravnu analizu i stručnost prilikom njegovog rešavanja.

Osnovna ideja ovog rada je analiza navedenog pravnog problema, uz pomoć primene metoda analize i sinteze (objašnjavaju se i sistematizuju postojeće pravne norme (*de lege lata*)). Tumačenjem i analizom postojećih pozitivnopravnih rešenja i stručnih tekstova ukazuje se na manjkavosti domaćeg zakona koji reguliše ovu oblast, a uporednopravnom analizom i analizom međunarodno prihvaćenih principa u ovoj oblasti ukazuje se na potencijalno adekvatna rešenja koja su prisutna u funkcionalnim pravnim sistemima drugih država.

Rad je podeljen na osam poglavlja koja se mogu svrstati u dve celine. Prva objašnjava pojam tajnog podatka i okvir u kome on funkcioniše, susret sa transparentnošću i probleme država u tranziciji. Druga se bavi analizom pozitivnopravnih normi u Srbiji. Strukturu rada čine poglavlja: Uvod- Upoznavanje stručne i laičke javnosti sa pravnim aspektima tajnosti i zaštite tajnih podataka u Republici Srbiji, njihovim nedostacima i mogućim adekvatnijim rešenjima određenih pitanja. Prvo poglavlje- Objašnjenje značaja informacija i potrebe pravnog regulisanja sfere podataka i informacija u savremenom društvu. Drugo poglavlje - Analiza osnovnog pojma kojim se bavi ovaj rad raščlanjivanjem sintagme „tajni podatak“ na njene

sastavne delove i njihovim objašnjenjem. Treće poglavlje- Prikaz prednosti i mana tajnih podataka u savremenoj državi i opis upotrebe i zloupotrebe odnosnog fenomena. Četvrto poglavlje- Objašnjenje odnosa tajnosti i demokratskog uređenja. Opis funkcionisanja tajnih podataka u okviru demokratski uređene države. Peto poglavlje- Analiza dva osnovna pravna problema vezana za tajnost podataka u državama u procesu tranzicije, pa i u Srbiji. Prvi je nastao kao odraz primene savremenih pravila o tajnosti podataka i njihovog susreta nasleđenim tajnim podacima iz vremena nedemokratskih vlada, a drugi je pitanje otvaranja tajnih dosijea kao aktuelne i politizovane teme u domaćoj javnosti. Šesto poglavlje- Pravni odnos dva Ustavom i zakonima zagarantovana prava (prava na slobodan pristup informacijama od javnog značaja i prava na izuzimanje određenih podataka iz sfere javnih informacija. Prikaz funkcionisanja prava na informaciju u domaćem pravnom sistemu i primene tripartitnog testa, kao i problema u primeni i tumačenju postojeće regulative. Sedmo poglavlje- Analiza domaćeg Zakona o tajnosti podataka kroz opis i kritku određenih najbitnijih normativnih rešenja ovog zakona. Pregled problema koji nastaju u primeni pozitivnih normi i poređenje sa sličnim rešenjima u drugim pravnim sistemima uz predstavljanje hipotetički mogućih rešenja na osnovu sinteze opisanih pravila. Osmo poglavlje– Prikaz postojeće organizacije Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka kao stručne službe Vlade, analiza nedostataka takvog rešenja i pravnih nedoslednosti pozitivnih normi u domaćem pravnom sistemu i opis drugačijeg modela ustrojstva nacionalnog tela za rad sa tajnim podacima na osnovu uporednopravne analize.

Republika Srbija je nakon politički turbulentnog perioda, koji je bio izuzetno težak po sve sfere društva, krenula u izgradnju funkcionalnog pravnog sistema, čiji je veoma bitan segment pravna regulativa koja se odnosi na tajnost podataka. Kao i svi počeci, početak normiranja jedne važne oblasti je težak posao koji zahteva određenu praksu i vreme kako bi postigao odgovarajući kvalitet. Cilj ovog rada je upoznavanje šire javnosti sa postojećim rešenjima domaćeg pravnog sistema u oblasti tajnih podataka i njihove zaštite, uticaja na druga prava i potencijalnih manjkavosti ovih normi. Kako je trenutno u radu stručna radna grupa koja ima za zadatak da predloži izmene i dopune Zakona o tajnosti podataka ili čak da izradi model novog zakona, analiza manjkavosti postojećih normi bi mogla poslužiti i stručnom delu javnosti.

1. TAJNI PODACI I POTREBA PRAVNE REGULATIVE

Svedoci smo vremena u kome je teško zamisliti da bilo šta prođe nezapaženo. Danas smo u mogućnosti da budemo u toku sa dešavanjima sa drugog kraja planete u veoma kratkom roku. Informacije kruže u ogromnom broju i neverovatnom brzinom. Mogućnost da se dođe do informacija je znatno proširena u odnosu na ne tako davnu prošlost. Promena načina života i rada, napredak informacionih tehnologija, sredstava komunikacije, masmedija, tehike, uslovili su da broj podataka koji je dostupan bude veći nego ikad u istoriji. Pristupačnost i količina informacija je tolika da bi se o savremenom društvu moglo govoriti kao o informacionom društvu .[1]

„ Svi mi naime, svakodnevno dajemo drugima informacije o sebi i drugima i svi mi od drugih dobijamo informacije o sebi i drugima. Od kad je čoveka, on je oduvek morao biti informaciono bića, samim tim što nije sam na svetu...ali danas nismo svi mi samo informaciona bića, što smo oduvek bili nego danas i bivstvujemo u tzv. Informacionom društvu." (Vodinelić, 2012, p. 18).

Svaki pojedinac bi se u takvom društvu prepunom informacija mogao odrediti kao svojevrstan prijemnik i odašiljač podataka. Savremeni građanin barata sa mnogo podataka koje saznaje, ali istovremeno i daje brojne podatke akterima sa kojima stupa u kontakt u svakodnevnom životu. Posmatrano iz perspektive jedne informacije, njeno postojanje, zastupljenost i neophodnost u savremenom društvu dovodi do njene široke eksploatacije u različitim sferama života. Fenomen koji zauzima ovoliki prostor i ima neprocenjiv značaj za funkcionisanje čitavog sistema današnjice zahteva izradu pravnih pravila, koja na jasan način propisuju granice njegove korisne upotrebe. Zastupljenost različitih interesa u širokom polju delovanja jedne informacije čini je složenim objektom pravne regulative, koja zahteva ozbiljno razmatranje iz više perspektiva kako ne bi dolazilo do kolizije prilikom susreta različitih interesa, odnosno kako bi bilo omogućeno efikasno rešavanje svih spornih situacija.

Pojave koje su obeležile proteklih dvadesetak godina uticale su na promenu obima brojnih prava i shvatanja njihove suštine. Globalizacija, koja je prisutna kao proces, pored uticaja na društvo izvršila je i snažan uticaj na shvatanje tradicionalnog pojma države i njenih funkcija,

[1] Pojam prof. dr Vladimira Vodinelića

pa samim tim i položaja građana i njihovog odnosa prema državi i njenim institucijama. Promocija građanskih prava i sloboda je postala centralno pitanje demokratskog poretka. Ovaj trend u pojedinim segmentima neretko ide do te mere da se pretvara u svoju suprotnost.

Brojnost i lak način saznavanja informacija uz razvoj zagarantovanih ljudskih i građanskih prava povezanih sa ovom pojavom uslovili su da oblast podataka i informacija mora biti pravno regulisana. Kako je informacija širok pojam, jasno je da regulisanje njenog toka, upotrebe, zabrane ili ograničavanja zahvata mnoge segmente pravnog sistema. Ipak, centralno pitanje je susret prava na obaveštenost i dostupnost informacija i ograničavanja tog prava do koga dolazi kada se informacije kojima se štite interesi nacionalne bezbednosti označe kao tajne. Svaka zabrana ili ograničavanje zagarantovanih prava izaziva kontroverze i brojne polemike, ali i izradu jasnih pravila po kojima se takvo ograničavanje prava vrši.

Kao što pojedinac vrši svojevrsnu sopstvenu klasifikaciju podataka i informacija sa kojima dolazi u kontakt (trudi se da neke sazna, spozna, upotrebi ili zadrži za sebe), slična stvar se dešava šire posmatrano na nivou društva odnosno države. U svom radu organi javne vlasti prikupljaju i obrađuju veliki broj podataka koje klasifikuju na određeni način. To su najrazličitije informacije koje za potrebe svog rada državni organi prikupljaju i drže u svom posedu. Po prirodi stvari, državni organi će svakako uvek raspolagati sa više informacija nego sam pojedinac, odnosno civilno društvo. Ta činjenica daje moć državnim organima, ali onu moć koja im je neophodna da rade u javnom interesu, što je i njihova osnovna funkcija. Građani, koji se u demokratskom društvu pojavljuju kao nosioci suvereniteta i poreski obveznici, moraju biti informisani o radu svojih predstavnika kojima su poverili vršenje vlasti, kako bi mogli formirati svoju političku volju, kroz procenu i kontrolu rada onih koje su slobodno birali na izborima. Na taj način se kroz pravo pristupa informacijama od javnog značaja ostvaruje svojevrsna kontrola rada organa javne vlasti. Pravo na pristup ovim informacijama u posedu organa javne vlasti je promovisano kao jedno od ljudskih prava, koje je pretpostavka funkcionalnih i demokratskih institucija. Otvorenost i transparentnost rada, naročito organa izvršne vlasti je jedna od osnovnh pretpostavki za uobičajenu komunikaciju organa vlasti sa građanima odnosno civilnim društvom.

" Osnov građanskog društva je slobodan pojedinac.. dva najvažnija pokazatelja civilnog društva su ljudske i građanske slobode i slobodna privreda..." (Marković, 2008, p. 453).

Značaj ovog prava ogleda se i u tome što je ono zagarantovano mnogim dokumentima o ljudskim pravima univerzalnih i regionalnih međunarodnih organizacija, kao i nacionalnim ustavima. Ustav republike Srbije (Službeni glasnik RS, 98/2006), u članu 51. u okviru prava na obaveštenost prepoznaje i pravo na slobodan pristup informacijama od javnog značaja.

Pored prava koje garantuje pristup informacijama koje poseduju organi javne vlasti postoji i pravo državnih organa da određene podatke izuzmu od obaveze prezentovanja javnosti, ako se proceni da bi time bili narušeni vitalni interesi države. Da bi uspešno obavljala svoju bezbednosnu funkciju, država mora zaštiti određene informacije koje se odnose na najvažnije nacionalne interese, kako bi ih zaštitila od ugrožavanja (Grčić, 1979). Odraz takve potrebe je pravo da se takve informacije, koje se odnose na nacionalnu bezbednost, označe kao tajne i izuzmu od prava na slobodan pristup. Ovakvo pravo, koje je u stanju da ograniči drugo je uvek u centru pažnje, naročito od strane onih čija se prava time ograničavaju, a to su u ovom slučaju građani i njihove organizacije. Prednost jednog interesa nad drugim je osetljivo pravno pitanje koje mora biti odmereno na pravedan i legitiman način. Kod primene tajnosti zaštita nacionalne bezbednosti se pojavljuje kao pretežniji interes od prava na slobodan pristup informacijama i stoga dozvoljava izuzetak od pravila. Ovo je polje gde se susreću zagarantovana građanska prava, politika i bezbednost. Složenost susreta ovakvih interesa podrazumeva opsežnu pravnu analizu kao neophodan segment prilikom normativnog uređivanja ove oblasti.

Međunarodni standardi u oblasti bezbednosti i prava na informaciju podrazumevaju da ograničenje međunarodno garantovanog i ustavnog prava bude propisano zakonom i neophodno u demokratskom društvu radi zaštite legitimnog interesa (najčešće definisanog kroz pojam nacionalne bezbednosti).

Bezbednost je s toga nezaobilazan okvir, kada se radi o primeni mera zaštite tajnih podataka od strane organa javne vlasti. Kao potvrda toga je i stav da se pod merama bezbednosti, pored proglašenja vanrednog ili ratnog stanja, mera pripravnosti, mera mobilizacije, smatraju i mere zaštite tajnih podataka[2] (Mijalković, 2011).

[2] Ovaj stav deli i dr Goran Matić direktor Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.

Kako je bezbednost stanje kome prirodno teži svako, od pojedinca do saveza država, reč je o širokom pojmu koji se može odnositi na mnoge sfere a čije ugrožavanje isto tako može imati najraznovrsnije oblike i modele. Ovakav sveobuhvatan pojam, brojni faktori ugrožavanja vitalnih interesa koji se štite i primena različitih mera za njihovu zaštitu su već sami po sebi pogodno tle za mogućnost zloupotrebe samog pojma i namensko proširivanje ili sužavanje njegovog obima u cilju ostvarivanja najrazličitijih nelegitimnih i nelegalnih interesa. Ovaj rizik izražen je kroz mogućnost da se podaci o zloupotrebama označe kao tajni i time zaklone javnosti. Ovo je uzrok što ova oblast izaziva toliko polemika i nedoumica u gotovo svakom društvu. Pitanje tajnosti podataka je polje, gde se najčešće spore predstavnici civilnog društva i države. Prvi, neretko, u preteranim zahtevima za transparentnošću iz različitih pobuda i apriori negativnom stavu prema tajnosti i drugi često prenaglašavanjem potreba zaštite interesa države i insistiranjem na potrebi zatvorenosti organa javne vlasti kao faktoru povećanja bezbednosti.

Ravnoteža između ovih potreba je ono što predstavlja demokratski princip. Rad državnih organa treba da bude transparentan do one mere dok to ne počne da ugrožava druge vrednosti i osnove funkcionisanja same države kao političke organizacije društva koja je okvir u kome se ostvaruje funkcionisanje institucija, zaštita ljudskih prava i sloboda te na taj način demokratskih vrednosti i principa uopšte. Kako se upotrebom tajnosti ograničavaju građanska prava zagarantovana najvišim pravnim aktima kako država tako i univerzalnih i regionalnih međunarodnih organizacija, uobičajeno je da se u takvim slučajevima pri regulisanju ovih odnosa na nacionalnom nivou poštuju određeni međunarodni principi i preporuke.

Pored toga što savremena država podrazumeva postojanje funkcionalnog pravnog sistema uopšte, može se primetiti da je izrada kvalitetnih zakona u oblasti regulisanja tajnosti podataka bitna iz dva razloga. Prvi je taj što se na taj način štiti nacionalna bezbednost, a drugi je taj što je upotreba tajnosti u sferi politike i bezbednosti pitanje koje je veoma osetljivo i podložno zloupotrebi pa se kvalitetnom regulativom koja omogućava različite načine kontrole štiti i demokratski poredak. Ograničavanje prava na slobodan pristup informacijama, preko koga se vrše brojne kontrolne funkcije bitne za demokratsko društvo, zahteva jasna i nedvosmislena pravila kako se i kada primenjuje tajnost.

Savremeni trend u državama koje su prošle ili su još uvek u procesu tranzicije i njihova težnja ka evropskim i evroatlantskim integracijama uslovili su unifikovanje ove procedure po ugledu

na NATO i EU sisteme u kojima se takva regulativa već pokazala kao uspešna. To podrazumeva obiman rad na reformi javnog sektora u celini, a naročito organa izvršne vlasti (u okviru njih, organa koji su nosioci sistema bezbednosti) u cilju sprovođenja takvih normativnih rešenja.

Između pojedinca, države i društva se razmenom i upotrebom mnoštva podatka stvaraju odnosi koji su rezultat različitih interesa svakog od subjekata. Svaki od pomenutih interesa, uobličava se i može da se imenuje određenim pravom. To su: 1) pravo na zaštitu podataka o ličnosti; 2) pravo na slobodan pristup informacijama od javnog značaja; 3) pravo da se određene informacije proglase tajnim i izuzmu od pogleda neodređenog kruga lica.

Jedna ista informacija se može naći u objektivu interesa različitih subjekata, pa je neophodno odrediti potencijalne sporne slučajeve i artikulisati pravna načela po kojima bi se svaka takva situacija rešila na pravedan, legitiman i legalan način. Uređenost društva podrazumeva izvesnost, a ona se ogleda u tome koliko su pojave i dešavanja u njemu regulisani normama. Informaciono doba i informaciono društvo zahteva jasan stav i pravila: Ko? Šta? I kako može, i treba da zna. *„Kao informaciono biće u informacionom društvu, svako od nas živi i kreće se u jednom informacionom trouglu: između informacija od javnog značaja, tajnih informacija od javnog značaja i informacija o ličnosti...Ako su u jednom društvu sve tri strane informacionog trougla normativno definisane, tj. Ako su sva tri prava priznata i uređena tada čovek živi u svetu relativne informacione izvesnosti"* (Vodinelić, 2012, p. 19).

U Srbiji je ova oblast bila dugo vremena uređena nizom raštrkanih pravila uglavnom podzakonske snage. Ovakva situacija stvarala je brojne probleme prvenstveno između državnih organa jer su građani u velikoj meri bili isključeni iz uvida u rad javnih službi. Nakon 2000. godine započelo se sa reformama u oblastima na koje se ova regulativa odnosi. Donošenjem i pripremanjem regulative polako, ali sigurno uređuje se veoma važno pitanje podataka i informacija u Srbiji. Zakon o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009 i 36/2010), Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012), Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009), trenutno je u radu radna grupa zadužena za izmene i dopune ovog zakona, Zakon o elektronskim komunikacijama (Službeni glasnik RS, 44/2010, 60/2010, 60/2013-odluka US i 62/2014), Zakon o informacionoj bezbednosti i Nacionalna strategija sajber bezbednosti su propisi u

pripremi. Ovim se nastoji da se kompletira i uobliči pravni okvir neophodan za obezbeđivanje informacione izvesnosti.

Zakonom o tajnosti podataka (Službeni glasnik RS, 104/2009) unifikovana su pravila o označavanju tajnih podataka, čime je formalno onemogućeno da svaki državni organ označava kao tajne podatke koje hoće i kako hoće. Ova regulativa, još uvek mlada, susrela se sa brojnim problemima već u samom nastanku. Postojanje brojnih manjkavosti je očigledno, ali se u narednom periodu mogu očekivati razrada i poboljšanja koja treba da idu sve dok se ne dobije jedna jasna, skladna, efikasna i međusobno usklađena pravna regulativa u celokupnoj sferi podataka i informacija.

2. POJAM TAJNOG PODATKA/INFORMACIJE

Država propisivanjem pravnih normi prinudno usmerava određene društvene odnose ili pojave i na taj način ih oblikuje i usmerava u željenom pravcu. Zakonski tekstovi u uvodnim članovima definišu pojmove kojima se zakon bavi, kako bi se izbegle nedoumice oko njihovog eventualnog različitog definisanja i tumačenja. Definisanje pojma predstavlja određenje pojma u formalnopravnom i materijalnopravnom smislu.

Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009), u članu 2. stav 2. definiše tajni podatak: *„Tajni podatak je podatak od interesa za Republiku Srbiju koji je zakonom, drugim propisom ili odlukom nadležnog organa donesenom u skladu sa zakonom, određen i označen određenim stepenom tajnosti;"*

Iz ove definicije saznaje se samo da je to podatak, koji je na osnovu zakona i odluke nadležnog organa označen kao tajni. Ovakvo određenje karakteristično za pravnički jezik, teško može čitaocu suštinski da da odgovor na pitanje šta je to tajni podatkak. Iz tog razloga, akademska analiza svakog pojma zahteva da se uz prethodni osvrt na prirodu pojave i efekte, koje ona izaziva u realnosti pokuša odrediti pojam u materijalnopravnom smislu, u cilju njegovog šireg sagledavanja, razumevanja i fokusiranja na ona pitanja, koja predstavljaju tačke dodira i preklapanja različitih interesa, čije postojanje je motiv i osnov za nastank normi koje regulišu datu pojavu.

2.1. Podatak/informacija

U raščlanjivanju sintagme "tajni podatak", prvo treba dati odgovor na pitanje šta se sve može smatrati podatkom. Formalnopravno, odgovor na to se obično nalazi u uvodnim članovima zakonskih tekstova, koji kao predmet regulative imaju podatak ili informaciju. Tako npr. Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012), u članu 3. stav 1. daje odrednicu:
„Podatak o ličnosti je svaka informacija koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski medij i sl.)... ili bez obzira na drugo svojstvo informacije (u daljem tekstu: podatak)"

Zakon o tajnosti podataka Republike Hrvatske (Narodne Novine,79/07, 86/12), u članu 2. stav 1. definiše pojam na sledeći način: *„Podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika"*

Zakon o tajnosti podataka Bosne i Hercegovine (Službeni glasnik Bosne i Hercegovine, 54/05) član 4. stav 1. : *„ Tajni podatak je činjenica ili sredstvo koje se odnosi na javnu bezbjednost, odbranu, spoljne poslove ili obavještajnu i bezbjednosnu delatnost Bosne i Hercegovine, koji je potrebno, u skladu sa odredbama Zakona, zaštiti od neovlašćenih lica i koji je ovlašćenolice označilo oznakom tajnosti."*

Poređenjem ovih nekoliko odredbi vidi se da zakonodavci u navedenim slučajevima ili proširuju pojam podatka taksativno nabrajajući šta sve on podrazumeva, ili ga poistovećuju sa pojmom informacije. Ovo možda sa teoretske strane nije najprikladnije, ali je praktično zbog izbegavanja nedoumica, koje mogu nastati u tumačenju ova dva pojma, kao i mešanjem značenja ovih pojmova sa njihovim pojavnim oblicima odnosno njihovim nosačima (dokument, audio, video zapis, fleš memorija i drugi.). Kada se dva pojma koriste paralelno, neophodno je najpre odrediti značenje svakog od njih, kako bi se ustanovili njihov obim i značenje.

„O značaju opšteg pojma informacija govori činjenica da je od pre nekoliko godina utvrđen međunarodnim standardom ISO/IEC 2382.... Prema njemu, informacija se izjednačava sa znanjem koje se odnosi na objekte, kao što su činjenice, događaji, stvari, procesi ili ideje, uključujući i koncepte, a koje u određenom kontekstu ima posebno značenje." (Milenković, 2010, p.19).

Ovakva definicija informacije ukazuje na to da se radi o širem pojmu, odnosno da je pojam podatka neraskidivo vezan za pojam informacije, upravo time što podatak predstavlja sastavni deo informacije, odnosno njen osnovni deo. Obradom podataka nastaje informacija i ona predstavlja znanje o nečemu. Kao takva, ona ima svoju vrednost koja je u direktnoj zavisnosti od prethodnog znanja primaoca informacije, što pojam informacije čini kompleksnim, dajući mu subjektivni i objektivni element (Parezanović, 1995, pp.15-17).

U Zakonu o tajnosti podataka (Službeni glasnik RS, 104/2009), u uvodnim članovima koji se bave utvrđivanjem pojmova, pojam tajnog podatka je definisan kroz formulaciju da je to "*podatak od interesa za Republiku Srbiju*". A podatak od interesa za Republiku Srbiju je definisan kao "*podatak ili dokument kojim raspolaže organ javne vlasti a koji se odnosi na teritorijalni integritet i suverenost, zaštitu ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalnu i javnu bezbednost, odbranu, unutrašnje poslove i spoljne poslove;"*
Primetno je da ovde izostaje konkretnije objašnjenje samog pojma podatak.

Nije sporno da podatak, kao osnovni element informacije može imati takvu važnost da je neophodno da bude označen određenim stepenom tajnosti, ali će se i u tom slučaju tajnost iskoristiti u cilju sprečavanja povezivanja podataka i njihove obrade, što bi već za rezultat imalo informaciju.

Analizom pravnih normi, koje regulišu tajnost u državama sa dugom tradicijom i praksom u ovoj oblasti (prvenstveno misleći na Sjedinjene Američke Države, Ujedinjeno Kraljevstvo i Kraljevinu Švedsku), može se zaključiti da se u pravnim aktima ovih država koristi pojam informacija kao generički pojam, koji podrazumeva svaki vid činjenica i saznanja, posredno ili neposredno vezanih za nacionalnu bezbednost, a koji bi obuhvatio svakako i pojam podatka.
Američka predsednička uredba 13526
(https://www.whitehouse.gov/the-press office/executive-order-classified-national-security-information) definiše tajnu klasifikaciju informacija od značaja za nacionalnu bezbednost, određujući da tu spadaju informacije koje su u posedu, pod kontrolom, ili su nastale od strane Vlade Sjedinjenih Država, taksativno nabrajajući oblasti na koje se informacija može odnositi da bi mogla biti predmet klasifikacije.

Upotreba pojma podatak u domaćoj zakonodavnoj praksi, koja reguliše ovu oblast-Zakon o tajnosti podatka (Službeni glasnik RS, 104/2009), Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012), dolazi najverovatnije iz prakse upotrebe ovog pojma u srpskom jeziku, a koji sam po sebi, u govoru, ima šire značenje od onoga koje mu daje akademska definicija pojma i stručni prilaz strogog razgraničavanja značenja pojmova.

2.2. Pojam tajnosti

Kod analize pojma tajnosti mora se uzeti u obzir da se radi o vrlo složenom, višedimenzionalnom pojmu, čija primena u praksi organa javne vlasti predstavlja vrlo osetljivo pravno i političko pitanje. Za početak, treba razgraničiti, da li se o tajnosti i njenoj primeni govori u akademskom smislu, sa aspekta struke, ili se radi o kolokvijalnom pristupu, koji je često prisutan na dnevnopolitičkoj sceni i sa kojim javnost ima više kontakta, jer se preko medija plasira i koristi kao sredstvo političke propagande, neretko u cilju napada i rušenja kredibiliteta određenih važnih državnih institucija, ili vlada u celini. Zbog složenosti samog pojma i osetljivosti koje njegova primena stvara kao i negativnog prizvuka stvorenogslučajevima njegove zloupotrebe, tajnost je pojam vrlo pogodan za manipulaciju i pogrešnu interpretaciju.

U daljem tekstu pokušaćemo da analizom pojma izdvojimo neke njegove bitne karakteristike i utvrdimo njegovu višestranu prirodu, značaj u praksi savremene države, ali i nedostatke, potencijalne opasnosti i posledice koje mogu nastati njegovom upotrebom u sferi politike i društva.

Tajnost je fenomen koj je prisutan u mnogim sferama čovekovog postojanja i koji ima odraz na gotovo svim društvenim poljima (psihološkom, sociološkom, političkom, pravnom). Svaki pojedinac možda ne zna šta je državna tajna, ali nema onoga ko nije imao na ličnom planu susret sa tajnom. Još u ranom periodu života čovek stiče svest da je postojanje neke tajne i njeno čuvanje nešto važno, nešto što daje moć ili učvršćuje određeni odnos. Da bi tajna postojala, imala smisao, neophodno je postojanje minimum dve individue, -one koja nešto skriva, i druge od koje se skriva. Uslov i okvir za postojanje tajne je društvo, pa se može reći da je to društvena pojava. Tajnost podrazumeva postojanje određenog društvenog odnosa i gotovo uvek sa sobom nosi mogućnost uticaja na taj odnos. Čovek je po prirodi radoznao, teži saznanju, ali istovremeno oseća potrebu za svojom privatnošću. Psihološki se ta potreba za saznanjem pojačava kada je u svesti prisutno da je nešto tajno, odnosno namerno sklonjeno od spoznaje. Dodatno interesovanje prouzrokuje sumnja da se prikriva, nešto što se može okarakteristati kao loše, sa etičkog aspekta. Istina je da su loši i nemoralni postupci u najvećem broju slučajeva prikriveni i da je tajnost čest pratilac ovakvog ponašanja i radnji, ali ne bi se moglo reći da je to nekakav uslov ili apsolutna pretpostavka ovog fenomena. *„Razumljivo je gledište po kome su tajne po prirodi negativne i diskreditujuće; mnoge*

otkrivene tajne su usadile strah. Strah od zavera, osveta, nepopravljivih posledica otvaranja pandorine kutije " (Bok, 1983, p. 8).

„*Tajnost nije nužno povezana sa zlom, ali zlo jeste sa tajnošću. Iz očiglednih razloga nemoral se prikriva čak i kada ga ne prati nikakva sankcija"* (Simmel, 1906, p.453).

Ovako negativno određen pojam tajnosti i njegova dokazana prisutnost izaziva kontroverze na polju unutrašnje politike. Zbog toga javnost želi da sazna što više informacija, u strahu da se zloupotrebom tajnosti od građana skrivaju greške administracije, protivpravna ponašanja ili pogrešni politički potezi vlada. Ovakva zloupotreba tajnosti od strane vrha vlasti ili delova izvršne vlasti, najčešće obaveštajno-bezbednosnih struktura dovodi do nepoverenja, otuđivanja i jaza između vlasti i civilnog društva, što je čest osnov i uzrok političkih nestabilnosti i previranja.

„*Svrha tajnosti u slučajevima kao što je američko bombardovanje Kambodže ranih sedamdesetih ili miniranja luka u Nikaragvi kasnih osamdesetih, svakako nije bila sakrivanje informacija od neprijatelja, koji su bili veoma svesni šta mi radimo. Pre je cilj bio da se izbegne javna rasprava i zakonodavna debata o politikama koje bi mozda bile blokirane da je demokratsko donošenje odluka bilo omnogućeno***"** (Schulhofer, 2010, p. 15)

Ako je pretpostavka da se kao tajna čuva nešto negativno, kompromitujuće ili nešto što bi, ukoliko bi se saznalo, moglo negativno uticati na onoga ko to skriva, želja za otkrivanjem takve tajne od strane drugih je podstaknuta i činjenicom da se upoznavanjem sa takvim činjenicama stiče moć u odnosu sa onim ko pokušava da svoje slabosti zaštiti tajnom. Čovek ima potrebu da sačuva svoje i želju da otkrije tuđe tajne. „*Ljudskoj prirodi je svojstven dvostruk odnos prema tajni. Rano spoznajemo, s jedne strane, da je važno da sakrijemo svoje tajne od drugih da bismo izbegli probleme, a, s druge strane, i da je važno da saznajemo tuđe tajne budući da od toga možemo imati samo koristi, makar i u vidu zadovoljenja radoznalosti"* (Simeunović, 2009, p. 109).

Otkrivanje tuđe tajne odnosno upoznavanje sa nečijim slabostima ili kompromitujućim činjenicama može dati poziciju moći u određenom odnosu. Preneto na makro plan, država ima svoje tajne koje čuva i tako sprečava protivnike da saznaju informacije na osnovu kojih bi je mogli lakše ugroziti. Državni organi imaju zadatak da sačuvaju svoje tajne, ali istovremeno

preko obaveštajnih službi država nastoji da otkrije što više onoga što druge strane pokušavaju da zadrže tajnim. Saznavanjem tuđih tajni može se steći prednost u različitim sferama (politička, vojna, ekonomska, tehnološka). Nisu retki primeri u kojima se otkrivanjem neke tajne menjao odnos snaga, pa ponekad, može se reći i tok istorije. Jedan od najeklatantnjih primera je svakako uspešna akcija sovjetske obaveštajne službe vezana za projekat Menhetn (razvoj atomske bombe u SAD), što je omogućilo SSSR-u da već 1949. razvije ovo oružje i tako uspostavi ravnotežu sile koja je postala simbol savremenog doba (Holloway, 1994).

Za ispravno donošenje odluke ili postupanje u određenim okolnostima, neophodno je poznavanje situacije odnosno svih relevantnih činjenica. Ako je kompletno činjenično stanje poznato samo užem krugu ljudi, koji odluče da to saznanje čuvaju kao tajnu i time spreče upoznavanje ostalih sa datim činjenicama, to stvara ekskluzivitet u donošenju ispravne odluke a samim tim i adekvatnog postupanja u toj situaciji. Tajnost većinu drži u neznanju o određenoj pojavi, događaju, stanju. Gledano sa strane spoljašnjih subjekata u odnosu na tajni podatak, oni mogu biti svesni postojanja nekih činjenica i toga da im nešto nije poznato u celosti ili sa druge strane mogu biti u potpunom neznanju. „*Sva dosadašnja izučavanja pojma tajne polaze sa stanovišta da je moguće govoriti o dve osnovne vrste tajni:-apsolutnoj (opštoj) tajni- nepoznatoj svima (tajne nauke, prirode isl.) i relativnoj, koja predstavlja nepoznanicu samo za nekoga (određeni krug ljudi, neko društvo itd.)*“ (Stajić, 2010, p. 344)“

„Kao što znamo, postoje poznata saznanja; postoje stvari koje znamo da znamo. Takođe svesni smo da postoje poznate nepoznanice; Tako reći znamo da postoje stvari koje ne znamo. Ali takođe postoje nepoznate nepoznanice- one koje nismo ni svesni da ih ne znamo. Ako se pogleda kroz istoriju naše i drugih slobodnih država, ova poslednja kategorija spada u najteže.” (Rumsfeld, 2002).

Postojanje svesti da nešto ne znamo (poznata nepoznanica) znači da smo ipak svesni postojanja toga što ne znamo. Svesni smo dakle, da nešto postoji, ali nemamo uvid u kompletno činjenično stanje. Zaklanjanjem samo dela činjenica, tajnost nas i ovde ipak onemogućava u donošenju odluke, ili preduzimanju radnje po tom pitanju. U odnosu na nepoznati deo činjeničnog stanja možemo baratati samo pretpostavkama, što automatski znači više potencijalnih rešenja, pa samim tim i nesigurnost u opredeljivanju za ispravnu odluku ili postupanje. U drugom slučaju, ukoliko je primenom tajnosti od svesti većine sakriveno da

nešto uopšte postoji, u tom slučaju se ni ne postavlja pitanje pogrešne procene u odlučivanju, jer se ne može baratati informacijom koja nije ni delimično spoznata.

Ovde se ispoljava još jedna karakteristika tajnosti, a to je njeno stepenovanje. Nema svaka informacija isti značaj. Efekat iznenađenja koji bi usledio pri otkrivanju određene informacije označava vrednost te informacije (Parezanović, 1995). A u odnosu na vrednost informacije donosi se odluka o stepenu njene zaštite, odnosno stepenu tajnosti. Sa tim je u direktnoj vezi i broj onih koji su sa tajnom upoznati. Što je krug ljudi koji znaju tajnu veći to se smanjuje značaj funkcije tajnosti u tom slučaju. Stepen tajnosti je u direktnoj vezi i sa brojem lica upoznatih sa informacijom. Što je taj broj veći, utoliko je tajna na nižem stepenu tajnosti. Ako su svi članovi jedne zajednice upoznati sa nekom informacijom, ona se ne smatra tajnom. Što je krug onih koji znaju informaciju manji to znači da se radi o strože čuvanoj tajni. „*Kako se krug ljudi svesnih postojanja tajne širi, postaje sve verovatnije da će tajna biti otkrivena, i direktno- jer postoji više strana koje bi je mogle smišljeno ili omaškom otkriti drugima i indirektno-jer će doći do povećane komunikacije između onih koji su sa njom upoznati, usled čega ostali mogu doći do informacije"* (Pozen, 2010, p. 286).

Ekskluzivitet potpunog poznavanja situacije je uvek bio privilegija vladara i bliskog kruga njegovih saradnika, a kasnije nosilaca najviših državnih funkcija. Tajnost je oduvek sredstvo održavanja moći. Prava informacija je uvek imala vrednost, ali se ovaj kvalitet menja u odnosu na vreme. Uticaj na to imaju političke, kulturne, društvene, socijalne, tehnološke i druge promene tokom različitih perioda. U odnosu na to se menjala i potreba da nesto bude tajno. Nekada su strogo čuvane tajne bili ekonomski i demografski podaci koji danas spadaju u osnovne podatke o svakoj zemlji koji su dostupni svakome. Povezivanje, napredak tehnologije i različite mogućnosti utvrđivanja podataka obesmislili su označavanje ovih podataka kao tajnih. Protok vremena i vrednost informacije su obrnuto proporcionalni, pa je samim tim i potreba čuvanja informacije kao tajne vremenom opada. Nešto što je pre pedeset godina bila državna tajna danas teško da može da ima isti značaj, jer su protok vremena i nastupeli događaji uglavnom izneli na videlo sadržaj takve tajne, načinivši je arhivskom i istorijskom građom. Ovo je razlog zbog koga je potrebno periodično vršiti reviziju klasifikovanih dokumenata kako bi se izvršila deklasifikacija onih koji više po prirodi nisu takvi da bi bili čuvani u tajnosti. Stoga velika većina zakonskih rešenja predviđa protok određenog vremena kao jedan od načina prestanka tajnosti informacije.

3. (ZLO)UPOTREBA TAJNIH PODATAKA

Tajnost je veran pratilac vlasti. Ona nalazi svoju upotrebu na svim nivoima vladavine. U prošlosti je bila pravilo i osnovno sredstvo održavanja moći vladara. Vremenom, prolaskom pojma države i vlasti kroz različite faze dostignut je nivo političke svesti da država nije vlasništvo vladara koji je bogom dat, već nosilac suverenosti postaje narod odnosno, nacija [3] (Marković, 2008).

Borba između prava na informaciju, odnosno transparentnosti i tajnosti je obeležje savremenog doba, naročito proteklih dvadesetak godina, kada je došlo do globalnih promena u svetu i drugačijih tumačenja mnogih pojmova, među kojima i pojmova demokratije i građanskih prava i sloboda. Promene u poimanju granica pojma bezbednosti bitno su izmenile pogled na učešće brojnih faktora u vršenju funkcije bezbednosti, čije je ostvarivanje i dalje zadatak države, ali činioci koji sudeluju na ostvarenju tog cilja nisu više isključivo državni organi.

Ako pođemo od pretpostavke demokratske ustavne države [4] (Simeunović, 2002) i načela podele vlasti, može se zaključiti da u svom radu po prirodi stvari sa najviše podataka i informacija barata izvršna vlast. Organi izvršne vlasti, po redovnom toku stvari ostvaruju najviše kontakata sa građanima, drugim državnim organima i organima drugih država. Koncepcija njihovog rada je usmerena na rad sa informacijama i delanje koje je rezultat obrade i analize u radu prikupljenih podataka. Vlada, kao centralni organ izvršne vlasti, kreira i oblikuje politiku države koja se operacionalizuje na unutrašnjem i spoljnjem planu upravo kroz rad izvršnih organa. Istovremeno su prisutne, težnja da oni na što bolji način obavljaju svoju funkciju i konstantna potreba nadzora nad njihovim radom, jer je nesporno da je u rukama izvršne vlasti najveća koncentracija političke moći. Ta činjenica, sama po sebi nosi rizik od zloupotrebe datih ovlašćenja i zahteva dobre mehanizme kontrole u cilju što efikasnijeg funkcionisanja administrativnog aparata.

[3] Razlika u teoretskom određivanju nosioca suverenosti. U zavisnosti od toga razlikuje se i način predstavljanja.

[4] Idealni tip demokratske države nastao kao spoj zapadnih demokratija i načela pravne državnosti. Nakon Drugog svetskog rata postaje pravilo ustavotvorstva širom sveta. (Simeunović 2002)

Osetljive informacije, koje su od značaja za očuvanje interesa države, pretežno dolaze iz sfere rada izvršne vlasti. Procena ugrožavanja bezbednosti, koje bi izazvalo odavanje osetljivih informacija, sprečavanje tog ugrožavanja i sama zaštita podataka spada u delokrug rada organa sistema nacionalne bezbednosti, koji takođe pripadaju izvršnoj vlasti. Po prirodi stvari, zakon o tajnosti podataka je namenjen najviše službama bezbednosti, koje obrađuju, stvaraju i prikupljaju najviše podataka koji ispunjavaju uslove da budu označeni kao tajni.

Monopol izvršne vlasti nad kontrolom i stavljanjem oznaka tajnosti na osetljive podatke izložen je brojnim kritikama, jer sa sobom nosi opasnosti po demokratski poredak. Ovaj problem je prisutan kako u državama sa razvijenom demokratijom i funkcionalnim državnim aparatom, tako i u nadnacionalnim zajednicama. Mehanizmi ograničavanja dominantne pozicije izvršne funkcije u kontroli i baratanju sa tajnim podacima je goruće pitanje ne samo na nacionalnom nivou već i u okviru EU. „*Jednostrana kontrola izvršne vlasti nad svakom informacijom koju odabere da smatra osetljivom prekida odnos sa osnovnim principom funkcionisanja predstavničke demokratije"* (Curtin, 2013, p.6). Za ovu dominantnost izvršnog aparata ima više razloga. U prvom redu izvršni apparat je taj koji čini većinski deo javnog sektora i radi sa najviše podataka, pa će samim tim od njega i poticati najveći broj tajnih podataka. Organi izvršne vlasti su ti koji operativno deluju u cilju zaštite nacionalne bezbednosti, pa u skladu sa tim vrše prikupljanje i obradu najvećeg broja podataka koji mogu biti označeni kao tajni.

Skoro svako delovanje državnih organa u sebi sadrži neka ovlašćenja, čijom primenom se utiče na obim prava građana. U tom, kao i svakom drugom poslu može doći do zloupotreba datih ovlašćenja, ali to ne bi trebalo i smelo da dovodi u pitanje suštinu postojanja tog posla, niti ovlašćenja za njegovo vršenje. Takođe, rasipanje resursa i vremena bi bio pokušaj kontrole svakog pojedinačnog posla ove prirode. Teško je zamisliti da se može uspostaviti nekakava vrsta kontrole koja bi predupredila svako prekoračenje ovlašćenja organa izvršne vlasti ili zaustavila namernu ili nehatnu zloupotrebu primene tajnosti. Takva kontrola zahtevala bi aparat, veći od onog koji kontroliše, što bi sa materijalne i efektivne strane bilo neodrživo rešenje. Zato je najefikasniji kontrolor upotrebe javnih ovlašćenja postojanje odgovornosti za njihovu primenu (počevši od lične preko institucionalne do političke).

Ovde je zanimljivo što dolazi do izražaja postojanje dvostrukih standarda, u pogledu zainteresovanosti javnosti za suzbijanje zloupotrebe datih ovlašćenja. Kada dođe do primene

tajnosti van pravnih okvira postoji razlika u odnosu domaće javnosti prema tome da li se prikrivani postupci odnose na unutrašnja ili spoljna pitanja. Primetna je manja osetljivost članova nekog društva kada, nakon obelodanjivanja tajnih podataka postane javno da je tajnost korišćena u svrhu prikrivanja akcija ili nehumanog postupanja van matične teritorije nad "nekim drugim ljudima", u odnosu na slučajeve kada se odnosi na kršenja zakonskih i društvenih normi prema vlastitim građanima. Dokaz tome je poređenje efekata obelodanjivanja podataka vezanih za dve afere koje su potresle SAD (Votergejt i Wikileaks), gde je jedna faktički dovela do smene predsednika, a druga osim brojnih polemika javnosti i kongresa, nije imala veće posledice po nosioce političke vlasti. Američke građane nije isto uzbudilo prisluškivanje stranih predsednika država i vlada od strane NSA[5], kao činjenica da su i sami bili objekti primene mera nadzora nad elektronskim komunikacijama. Povremena "curenja" tajnih podataka u javnost, pokazala su da ovakava zloupotreba tajnosti nije strana državnom aparatu, te da je postojanje apsolutnog poverenja civilnog društva u ispravnu svrhu tajnosti, nije moguće.

U praksi, može se napraviti razlika između tri vida vladine primene tajnosti. Prvi predstavljaju tajne, koje su zaista vezane za nacionalnu bezbednost i služe njenoj zaštiti. Drugi su one tajne koje se kriju iza nacionalne bezbednosti, nastaju kao odraz potrebe administracije za radom u tajnosti („birokratske tajne") . Treći vid tajni su najopasnije „političke tajne". Ovde se tajnost koristi za sticanje političke prednosti i mogu skrivati različite vidove nelegitimnog ili nelegalnog delovanja (Aftergood, 2009). Sve administracije, pa i one najefikasnije su podložne zloupotrebama ovlašćenja bilo pod političkim pritiskom funkcionera, bilo radi zataškavanja svojih grešaka i zloupotreba, bilo iz nestručnosti. Sve ovo ukazuje da u dilemi da li se zloupotreba tajnosti može potpuno sprečiti i iskoreniti, prevagu odnosi negativan odgovor, što ipak ne znači da se sa tim treba pomiriti i prepustiti administracijama da rade van pravnih okvira. Ipak pravo nije svemoćni regulator koji rešava svaki problem. Zakoni kao takvi mogu biti besprekorno izrađeni, ali ako oni funkcionišu samo na bazi teorije rezultat je isti kao da norme ni ne postoje. Važan element svake primene prava, a naročito one koja se odnosi na tajnost je i nivo političke svesti jednog društva kao i

[5] NSA- National Security Agency- Osnovana 1952. obaveštajna agencija američke vlade, koja prvenstveno vrši nadzor nad svim oblicima elektronskih komunikacija. O njenom radu se vrlo malo znalo do afere Snouden kada je obelodanjeno da pored prikupljanja podataka iz inostranstva NSA vrši masovni nadzor i skladištenje podataka o elektronskim komunikacijama američkih građana.

određeni setepen bezbednosne kulture koji bi trebalo da poseduju ne samo pripadnici nacionalnog sistema bezbednosti nego i svi građani. Svest o postojanju ovog problema trebalo bi samo da bude signal i motiv za uspostavljanje boljeg i usavršenijeg sistema demokratske kontorle rada institucija i razrade poboljšane pravne regulative u ovoj oblasti, a nikako osnov za političku propagandu, stalnu sumnju i razvijanje nepoverenja prema državnom aparatu, službama bezbednosti ili nekim drugim nosiocima javne vlasti.

Zakonodavna vlast oličena u parlamentu odnosno njegovim užim telima (skupštinski odbori) najčešće se nalazi u poziciji da prima već pripremljene informacije i dokumenta od strane izvršnih organa koje kontroliše, tako da su predstavnici ovih tela češće u ulozi lica koja su upoznata sa sadržinom tajnih dokumenata nego u ulozi lica koja neposredno stavljaju oznaku tajnosti. Samim tim broj tajnih podataka koje će predstavnici ove grane vlasti stvoriti nije tako velik.

Sudska vlast uživa visok stepen nezavisnosti i autonomije. Podaci i informacije sa kojima barata se pretežno odnose na postupke i sistem izdržavanja sankcija, te većinom na podatke o preduzimanju istražnih radnji i podatke o ličnosti, pa će u praksi o tajnosti informacija, koje su od značaja za nacionalnu bezbednost, a dolaze iz ove grane vlasti opet odlučiti organi izvršne vlasti. Takođe, treba uzeti u obzir da kada se radi o primen tajnosti od strane pravosudnih organa ona će u retkim slučajevima biti na meti kritike i prigovora zloupotrebe. Može se reći da oko upotrebe tajnosti, vezane za rad pravosudnih organa postoji javni konsenzus, te je proizvodnja tajnih podataka ove grane vlasti uživa visok stepen legitimiteta kod civilnog društva.

Od ukupnog broja podataka sa kojima barataju organi javne vlasti jedan određeni broj je takve sadržine da nije podesan da bude dostupan javnosti i kao takav izuzet iz obaveze uvida i davanja građanima (Matić, 2012). Iako rad državnih organa nesumnjivo treba da bude u velikoj meri javan, pitanja i informacije, koji se tiču prevashodno nacionalne bezbednosti, opravdano moraju ostati izvan domašaja javnosti. Tu se radi o naročito osetljivim podacima čije bi objavljivanje i dostupnost svima moglo ugroziti samo funkcionisanje i postojanje države. U svakom društvu se ovakvi podaci tretiraju kao tajni, a načini i tehnike njihove klasifikacije se donekle razlikuju. Najveći broj osetljivih podataka koji mogu biti tajni je vezan za nacionalnu bezbednost i odnosi se na zaštitu najviših nacionalnih interesa, kao što su zaštita ustavnog uređenja, teritorijalne celovitosti, života i zdravlja građana, vitalne

infrastrukture, ekonomske stabilnosti, tehnologija. Ti podaci spadaju u sferu regulisanja Zakona o tajnosti podataka (Službeni glasnik RS, 104/2009) .

Podaci koji zahtevaju poseban tretman zbog svoje osetljivosti, kao što su lični podaci građana, podaci o privrednom poslovanju, zdravstvenom stanju ne spadaju u tajne podatke u užem smislu značenja. Njihovo prikupljanje, obrada i deljenje obično se regulišu posebnim zakonima (Zakon o zaštiti podataka o ličnosti-Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012, Zakon o zaštiti poslovne tajne (Službeni glasnik RS, 72/2011), a "tajnost" ovih podataka se ogleda u obavezi držalaca ili obrađivača ovakvih podataka da ih čuvaju i koriste na zakonom propisan način. Ovi podaci, ne spadaju u tajne podatke, u smislu zakona koji uređuje tajnost podataka.

Upotreba tajnosti ima svoje prednosti i mane. Kao osnovne pozitivne strane primene tajnosti mogu se navesti:

1. Zaštita nacionalne bezbednsoti od najrazličitijih mogućnosti ugrožavanja, do kojih bi došlo ukoliko bi sa podacima bio upoznat neodređen krug lica koja čine javnost.
2. U kriznim situacijama, kada je neophodna brzina reagovanja, može ubrzati rad tromog državnog aparata, skraćujući vreme odlučivanja i eventualne debate oko određenog pitanja.
3. Omogućava efikasnu borbu protiv terorizma, na taj način što same mere i prikupljanje podatka bitnih za suzbijanje ove pojave ostaju nedostupni za protivnika.
4. Omogućava kreiranje efikasne spoljne i unutrašnje politike Vlade (Tajnost ovde u početnoj fazi pomaže da se lakše dođe do gotovog proizvoda (plana, strategije, politike) izbegavajući pri tom suvišne polemike i debate oko svakog njegovog elementa. Kada dođe do operacionalizacije tajnost prestaje da bude zaštita kreirane politike i ona će vrlo brzo biti izložena sudu političkih protivnika, inostranih vlada i samog domaćeg biračkog tela.
5. Omogućava borbu protiv kriminala i efikasno funkcionisanje sudske vlasti.
6. Onemogućava zloupotrebe do kojih bi došlo ako bi određena informacija bila javna.
7. Efikasan je zaštitnik prava na privatnost. Organi javne vlasti imaju pristup ogromnom broju različitih podataka o građanima. Objavljivanje ovakvih podataka predstavljalo bi ozbiljno narušavanje privatnosti, kao ustavom i međunarodnim konvencijama zagarantovanog prava i moglo bi dovesti do ozbiljnih posledica (Epps, 2008). Zato

svaka odgovorna država donosi zakone kojima štiti privatnost svojih građana time što podatke o ličnosti stavlja u poseban režim zaštite.

Neki od negativnih efekata primene tajnosti:

1. Mogućnost da tajnost bude zloupotrebljena i korišćenja u suprotne svrhe od onih zbog kojih postoji- prikrivanje krivičnih dela, prekoračenja ovlašćenja ili nestručnog rada.
2. Opasnost od prekomerne koncentracije moći u rukama izvršne vlasti- Izvršna vlast ispoljava kao svojstvo težnju da radi u tajnosti. „ *Svaka birokratija teži da uveća superiornost profesionalne obaveštenosti čuvanjem svojih znanja i namera u tajnosti"* (Weber, 1991, p. 233). Birokrate skrivaju informacije, ne samo od javnosti već i od drugih organa, čak i od viših instanci. Nije redak slučaj da se u okviru obaveštajnih službi pojavi ovakvo zastranjenje prilikom koga se prikuplja i zadržava deo važnih informacija, ili se čak one pogrešno ili potpuno izmenjeno prezentuju vladama i političkim rukovodiocima. Puštanje ovakvih informacija u javnost može da posluži za političko uzdrmavanje ili čak da dovede do ostavki ili smena državnih funkcionera. Ovo je jedan od načina svojevrsnog "unovčavanja" vrednih informacija (Sulchofer, 2010) koje poseduju službe. Ove informacije se i čuvaju unutar ovakvog zatvorenog kruga kako bi se iskoristile u pogodnom trenutku na najpodesniji način pri čemu pojedinci nastoje da u to ugrade lični interes.
3. Nepouzdanost-tajne informacije su sklone "curenju" u javnost i teško održive u režimu tajnosti u dužem periodu, primer-Wikileaks, Snouden (Fenster, 2014)
4. Cena tajnosti- održavanje podataka u režimu tajnosti, rad sa tajnim podacima pa i ukidanje tajnosti košta državu tako što uvećava administraciju na dva načina. Prvi je vezan za deo aparata koji radi na očuvanju tajnosti a drugi na organima koji nastaju kao mehanizam kontrole ovog sistema (Epps, 2008).
5. Onemogućava javno raspravljanje i debatu po pitanjima od društvenog značaja. (Mnoge aktivnosti Vlada u zemlji i inostranstvu teško bi bile sprovedene ako bi prethodno bile izložene javnoj raspravi u parlamentu ili sudu javnog mnjenja).

Na svaku prednost ili nedostatak iz ovog nabrajanja bi se mogla otvoriti polemika i dati niz argumenata "za" i "protiv". Praksa je pokazala da je tajnost nužan faktor zaštite svake države koji ispoljava pozitivne efekte i služi javnom interesu samo onoliko koliko se upotrebljava na stručan način i u ispravne svrhe. Sve preko toga povećava negativne efekte ove pojave.

4. TAJNI PODATAK U DEMOKRATSKOM OKRUŽENJU

Demokratski principi nalažu transparentnost rada organa javne vlasti. Pristup informacijama kojima raspolažu državni organi je jedan od važnih elemenata legitimiteta vlasti.

„*Uređivanje pristupa vladinim informacijama je demonstracija službenih ovlašćenja, ništa manje važna od uspostavljanja poreske stope, pretresa kuća osumljičenih za špijunažu ili izgradnju raketnog štita-sve oblasti koje su predmet strogih mehanizama uzajamne kontrole."*. (Schulhofer,2010, p.3)

Predstavnička demokratija nalaže da izabrani politički predstavnici imaju odgovornost prema svojim biračima. Kreiranje odgovorne politike u najširem smislu i organizovanje funkcionalnih institucija za njeno sprovođenje su ozbiljni zadaci čiju uspešnost birači procenjuju i u skladu sa tim na sledećim izborima daju ili uskraćuju poverenje vladajućoj političkoj opciji. Da bi ovakav sistem participativne demokratije i političke odgovornosti funkcionisao neophodno je da građani budu obavešteni o radu i funkcionisanju državnog aparata. Kontrola koju vrše na ovaj način je značajna, kako bi i tokom mandata bila vršena procena da li vlasti rade u javnom interesu i kako bi se na taj način sprečila koncentracija moći i zloupotreba poverenih ovlašćenja jednom izabranih predstavnika naroda. Interes javnosti da sazna šta se dešava iza vrata kancelarija administracije je nesumnjivo opravdan i to je razlog zašto je većina evropskih zemalja po ugledu na SAD, zakonski regulisala pravo na pristup informacijama kojima raspolažu organi vlasti. Do kraja 2012. Zakon o slobodnom pristupu informacijama od javnog značaja usvojila je 91 država širom sveta (Brown, et al., 2014).

Pravo na informisanost se sve više izdvaja kao samostalno pravo koje je proklamovano, kako u brojnim međunarodnim aktima, tako i u velikom broju nacionalnih ustava. Ono svoj koren ima u pravu na slobodu izražavanja, koja predstavlja osnovno ljudsko pravo prve generacije. (Milenković, 2010). Ograničavanje ovakvog prava je već samo po sebi opasnost za pravni život jenog otvorenog društva u kome se pretenduje na ostvarivanje demokratskog uređenja. Međunarodni principi koji definišu odnos između nacionalne bezbednosti i transparentnosti polaze od pretpostavke da svako ima pravo da traži, dobije, koristi i saopšti informaciju koja je u posedu organa javne vlasti, a kako Vlada snosi punu odgovornost za nacionalnu bezbednost, „*samo Vlada i može istaći da informacija ne može biti javna ako bi to ugrozilo*

nacionalnu bezbednost“ (Open Society Foundations, Open Society Initiatives, 2013). Uz to, ograničenje prava mora biti - definisano zakonom koji je dostupan, jasan, nedvosmislen i omogućava svakome da shvati koje informacije su poverljive, koje bi trebalo da budu javne i koje radnje su sankcionisane, usmereno na zaštitu ili ostvarivanje legitimnog interesa (nacionalne bezbednosti) i neophodno u demokratskom društvu (Transparency International, 2014).

Kao što pojedinac u odnosu sa drugima nastoji da ostvari visok stepen spoznaje jer se na taj način ostvaruje odnos poverenja, a samim tim i sigurnosti (Simmel, 1906) slično se dešava u kolektivnom odnosu civilnog društva sa organima vlasti. Što je više tajni i zatvorenosti u tom odnosu, manje je društveno poverenje u državni aparat i nosioce vlasti.

U nedemokratskim režimima rad celokupnog državnog aparata je pod velom tajne i mistifikacije. Jedno od glavnih sredstava za održavanje moći ovakvih režima je tajna policija. Obeležje odnosa društva prema ovakvoj državi je strah, a to uzrokuje apsolutno odsustvo poverenja. „ *Opšti strah koji vlada u totalitarnim državama je njihova važna karakteristika. Taj strah, tačnije zebnja obezbeđuje se terorom koji vrši tajna policija“* (Simeunović, 2009, p. 94). U takvom, nedemokratskom okruženju nema potrebe za razmatranjem postojanja i primene tajnosti jer je vlast potpuno otuđena od društva. Radnje svih državnih organa, i zakonite i nezakonite, su zaklonjene od javnosti, usmrene na potrebe i očuvanje vlasti, a građani su u takvom okruženju više podanici nego punopravni članovi društva.

Demokratska država i ono što ona podrazumeva (postojanje civilnog društva, koje podrazumeva otvorenost i tranparentnost, kako prema spolja tako i unutra, vladavinu prava i postojanje pravne države, zagarantovan širok opus ličnih, političkih i ekonomskih prava i sloboda, društveno odgovorno postupanje vlasti, tolerancija i druge vrednosti) podrazumeva da primena tajnosti bude izuzetak, s obzirom da može imati snažan uticaj na zagarantovana prava i slobode koje su osnova demokratije. Ovo, naizgled "neprijateljsko" okruženje za tajnost, nikako ne znači da ona u demokratkim državama ne postoji, već da je podvrgnuta normativnim ograničenjima i kontroli. Tajnost se i u demokratskom uređenju, smatra važnim elementom očuvanja vitalnih vrednosti države i vezuje se prvenstveno za okvir nacionalne bezbednosti.

U demokratskom uređenju svaki državni organ je dužan da se stara prvenstveno o zaštiti javnog interesa. Da bi se procenilo šta je u javnom interesu, neophodno je da se izvrši procena sučeljenih prava u svakom konkretnom slučaju. Vaganje ovih interesa, procena da li bi šteta usled omogućavanja pristupa tajnim podacima bila veća od uskraćivanja zagarantovanog prava na informaciju. Ovakav test javnog interesa je idealno rešenje, međutim da bi on dao dobre rezultate, neophodno je da bude stručno i ispravno sproveden, što je u praksi veoma diskutabilno pitanje.

„Naši demokratski principi zahtevaju da američki narod bude obavešten o aktivnostima njihove vlade. Takođe, napredak naše nacije zavisi od slobodnog protoka informacija, na oba nivoa, kako unutar vlade, tako i među američkim narodom. I pored toga, tokom naše istorije nacionalna bezbednost zahtevala je da određene informacije budu zadržavane kao poverljive u svrhu zaštite naših građana, demokratskih institucija, bezbednosti naše zemlje i naših odnosa sa drugim nacijama. Štiteći informacije bitne za našu nacionalnu bezbednost i pokazujući našu posvećenost ka otvorenosti vlade kroz pažljivu i odgovornu primenu i praksu standarda klasifikacije, sigurnost i efektivna deklasifikacija su podjednako važni prioriteti.“ (https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information)

I pored ovakve uvodne reči iz američke predsedničke uredbe, koja sa teoretske strane daje dobro objašnjenje o odnosu između tajnosti i prava na informisanost u demokratskoj državi, svedoci smo da upravo administracija Sjedninjenih Država često krši propisana pravila i zloupotrebljava tajnost u velikoj meri. Najsvežiji primer tome je afera Snouden, kada je jedan od spoljnih saradnika NSA, Edvard Snouden obelodanio dokumenta, iz kojih se vidi da se vrši masovno prikupljanje podataka o komunikaciji širom sveta, što je trend američkih, ali i drugih velikih službi. To je BIG DATA projekat, koji podrazumeva prikupljanje velikih količina ličnih podataka sa kamera, telefona, GPS sistema i nadzora nad internetom koje se skladište u velikim bazama podataka i analiziraju pomoću kompjuterskih algoritama (Van der Sloot, 2014). Primena torture nad zatvorenicima osumnjičenim za terorizam, lišavanje slobode i zadržavanje na neograničeno vreme bez prava na odbranu i kontakt sa pravnim zastupnikom, primena nečovečnih tehnika, ispitivanja nad osumnjičenima za ugrožavanje nacionalne bezbednosti, slike postupanja sa zatvorenicima iz iračkog zatvora Abu Graib samo su neki od primera, kako se upotreba tajnosti može koristiti za nedemokratske aktivnosti demokratske države. Ovaj eklatantan primer kršenja najšireg opusa ljudskih i građanskih prava, od strane

jedne od najvećih administracija na svetu i države, koja po mnogo čemu predstavlja uzor demokratski organizovanog društva samo potvrđuje ekstenzivnost pojma demokratije. Obim pojma i prava, koja on podrazumeva neraskidivo je vezan za doktrinu očuvanja nacionalne bezbednosti. U stanju, kada je ona ugrožena, svaki pravni poredak predviđa mogućnost ograničavanja zagarantovanih prava i sloboda građana. U takvom stanju često dolazi do zatvaranja institucija i široke upotrebe tajnosti na svim nivoima. Najbolji pokazatelj da će ovakvu reakciju na ugroženost vitalnih interesa imati i demokratski uređena država je primer SAD. U stanjima opasnosti, dolazi do težnje da se izvršnoj vlasti, kao onoj koja mora brzo i efikasno da reaguje na date okolnosti, daju šira ovlašćenja i mogućnost da radi u tajnosti. Svako dodatno uplitanje zakonodavne ili sudske vlasti u ove procese bi smanjilo efektivnost odgovora na opasnost (Schulhofer, 2010.) Ovakav pristup, iako diskutabilan sa aspekta vladavine prava pokazao se kao realan u nedavnoj prošlosti. To se jasno ogleda u aktivnostima administracije Džordža Buša nakon terorističkih napada na SAD 11.9.2001. nakon čega je usledilo usvajanje USA PATRIOT ACT[6] i vrtoglav skok primene tajne klasifikacije.

„Istraživanja pokazuju da je američka vlada samo u 2004. Nakon pokretanja ratnih operacija u Iraku i Afganistanu, klasifikovala 15,6 miliona dokumenata ili 81% više nego u 2000. godini. Dok je broj deklasifikovanih dokumenata u konstantnom opadanju nakon 2001. Godine. „ (The CQ Researcher, 2005).

Postojanje ovih činjenica koje svedoče o zloupotrebi primene tajnosti ne znači da američka administracija ima loše normativne akte, koji regulišu ovu oblast, niti da je američko društvo nedemokratsko zato što su ovakvi podaci bili nedostupni javnosti, a takođe nije ni dovedeno u pitanje funkcionisanje američkog sistema nacionalne bezbednosti i delovanja njegovih službi širom sveta. Sjedinjene Države su naprotiv doajen u primeni propisa o pristupu informacijama u posedu organa vlasti, usvajanjem USA FOI ACT[7] još 1966. godine, imaju jedan od najrazvijenijih normativnih sistema u ovoj kao i oblasti tajnosti podataka i mehanizama njenog prestanka, pristupa tajnim podacima i kontrole od strane Kongresa i sudova.

[6] USA PATRIOT ACT- Uniting and Strenghtening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Dokument koji je u velikoj meri omogućio primenu tajnih metoda nadzora i praćenja dajući velika ovlašćenja bezbednosnim službama prvenstveno NSA.

[7] USA FOI ACT- Freedom of Information Act, zakon o pristupu informacijama od javnog značaja. Jedan od najbolje formulisanih pravnih akata o pristupu informacijama u posedu državnih organa i agencija.

Sve navedeno jasno pokazuje da demokratsko uređenje nije garant da će doći do apsolutnog poštovanja svih zagarantovanih prava i sloboda. Primenu tajnosti i ovde prate brojne zloupotrebe, ali je demokratska država trenutno najbolji okvir u kome je svako postupanje formalno uređeno zakonskim normama, a kršenje tih normi sankcionisano uz pomoć razvijenih mehanizmima kontrole. Ipak, i uz postojanje najbolje pravne regulative zloupotreba u radu sa tajnim podacima će uvek biti i one treba da budu sankcionisane, jer nanose višestruku štetu društvu, ali one nikako ne smeju biti predmet politizacije i napada usmerenih na rušenje institucija demokratske države.

5. TRANZICIJA TAJNOSTI

Demokratske promene i ulazak u proces tranzicije, težnja ka evropskim integracijama i izgradnja demokratskih državnih institucija su složen i zahtevan proces koji podrazumeva angažovanje svih činilaca jednog društva. Višegodišnji život i rad u jednom sistemu stvara određene navike kako kod društva, tako i u praksi državnih organa. Neophodan faktor promena ovakvih navika je vreme.

U post-socijalističkim društvima istočnoevropskih zemalja, slom jednog poretka i pritisak zapada ka ubrzanoj "demokratizaciji" čine da se društveno-političke i ekonomske promene odvijaju tempom koji je brži od samih promena u društvenoj svesti. Nastojanje da se brzinom nadoknadi vreme, koje je proteklo u nedemokratskom uređenju čini da period prilagođavanja bude kratak ili čak da ne postoji. Potreba institucionalnih promena i postulata njihovog funkcionisanja zahteva mnogo širi pristup u rešavanju ovog zadatka od prostog usvajanja niza zakona koji regulišu ovo pitanje. Kao što funkcionalna pravna regulativa, država sa demokratskim kontinuitetom, u nekoj oblasti ne znači automatski da će stanje stvari u toj oblasti biti perfektno, tim pre se ni od zakonodavstva država u tranziciji ne može očekivati da momentalno ispune visoke demokratske standarde, jer je stepen razvoja jednog društva taj, koji suštinski čini to društvo sposobnim za demokratsko uređenje. Tranzicija društva je dug put koji podrazumeva protok vremena, u kome pored izmene postojećih mora doći i do izgradnje potpuno novih elemenata sistema. Želju političke elite, da što pre ostvari date promene prati"demokratizacioni pritisak" spolja, uz prisutne strategije uslovljavanja, naročito od EU (Edmunds, 2007). Ovakav rad pod pritiskom, u već politički i socijalno uzdrmanim društvima u velikoj meri otežava efikasnost samog procesa, jer je za njegovo sprovođenje potreban period navikavanja i dosezanja određenog stepena političke kulture. *„Interakcija nekog oblika demokratske promene i ukorenjene lokalne političke prakse dovodi do nekozistentnosti. Lokalna politička kultura menja se mnogo sporije no što je u literaturi o tranziciji pretpostavljeno."* (Edmunds 2007, p. 6). U zemljama tranzicije je čest slučaj da se kroz želju da se što pre dođe do demokratije stvara atmosfera odbojnosti i neprihvatanja svega što spada u zaostavštinu socijalističkog sistema i autoritarnih režima. Borba za vlast u takvim slučajevima, neretko vodi tome da se u težnji ka promenama ide na rušenje postojećih institucija sistema, ili želju da se sa njima raskrsti kao sa elementom nepoželjne prošlosti, pri čemu se zaboravlja da je sama tranzicija složen proces, koji u njegovoj biti moraju sprovesti i izneti upravo postojeće institucije. One su element sistema koji je funkcionalan, što je

dokazano time što su radile dugi niz godina. Političko opredeljenje bi u ovom slučaju trebalo da bude samo smernica za dalje funkcionisanje nasleđenih elemenata sistema. Korišćenjem funkcionalnih institucija, uz njihovo usputno postepeno prilagođavanje i izmene u načinu rada omogućava da se proces tranzicije uspešno sprovede, jer od očuvanosti nasleđenih institucija zavisi kvalitet i brzina tranzicionog procesa.

„ Najvažnija politička razlika između zemalja nije u formi njihove vlade nego u stepenu vladanja. Razlike između demokratija i diktatura kao država čije politike otelotvoruju konsenzus, zajedništvo,legitimitet, organizaciju, efikasnost i stabilnost su manje nego kod onih država koje su manjkave u ovim kvalitetima. Komunističke totalitarne države i zapadne liberalne spadaju generalno pre u kategoriju efikasnih nego u kategoriju zaostalih političkih sistema.“ (Huntington, 1973, p. 1).

Brojni su primeri u kojima je ovakvo postupanje u periodu tranzicije dovelo do otežanog funkcionisanja, usled neplanskog i nekoordiniranog prilagođavanja pravne regulative u različitim, a povezanim oblastima. Pravna regulativa koja se odnosi na podatke i njihovu zaštitu u republici Srbiji je jedan od primera “tranzicionog normativnog srljanja”. Regulisanje ove oblasti podrazumeva paket međusobno usklađenih zakona, koji podrazumevaju da njihova primena počne, ako ne istovremeno, onda barem u razumnim vremenskim intervalima koji bi onemogućili postojanje nedefinisanih momenata u primeni svakog zakona pojedinačno. Osim što su kod nas ovi zakoni doneti u priličnom vremenskom razmaku (2004, 2008, 2009) i sam sled njihovog donošenja je nelogičan. Prvi u nizu je bio Zakon o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009 i 36/2010), zatim par godina posle njega Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012), da bi Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009) došao tek na kraju, iako on, po mišljenju brojnih stručnjaka predstavlja osnovu odnosno “krovni zakon"[8] u ovoj oblasti.

Ovakva praksa dovodi do potrebe za brojnim izmenama i dopunama postojećih zakona, a često i do potrebe usvajanja potpuno novih zakonskih tekstova, u kratkim vremenskim intervalima od donošenja prvobitnog normativnog akta, što je odraz neozbiljnosti pravnog

[8] Pojam označava da Zakon o tajnosti podataka uvodi jedinstven sistem označavanja tajnih podataka što znači da ovo pitanje ne može na drugačiji način da se uređuje drugim zakonima.

sistema. Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009), zbog brojnih manjkavosti i sporosti u donošenju pratećih podzakonskih akata u velikoj meri je ostao van praktične primene, čime dolazi do situacije da imamo pravnu regulativu, a da se faktički primenjuju stare norme i ustaljena pravila rada u organima.

Usvajanjem Zakona o tajnosti podataka (Službeni glasnik RS, 104/2009), propisano je koji stepeni tajnosti postoje, čime su pojmovi iz ranijeg perioda i nejedinstveni sistem klasifikovanja tajnih podataka prestali da važe. U SFRJ primenjivana su pravila o tajnosti na osnovu koncepta opštenarodne odbrane i društvene samozaštite i ona su razrađivana po resorima u smislu konkretizacije samog postupka označavanja tajnih podataka. (Matić, 2014). S obzirom na zatvorenost kompletne državne uprave i njenog rada u socijalističkom režimu ovakav model organizovanja je razumljiv. Resorni model je značio da postoje zasebna pravila o radu sa tajnim podacima u Vladi, ministarstvu odbrane, unutrašnjih poslova, diplomatiji, bezbednosnim službama, ministarstvu pravde, kao i privrednim društvima od značaja za odbranu i bezbednost. (Matić, 2014). Na osnovu ovoga se može reći da je ovo bilo zlatno doba birokratije. Deo ovih propisa je nasledila SRJ, uz njihove izmene i dopune, ali i neizbežne posledice sloma jednog sistema, koji je dugo godina funkcionisao po određenim ustaljenim pravilima. Naslednik samog koncepta opštenarodne odbrane je postao sistem odbrane, dok je bezbednosni sitem dugo "lutao" između ostataka saveznog sistema i republičkog, koji zbog nedostatka adekvatne infrastrukture nije imao kapacitete da preuzme sve poslove i zadatke. Jedna od prvih žrtava ovakve tranzicije nadležnosti bila su pravila i protokol vezan za tajnost podataka.

Jedna od karakteristika ovog perioda je pojam službene tajne, koji je samo posredno bio objašnjen i to kroz Krivični zakonik (Službeni list SFRJ, 44/76-1329; Službeni list SRJ, 35/92-651) koji je u svom posebnom delu, kao krivicno delo protiv službene dužnosti poznavao odavanje službene tajne. To je podrazumevalo da ovlašćeno službeno lice koje drugoj nepozvanoj osobi preda ili učini dostupnim službenu tajnu bude kažnjeno kaznom zatvora od tri meseca do pet godina. U samom Krivičnom zakoniku (Službeni list SFRJ, 44/76-1329; Službeni list SRJ, 35/92-651) nije preciziran sadržaj pojma službena tajna. Tu se radi o vrsti tajnog podatka koja je imala odgovarajuće stepene tajnosti, a ne kako se često pogrešno tumači o samom stepenu tajnosti. Službena tajna je pojam koji je označavao osetljive podatke koji nastaju u radu državnih organa čijim bi otkrivanjem nastale štetne posledice po službu ili bezbednost zemlje. U sadašnjem zakonu najbliže ovom pojmu je

oznaka tajnosti „INTERNO“, s tom razlikom što je ovaj stepen tajnosti već u startu omeđen samom suštinom primene tajnosti, koja je objašnjena u uvodnom delu zakona. Pored službene tajne podaci od najvišeg značaja za bezbednost spadali su u kategoriju državne tajne. Ovakva podela jasno upućuje na dvojaku orijentaciju svrhe tajnosti podataka. Vojna tajna je primenjivana u sistemu odbrane, prvenstveno vojsci i takođe je imala svoje stepenovanje (Stajić, 2010). Ovakvo stanje stvari stvaralo je dosta konfuzije i nejasnoća te je s toga bilo neodrživo čak i u manjkavom demokratskom sistemu.

Težnja ka evrointegracijama i međunarodna saradnja uslovile su donošenje novog zakona o tajnosti podataka, koji bi na jedinstven i koncizan način odredio šta se može, a šta ne klasifikovati određenim stepenom tajnosti. Novi zakon je pored službene tajne u prošlost poslao i kategoriju vojne tajne čije je postojanje u prošlosti bilo odraz bezbednosnog koncepta, po kome je Vojska bila potpuno odvojen i autonoman sistem, sa svojim internim propisma i pravilima, što je u suprotnosti sa savremenim konceptom nacionalne bezbednosti posmatrane kao celovitog sistema, koji podrazumeva saradnju i koordinaciju svih činilaca bezbednosti u jednoj državi, kako vojnih, tako i civilnih.

Nove norme teže da prate ritam promena i pojava koje su nastupile na globalnom nivou u poslednjih dvadestak godina. Osnovni problem koji se ovde pojavljuje je povezanost tajnosti podataka sa pojmom bezbednosti i njegovim nosiocima u jednoj državi. Da bi se uspešno primenjivala nova pravila neophodna je prvenstveno reforma sistema bezbednosti i njegovo prilagođavanje novim društveno političkim prilikama. „*Uređenje oblasti rada sa tajnim podacima nije samo sebi cilj i problem već je vezano za reformske procese kompletne državne uprave a posebno sektora nacionalne bezbednosti koji još uvek nije definisan u celosti, niti je do kraja kreirana nacionalana bezbednosna politika*.“ (Matić, 2014, p.24). Ukoliko donošenje zakona pretekne ovu reformu, bez izuzetka će zakon ostati mrtvo slovo na papiru, jer ključni činioci koji treba da ga primenjuju neće biti spremni za takvu promenu.

Propisivanjem četiri stepena tajnosti vrši se raskidanje sa prethodnom praksom i upotrebom pojmova, kao što su službena i vojna tajna. Svi podaci koji postaju tajni mogu biti označeni samo jednim od ova četiri stepena, u zavisnosti od potrebe. Pravilo je da se podatak označava najnižim stepenom tajnosti, koji omogućava sprečavanje štete po interese države. i ovo bi trebalo da bude jedno od načela, usmereno na sprečavanje prekomernog označavanja i stvaranja tajnih podataka. Ipak, brojni nedostaci ovog zakona, nekoordinacija državnih organa,

nedostatak obučenog kadra, uslovili su da i nakon stupanja na snagu novih pravila i dalje budu donošeni zakonski tekstovi u kojima se drugačije definišu tajni podaci. Ovu pojavu je teško shvatiti, a još teže objasniti budući da zakonodavni organ koji je usvojio jedan tekst zakona kasnije donosi zakon koji nije kompatibilan sa prethodnim rešenjima. Ovakve greške u radu, zahtevaju brojne kasnije izmene i dopune zakonskih tekstova čime se funkcionisanje normativnog sistema u najmanju ruku koči, a nekad i potpuno blokira.

Problem predstavlja i ostvarivanje veze između ranijih tajnih podataka sa novim sistemom tajnosti. Nesporno je da ovde postoji mnoštvo dokumenata koji ne potpadaju pod kriterijume tajne klasifikacije uopšte, ali takođe to ne može biti razlog kao što deo javnosti smatra da može doći do automatskog ukidanja tajnosti ovih podataka. Jedna od lakših mogućnosti je da sam zakon predvidi način tranzicije ovih dokumenata i njihovog stepenovanja po novim kriterijumima, što je primer Hrvatskog zakona o tajnosti podataka (NN 79/07, 86/12). Ovakvom odredbom se ipak rešava prvi korak, nastoji se da sva dokumenta ostanu na postojećem nivou tajnosti, a njegova relevantnost i eventualno ukidanje oznake tajnosti ostavljaju se za kasniju procenu stručnim službama. Zakon o tajnosti podataka Republike Srbije (Službeni glasnik RS, 104/2009) predviđa da će ovaj zadatak preispitivanja postojećih oznaka tajnosti sprovesti rukovodioci organa javne vlasti, u roku od dve godine od stupanja na snagu zakona. Do isteka tog roka, podaci zadržavaju vrstu i stepen tajnosti, označen po ranijim propisima. Ovakvo rešenje stvara konfuziju, s obzirom da u pravnom sistemu omogućava opstanak napuštenih stupnjeva tajnosti, te je sporno koja pravila se na njih primenjuju. Obimnost ovakvog posla i zahtevnost u stručnom, kadrovskom i tehničkom pogledu moraju biti povereni stručnoj i odgovornoj službi, koja se bavi tajnim podacima, što otvara pitanje razmatranja položaja i kapaciteta Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka u domaćem pravnom sistemu.

5.1. Dilema otvaranja tajnih dosijea.

U autoritarnim režimima rad organa državne bezbednosti je u velikoj meri orijentisan na održavanje pozicija vladajućih struktura. U nastojanju da ima potpunu kontrolu nad svim dešavanjima, totalitarni režimi su se u velikoj meri oslanjali na tajnu službu, preko koje su sprovodili teror (Simeunović, 2009). Tajnost je ovde bila sredstvo koje omogućava primenu nelegitimnih i nelegalnih sredstava pripadnika tajne službe, u cilju obavljanja zadataka koji su joj dati od vrha vlasti. Pored zaštite nacionalne bezbednosti, koja često postaje i sporedni

zadatak, služba se bavi pretežno zaštitom vlasti od političkog i svakog drugog ugrožavanja iznutra. Staljinistički model terora[9] je iznedrio doktrinu borbe protiv unutrašnjeg neprijatelja koja je kasnije, u različitim modalitetima primenjivana u socijalističkim zemljama, u većoj ili manjoj meri. Izjednačavanje ugrožavanja državne bezbednosti sa političkom borbom protiv vladajuće strukture, kao i primena svih metoda u borbi sa političkim neistomišljenicima, u prošlosti su stvorile negativnu sliku i prizvuk opasnosti, koji se vezuje za rad organa bezbednosti.

Kao odraz operativne potrebe vezan za praćenje političkih aktivnosti nastao je veliki broj tajnih dosijea kao rezultat obrade širokog kruga lica budući da je objekat zaštite ovde bio takav da je mogućnost njegovog ugrožavanja najširi opus radnji. Izvori informacija o licima i njihovom delovanju su bile različite mere obaveštajno-bezbednosnog rada. Obim ovog posla kao logičan sled, imao je potrebu stvaranja posebne arhive ovakvih dosijea. Kako su korišćene mere i aktivnosti protiv ovih lica bile pretežno zasnovane na političkim odlukama, a ne na profesionalnim potrebama službe, oznaka tajnosti je bila prirodan sled vezan za sadržinu ovih dosijea. Ovakva tajna arhiva, nakon rušenja nedemokratskih režima postaje vrlo osetljivo političko i bezbednosno pitanje za nove vladajuće garniture u zemljama tranzicije.

Otvaranje tajnih dosijea je tema koja s vremena na vreme dobija pažnju u Srbiji, ali osim turbulencija u medijima, koje tom prilikom nastaju nema konkretnih aktivnosti koje ukazuju da će dosijei ikada biti otvoreni na način kao što je to bio slučaj u Nemačkoj Demokratskoj Republici (NDR). Međutim, taj slučaj ne može biti univerzalno pravilo za ostale zemlje u tranziciji jer se u NDR nije radilo samo o političkoj borbi sa domaćim nedemokratskim režimom, već i o pokušaju da se eliminiše strani faktor, koji je imao veliki uticaj na datu vlast i funkcionisanje njenog aparata. Prekid kontinuiteta sa socijalističkom vlasti u Nemačkoj ima brojne specifičnosti koje proizlaze iz toga što je država bila podeljena, pa je na taj način postojalo paralelno funkcionisanje dva sistema, od kojih je jedan odneo prevagu na kraju i zamenio institucije drugog, veoma malo se oslanjajući na postojeću institucionalnu infrastrukturu.

[9] Prof. dr Simeunović govori o socijalističkoj staljinističkoj državi kao posebnom obliku socijalističke države zbog niza specifičnosti koje su je odlikovale što je odvaja od pojma socijalističke države uopšte. Pa i pojam terora primenjivan u ovakvoj državi ima svoje posebne karakteristike.

Potreba otvaranja dosijea, nastalih pod nedemokratskim režimima ima svoje mesto, u smislu upotrebe dosijea kao dokaza u postupcima rehabilitacije ili zahteva za restituciju, krivičnog gonjenja i ostvarivanja odštetnih zahteva, što je kod nas u određenoj meri omogućeno time što je određeni broj dosijea postao arhivska građa. Međutim, mogućnost uvida u ovu građu nije regulisana posebnim zakonom i pravilima već je oznaka tajnosti uklonjena na osnovu Vladine Uredbe o stavljanju na uvid određenih dosijea o građanima Republike Srbije u Službi državne bezbednosti (Službeni glasnik RS, 31/2001, 131/2001). U vreme donošenja ove uredbe nije postojao zakonski tekst, koji uređuje rad sa podacima o ličnosti, pa je i sama uredba kasnije označena kao neustavna (Odluka Ustavnog suda U 149/01). Oznaka tajnosti je uklonjena samo sa dela tajnih dosijea, koji se odnosi na problematiku unutrašnjih neprijatelja, odnosno unutrašnjeg ekstremizma i terorizma, u periodu od osnivanja službe do stupanja na snagu ove uredbe.

Prvo pitanje, koje mora biti jasno definisano i ugrađeno u odluku o otvaranju ovako osetljive građe je šta je cilj otvaranja dosijea? *„Bez identifikovanja ciljeva tog procesa nema dobrog smisla raspravljati oopravdanosti njegovog sprovođenja, tako da će o tome prvo biti reči u nastavku,a o dometima otvaranja dosijea u vidu njihovog premeštanja u Arhiv Srbije može se precizno govoriti tek kada se zauzme stav o tome koji je primeren način, metod otvaranja."* (Vodinelić, 2014, p. 41). Analiza ovog pitanja, mogući odgovori na njega i njihov odnos sa mogućim posledicama kreiraju političku volju da se arhiva tajne policije otvori. Potreba da svi građani mogu da budu upoznati da li su bili predmet obrade tajne službe i koliko je to uticalo na njihov život, otkrivanje krivičnh dela počinjenih od strane pripadnika tajnih službi, kršenje ljudskih prava i sloboda građana, politička odgovornost za zloupotrebu službi, neki su od razloga u korist otvaranja ove građe. Sa druge strane, postoje ozbiljne dileme vezane za posledice i pitanje mogućnosti sprovođenja takve odluke.

U Srbiji takve političke volje nema iz više razloga. „*Za razliku od većine problema koji se tiču tajnosti podataka, u pogledu čijeg regulisanja ne postoji pitanje "da li", već jedino "kako", u pogledu dosijea koje su političke policije autoritarnih režima u ovoj zemlji vodile o građanima i organizacijama i dana danas je aktuelno i pitanje: da li dosijee uopšte otvoriti a ne samo kako to učiniti."* (Vodinelić, 2014, p.40).

Prvi razlog je svakako taj, što bi otvaranje ovakvih dosijea, najverovatnije kompromitovalo one političke strukture koje su srušile prethodni autoritarni režim, ili uzdrmalo pripadnike

vladajućih političkih stranka, koalicione partnere ili finansijere političkih partija. Ne treba zaboraviti da do rušenja autoritarnih socijalističkih i post-socijalističkih režima nije dolazilo čisto demokratskom političkom utakmicom, već uglavnom nasilnim sredstvima. U organizovanju i pripremama ovakvih događaja pripadnici opozicije su pomagani i iz inostranstva. Budući da su kontakti sa inostranim faktorima, u ovim slučajevima zapravo kontakti sa pripadnicima stranih službi, kojima je u opisu posla rušenje režima u drugim državama, pitanje je koliko je apriori neopravdano u pojedinim slučajevima postojanje dosijea i stavljanje ovakvih političkih činilaca na bezbednosne mere. Kada bi uporedili ovakvo stanje stvari sa današnjim društveno političkim sistemom u zemljama tranzicije, koji je manje-više demokratski ili čak sa razvijenim demokratijama, teško je zamisliti da ovakve delatnosti ne bi bile u fokusu službi bezbednosti, prvenstveno, njihovog kontraobaveštajnog dela. Drugi razlog za oklevanje, po ovom pitanju je i taj što su u rušenju nedemokratskog režima u ovom slučaju pripadnici službi bezbednosti imali određenu ulogu, nakon čega nisu mogli podleći procesu lustracije od strane onih političkih subjekata u čijem su dolasku na vlast učestvovali. Za razliku od NDR i nekih socijalističkih država, ovde nije došlo do potpunog sloma jednog sistema i rasformiranja njegovih institucija koje su zamenjene drugim, već se ovde radi o specifičnom postepenom preuzimanju vlasti uz oslanjanje na postojeći kadar i institucije. Zato se ne može zaobići činjenica da su službe bezbednosti ostale u posedu ovog materijala i imale vremena za modifikaciju ili uništavanje svega onoga što bi ugrozilo aktivan ili bivši kadar. Prezentovanje ovakvog materijala za koji postoji opravdana sumnja da je izmenjen u značajnoj meri, obesmišljava samu suštinu otvaranja dosijea. Treći razlog je što nakon demokratskih promena nije došlo do ustaljivanja jedne vladajuće garniture, već je nastupio politički turbulentan period i više promena na pozicijama vlasti. Takvo stanje onemogućava planski i ubrzani rad na reformi institucija i zakonskoj regulativi. Ovakav protok vremena pogubno utiče na sam smisao otvaranja dosijea, jer je vreme faktor koji omogućava, ili obesmišljava pozivanje na odgovornost onih koji su kršili ljudska prava.

U slučaju otvaranja dosijea, pravno pitanje, koje je zanimljivo za razmatranje je da li je pretežniji interes građana koji su bili predmet obrade tajne policije da saznaju načine dolaska do podataka o njima, gde se prvenstveno misli na identitet saradnika službi, ili pravo ovih lica da im identitet ostane zaštićen. Ovo i ostala sporna pitanja vezana za tematiku tajnih dosijea obaveštajnih službi zahteva poseban zakon koji bi na precizan i jasan način uredio ta pitanja čime bi se izbegla pravna nesigurnosti i primena postojećih pravila koja nisu namenjena ovakvoj specijalizovanoj tematici (Vodinelić, 2014).

Bezbednsone službe su vrlo skeptične po pitanju otkrivanja identiteta svojih saradnika jer su ova lica od velikog značaja za sam rad i izvršavanje zadataka, a i sama pripadaju najrazličitijem krugu ljudi, od političara i intelektualaca do profesionalnih ubica i švercera (Stajić, 2010). Da bi se ovaj potencijal mogao koristiti i u budućnosti službe nastoje da zaštite bivše kako njihovom kompromitacijom ne bi dale loš primer sadašnjim i eventualnim budućim saradnicima.

Svi navedeni razlozi i problemi koji mogu nastati otvaranjem arhive tajnih službi upućuju na to, da ovaj proces mora biti prethodno detaljno analiziran, a zatim ustrojen posebnim zakonom, koji bi na jasan i precizan način propisao kako i u kojoj meri će dosijei postati dostupni javnosti, uz poštovanje principa, koji se odnose kako na zaštitu prava privatnosti i zaštitu ličnih podataka, tako i na regulisanje bezbednosnih problema, koji mogu nastati po ovom pitanju.

6. JAVNOST PROTIV TAJNOSTI, SLUČAJ SRBIJA

U Srbiji je Zakon o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010) započeo reformu u oblasti zakonskog uređivanja oblasti informacija. Njime se uređuje pravo na pristup informacijama od javnog značaja, radi ostvarenja i zaštite prava javnosti da zna, kroz koje se ostvaruju osnovni principi demokratskog društva. Usvajanje ovog zakonskog teksta je trend demokratskih država. Po ugledu na Sjedinjene Države, moderne demokratske države počele su sa donošenjem zakona kojim uređuju ovo pravo i određuju mu položaj u pravnom sistemu. Do 2012. godine preko 90 država u svetu,a gotovo sve u Evropi usvojile su zakonske tekstove koji regulišu pristup informacijama kojima raspolažu državni organi (Brown, et al., 2014).

„Kao što građansko društvo koristi medije u cilju omogućavanja transparentnosti, ta funkcija se kod državnih organa ostvaruje pravom na pristup informacijama od javnog značaja.“ (Brown, et al., 2014, p. 2).

Pravo pristupa informacijama u posedu organa vlasti igra bitnu ulogu na dva načina. Omogućava da se ideja demokratije ostvaruje bliže njenom izvornom obliku, gde se ispoljava kao pravo građana, ali istovremeno ono predstavlja i ograničenje i kontrolu državnih organa, jer zahteva da opravdaju svako ograničavanje prava na inormaciju. *„Bez adekvatne kontrole i odgovornosti svaka vlast, ma koliko izvorno (pri nastanku) bila demokratska, legitimna i legalna, nužno vremenom postaje birokratska, a njeno ukupno delovanje suprotno stvarnim potrebama i interesima građana koje predstavlja. Upravo takvu kontrolu, u savremenim uslovima, obezbeđuje pravo na pristup informacijama."* (Milenković, 2010, p. 22).

Vršenje ovog prava igra bitnu ulogu u kreiranju političke volje birača, pa se na ovaj način izražava njegova politička funkcija. Pored toga, mogućnost da saznaju informacije, koje su od opšteg interesa za sve članove jedne zajednice, omogućava da građani budu na vreme upoznati sa činjenicama koje mogu imati direktan odraz na kvalitet njihovog života. Mogućnost da sami reaguju, u cilju zaštite svojih prava, zdravlja, bezbednosti, utiče na kvalitet života, sigurnost i pouzdanost u državne organe. U takvim okolnostima građani imaju poverenje prema državnim organima, da oni neće sakrivati informacije koje su opšte dobro, te se na taj način povećava osećaj njegove sigurnosti.

Iako pravo na pristup informaciji i tajnost na prvi pogled deluju kao dve suprotnosti, gde se kod prvog teži da informacija postane dostupna, javna, a kod drugog da se ona sačuva kao poverljiva, dostupna samo užem krugu lica, do problema između ovih prava dolazi samo ako se jedno od prava prekomerno vrši. Balans i proporcionalnost u vršenju ovih prava su osnov uspešnog funkcionisanja državnog aparata i njegovog odnosa sa civilnim društvom.

Shvatanje pojma nacionalne bezbednosti, njenih činilaca i faktora ugrožavanja doživeli su velike promene u proteklih dvadesetak godina. Principi nacionalne bezbednosti i potreba njene zaštite menjali su se, u skladu sa promenama na globalnom nivou, pojavama novih rizika i pretnji, pa su samim tim i metode koje se koriste u ostvarivanju koncepta nacionalne bezbednosti doživele niz promena. U skladu sa tim menjao se i odnos tajnosti prema transparentnosti. Savremeni trend po kome su ljudska prava u strategijama nacionalne bezbednosti zamenila koncept nacionalnih vrednosti izmenio je opseg korisne primene brojnih prava i doneo promenu u njihovim međusobnim odnosima. Ovakve konceptualne promene i trendovi u sferi bezbednsoti su ozbiljne pojave o čijim se prednostima i nedostacima može dugo polemisati. Iz dosadašnje prakse primetna je razlika u pristupu i primeni čitavog ovog koncepta, u zavisnosti od toga da li se on tumači u odnosu na razvijene države, koje predstavljaju značajne političke i bezbednosne činioce na globalnom planu, ili se on tumači u odnosu na manje razvijene, u našem slučaju, zemlje u tranziciji.

Pristup informacijama je prepoznat kao ljudsko i političko pravo u mnogim međunarodnim aktima i deklaracijama. Zato zakonski tekst, koji reguliše pristup informacijama u posedu državnih organa predstavlja svojevrstan garant prava, koje je veoma bitno zbog toga što participira u ostvarivanju šireg kruga prava i sloboda građana na više nivoa. Ovo pravo, kako to nalažu pravna načela, nije neograničeno, ali s obzirom na njegovu važnost, prilikom njegovog ograničavanja, zahteva se ispunjenje jasnih standarda i principa. U cilju zaštite od ograničavanja, ovaj zakon u formi načela predviđa da se nijedna odredba ne sme tumačiti na način, koji bi doveo do ukidanja ili ograničavanja (u većoj meri od one koju sam predviđa u članu 8. stav 1.) prava koja ovaj zakon priznaje i garantuje (Sužbeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010).

Da bi se pravo na informaciju ostvarivalo, neophodno je postojanje uslova koji je naveden u članu 2. *„Informacija od javnog značaja, u smislu ovog zakona, jeste informacija kojom raspolaže organ javne vlasti, nastala u radu ili u vezi sa radom organa javne vlasti, sadržana*

u određenom dokumentu , a odnosi se na sve ono o čemu javnosti ima opravdan interes da zna." (Zakon o slobodnom pristupu informacijama od javnog značaja, Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010). Da bi se pravo uspešno ostvarilo neophodan uslov je opravdan interes javnosti da zna. Taj interes je definisan kroz neoborivu pravnu pretpostavku njegovog postojanja, uvek kada se radi o informacijama u posedu organa javne vlasti koje se odnose na ugrožavanje, zaštitu zdravlja stanovništva i životne sredine (time je ovim informacijama dat poseban značaj), a ako se radi o drugim informacijama, pretpostavka je da interes postoji, ali organ može da dokaže suprotno.

Do ograničenja prava može da dođe tako što će organ, koji odbije zahtev tražitelja, pored ispunjenosti drugih pretpostavki, dokazati ugrožavanje pretežnijeg interesa, u svakom konkretnom slučaju. Posebna zaštita ovog prava, iskazana je i kroz to što je već u Zakonu o tajnosti podataka (Službeni glasnik RS, 104/2009) vaganje pretežnijeg interesa određeno kao parametar koji omogućava označavanje podatka kao tajnog „ *...ako je potreba zaštite interesa Republike Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja."* Zakon o tajnosti podataka(„Sl. glasnik RS" br.104/2009).

Kasnije, kada se traži pristup određenoj informaciji, koja je označena kao tajna, pa je na taj način već jednom prošla test interesa, organ vlasti će ponovo morati da razmotri da li je ograničenje pristupa celishodno ili ne. Sama činjenica u formalnom smislu, da se radi o tajnom podatku nije sama po sebi razlog da se zabrani pristup informaciji, nego podrazumeva sprovođenje trodelnog testa (Šabić, 2012). Iako uživa visok stepen zaštite, ovo pravo nije apsolutno, ono je ograničeno drugim pravima za koja se pretpostavlja da zastupaju pretežniji interes. Sam Zakon o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010) u članovima 9.13. i 14. predviđa ograničenja od pretpostavke prava na pristup u jasno definisanim slučajevima.

Tako tražilac informacije neće biti u mogućnosti da ostvari pravo na pristup informaciji, ako bi time: Ugrozio zivot, zdravlje, sigurnost ili neko drugo važno dobro nekog lica; Ugrozio, omeo ili otežao sprečavanje ili otkrivanje krivičnog dela, optuženje za krivično delo, vođenje pretkrivičnog postupka, vođenje sudskog postupka, izvršenje presude ili sprovođenje kazne ili koji drugi pravno uređeni postupak; Ozbiljno ugrozio odbranu zemlje, nacionalnu ili javnu bezbednost ili međunarodne odnose; Bitno umanjio sposobnost države da upravlja ekonomskim procesimau zemlji, ili bitno otežao ostvarenje opravdanih ekonomskih interesa;

Učinio dostupnim informaciju ili dokument za koju je propisima ili službenim aktom, zasnovanim na zakonu određeno da se čuva kao državna, službena, poslovna ili druga tajna, odnosno koji je dostupan samo određenom krugu lica, a zbog čijeg bi odavanja mogle nastupiti teške pravne ili druge posledice po interese zaštićene zakonom koji pretežu nad interesom za pristup informaciji (Zakon o slobodnom pristupu informacijama od javnog značaja, Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010).

Organ vlasti neće tražiocu omogućiti ostvarivanje prava na pristup informacijama od javnog značaja ako tražilac zloupotrebljava prava na pristup informacijama od javnog značaja, naročito ako je traženje nerazumno, često, kada se ponavlja zahtev za istim ili već dobijenim informacijama, ili kada se traži prevelik broj informacija, kao ni u slučaju ako bi bi time povredio pravo na privatnost, pravo na ugled ili koje drugo pravo lica na koje se tražena informacija lično odnosi (uz uspostavljanje 3 izuzetka). (Zakon o slobodnom pristupu informacijama od javnog značaja, Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010).

Ova ograničenja od prava pristupa prilikom kojih organ javne vlasti mora da ospori pravnu pretpostavku postojanja opravdanog interesa javnosti da zna pokazuju da i ovaj Zakon, iako namenjen ostvarivanju prava javnosti, odnosno pristupa informacijama takođe vodi računa o poverljivosti, privatnosit i tajnosti podataka. Kroz propisivanje ograničenja zakon štiti privatne, poslovne i javne interese od ugrožavanja do koga bi došlo neograničenim pravom pristupa informacijama.

Na osnovu navedenog može se zaključiti da naš pravni sistem poznaje dva paralelna mehanizma zaštite podataka. Prvi, predviđen kroz izuzetke od prava na pristup informacijama i drugi, kroz poseban tretman podataka koji se proglašavaju za tajne podatke. Ovo je argument protiv tvrdnje da se ovde radi o nekakvim oštro suprotstavljenim pravima. Tajnost podataka se pojavljuje formalno, kao jedna od mogućnosti koja može dovesti do isključenja prava na pristup informaciji, iako bi suštinski većina nabrojanih slučajeva u praksi predstavljala tajne podatke po sadržini. I Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009) i Zakon o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010) imaju isti cilj, a to je pretpostavka za usklađenost i zaštitu prava i interesa u pravnom sistemu države. Osnovni zadatak oba zakona je da se u svakom slučaju proceni pretežniji interes i na osnovu toga odredi šta može biti javno, a šta

zaslužuje da ostane rezervisano. Ovo bi bila idealna slika koja bi podrazumevala da se svaki od datih interesa štiti legalnom i legitimnom primenom propisa.

Problem nastaje što su oba ova interesa podložna zloupotrebama. Bliskost politike dodatno komplikuje situaciju, jer će svaka kontrola i prigovor na loše vršenje neko od ovih prava u praksi biti politizovani. Ako se kao polazna tačka uzme da su ova dva prava komplementarna, a ne suprotstavljena, osnovni cilj razrade pravila je pronalaženje mehanizama što bolje kontrole u cilju izbegavanja i predupređivanja zloupotrebe ili necelishodne upotrebe svakog od ovih prava. Jasna i nedvosmislena pravila utiču i na smanjenu mogućnost politizacije spornih slučajeva, iako je apsolutno isključenje političkih uticaja u ovoj oblasti nemoguće.

6.1. Tripartitni test

Kada se radi o pravima koja su zagarantovana međunarodnim pravnim aktima, pa na osnovu toga ulaze i u ustavnu građu mnogih država, prilikom uspostavljanja izuzetaka, odnosno ograničavanja takvih prava neophodan je poseban oprez, odnosno sprovođenje mera koje imaju za cilj da se takvo ograničavanje svede na neophodni minimum.

Pravo na pristup informacijama od javnog značaja je jedno od takvih "zaštićenih" prava koje zbog svoje važnosti zahteva poseban oprez prilikom ograničavanja. Kako ovo pravo predstavlja pravilo, a njegova ograničenja izuzetak, u skladu sa međunarodnim principima i nacionalnim zakonom, prilikom njegovog ograničavanja podrazumeva se sprovođenje tripartitnog testa. Ovaj test je garant da prilikom zahteva za pristup informacijama, državni organi neće po automatizmu odbiti zahtev, ako se on odnosi na nabrojane slučajeve, u kojima potencijalno može doći do ograničenja prava, već da će u skladu sa standardom i načelom iz člana 8. Zakona o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010) preispitati zahtev u svakom konkretnom slučaju.

Organ vlasti nije dužan da omogući pristup, ako su u konkretnom slučaju kumulativno ispunjena tri uslova:
1) Ako je jedan od interesa nabrojanih u Zakonu suprotstavljen interesu tražioca da zna.
2) Ako bi pristupom informaciji suprotan (pretežniji) interes bio ozbiljno povređen.

3) Ako potreba zaštite suprotnog interesa preteže nad potrebom zaštite interesa tražioca za ostvarenje slobode pristupa informacijama, prosuđujući neophodnost uskraćivanja pristupa po merilima demokratskog društva (Milenković, 2010).

Činjenica da je zatražen uvid u informaciju u posedu organa javne vlast,i koja je tajna je samo prvi od uslova na putu ka odluci o onemogućavanju uvida. Ako bi interes zaštite Republike Srbije bio ozbiljno ugrožen takvim pristupom, te na taj način zahtevao zaštitu u odnosu na pravo pristupa i ako bi uskraćivanje bilo u skladu sa merilima demokratskog društva, tek tada bi ta odluka bila legalna i legitimna.

Ovako zamišljen trodelni test je ideal koji često u praksi ostaje u domenu teorije. Praksa Poverenika za pristup informacijama od javnog značaja i zaštitu podataka o ličnosti [10]ukazuje da državni organi u velikom broju slučajeva ne sprovode ovaj test, odnosno da donose rešenja u kojima ne obrazlažu sve elemente testa, koji kumulativno moraju biti ispunjeni da bi pravo pristupa informaciji bilo uskraćeno. Postoji više razloga za ovakvo manjkavo sprovođenje tripartitnog testa. Prvi, najopštiji treba tražiti u nepripremljenosti administracije da se reformiše u smislu otvorenije komunikacije sa civilnim društvom. Ovo je posledica dugogodišnje prakse nepolaganja javnosti računa za rad državnih organa. Da bi se ovakva praksa promenila, neophodno je mnogo rada na reformisanju i obuci državnih organa. Drugi razlog je kadrovska struktura u državnim organima koja je ovde na pravom testu znanja i sposobnosti, jer joj se kao zadatak postavlja jedno složeno pitanje vezano za pravno tumačenje koje je sastavni deo tripartitnog testa. Vaganje pretežnosti interesa najčešće završava tako što je polazna pretpostavka “mi smo u pravu” pretočena u pisanu formu, u vidu odluke kojom se onemogućava pravo uvida. Kao razlog takve odluke najčešće se navodi član 9. Zakona o pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010), što je po pozitivnopravnom rešenju samo prvi signal da se pokrene tripartitni test. Ovo često dovodi do uključivanja Poverenika u sam postupak traženja informacija. Da bi se test uspešno sproveo i omogućila zaštita tajnim podacima neophodno je da državni organi budu dobro upućeni i obučeni za primenu pozitivnog prava, naročito ako u opisu rada imaju i rad sa tajnim podacima. Treći razlog je, što ovakvo zakonsko rešenje i formulacija u sebi nose suviše apstraktnosti. Vaganje pretežnosti interesa, test povrede interesa, neophodnost uskraćivanja pristupa po merilima demokratskog društva, neki su od

[10] U daljem tekstu -Poverenik.

najapstraktinijih pravnih pojmova, čije prisustvo u startu stavlja znak pitanja na dalju kvalitetnu primenu od strane organa javne vlasti država sa mnogo razvijenijom administracijom i većom demokratskom tradicijom. Pored toga, međunarodni principi koji se odnose na bezbednost i pravo na informaciju nalažu da je uslov za ograničenja prava na informaciju da to ograničenje bude propisano zakonom koji je objavljen, nedvosmislen, jasan i precizan kako bi omogućio svakome da razume koja informacija može biti zadržana kao tajna, kojoj se može pristupiti i koje radnje vezane za informacije su sankcionisane. (Transparency international, 2014).

Jedan od prvih koraka ka boljem postupanju sa zahtevima bilo bi sastavljanje upitnika za uspešno sprovođenje ovog testa. Ovaj zadatak bi trebalo da bude poveren nacionalnom telu za rad sa tajnim podacima, a ne svakom organu pojedinačno, kako zbog stručnosti tako i da ne bi dolazilo do različitih tumačenja istog propisa od strane pojedinih državnih organa.

„*Za početak treba utvrditi da li se radi o tajnom podatku ili informaciji kojom raspolaže organ javne vlasti? Da li se utvrđivanjem tajnosti prikriva postojanje teških povreda osnovnih prava čoveka? Da li se utvrđivanjem tajnosti prikriva ugrožavanje ustavnog poretka I bezbednosti Republike Srbije? Da li se utvrđivanjem tajnosti podataka prikriva učinjeno krivično delo za koje se može izreći kazna zatvora u trajanju od pet godina? Da li se utvrđivanjem tajnosti prikriva postojanje krivičnog dela? Da li se utvrđivanjem tajnosti prikriva prekoračenje ovlašćenja? Da li se utvrđivanjem tajnosti prikriva zloupotreba službenog položaja? Da li se utvrđivanjem tajnosti prikriva drugi nezakonit akt? Da li je potreba zaštite interesa Republike Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja? Da li je interes nabrojan u zakonu (čl. 9,13. I 14. Zakona o slobodnom pristupu informacijama od javnog značaja) suprotstavljen interesu tražioca da zna.? Da li bi pristupom ovoj informaciji suprotan interes bio ozbiljno povređen? Da li potreba zaštite suprotnog interesa preteže nad potrebom zaštite interesa tražioca da zna, prosuđujući neophodnost uskraćivanja pristupa po merilima demokratskog društva.“* (Matić, 2014, p. 23).

Ovakav tripartitni test, Zakon o pristupu informacijama od javnog značaja značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010) čini jednim od najliberalnijih, sadrži apstraktne pojmove i zahteva ozbiljnu pravnu analizu. Kod ovog upitnika i davanja odgovora na njega čini se da ostaje sporno razjašnjenje kriterijuma na osnovu kojih će se odgovoriti na

pitanje 9. 11. i 12. Upravo je razlika u tumačenju odgovora na ova pitanja čest predmet spora između Poverenika i organa javne vlasti. Da bi odgovori na ova pitanja bili adekvatno dati neophodno je, pre svega, da je organ javne vlasti od koga je zatražen pristup informaciji, koja je označena kao tajna, na adekvatan način sproveo test povrede interesa koji predviđa Zakon o tajnosti podataka (Službeni glasnik RS, 04/2009) u članu 10. gde se predviđa da pri samom nastanku tajnog dokumenta ovlašćeno lice procenjuje moguću štetu o interes Republike Srbije. Uz to član 11. predviđa da odluka o stvaranju tajnog podatka bude u pisanom obliku i da sadrži obrazloženje. Ovakvo rešenje je pretrpelo brojne kritike stručne javnosti, mahom usmerene na obimnost i umnožavanje dokumentacije, prilikom označavanja tajnih podataka. Pismena odluka sa obrazloženjem, koja prati svaki tajni podatak bitno bi usporavala i otežavala rad organa javne vlasti, naročito onih, koji su veći proizvođači tajnih podataka. Ovaj problem je vezan i za samo poštovanje procedure pri nastanku tajnih dokumenata. Organ javne vlasti, koji stvara tajne podatke će najbolje, prilikom samog nastanka podataka sprovesti test ugrožavanja interesa i to obrazložiti. Ukoliko se to radi kasnije, tek prilikom sprovođenja tripartitnog testa, vremenska distanca može umanjiti kvalitet dokazivanja pretežnosti interesa, prilikom odbijanja zahteva za pristup tajnom podatku. To za sobom u praksi može imati posledicu, da u postupku pred Poverenikom, kao drugostepenim organom, žalba tražioca bude usvojena, a organu naloženo da omogući uvid u takav podatak. Poverenik bi, ipak, kao zaštitnik javnog interesa, a ne interesa jedne od strana, u ovakvim slučajevima trebalo da izvrši vaganje suprotstavljenih interesa i u ovakvom slučaju kada državni organ nije sproveo tripartitni test, ili ga je sporveo na neadekvatan način, te da na taj način spreči da formalin nedostaci dovedu do rešenja kojim se narušava javni interes. Položaj poverenika, kako i sam naziv organa kaže, nije poistovećen sa funkcijom sudije ili arbitra u slučaju suprotstavljanja interesa, već mu je obaveza prvenstveno procena i zaštita javnog interesa. (Gajin 2012). Ovaj položaj u ruke poverenika stavlja složen zadatak, jer mora da proceni da li tajni podatak zaslužuje da bude označen kao tajni, ne samo sa aspekta zaštite zagarantovanih građanskih prava, nego i sa aspekta bezbednosti. Poznavanje ovako usko stručnih potreba je težak zadak u čijem ispunjenju se moraju uzeti u obzir i stavovi onih državnih organa koji se prvenstveno bave zaštitom nacionalne bezbednosti.

Obzirom na zakonski položaj Poverenika kao nezavisnog organa, on bi morao da vodi računa o javnom interesu (dakle i o bezbednosnim potrebama) u svakom konkretnom slučaju kada se pokrene postupak pred njim, što znači da formalni nedostaci ne bi smeli da utiču na odluku Poverenika po žalbi. U odnosu na ovo, treba razmotriti da li je adekvatno samo jezičko

tumačenje zakonske odredbe o pisanoj formi odluke o označavanju tajnog podatka o čemu će biti više reči u drugom delu rada.

Pitanje potrebe u demokratskom društvu je osim pravnog i političko pitanje. Argumenti za omogućavanje prava pristupa su ti, da se tako omogućava konstruktivna otvorena javna debata o javnim interesima, povećanje pouzdanosti Vlada, omogućava kontrola kroz uvid u trošenje javnih sredstava, otkrivaju razlozi vladinih odluka, otkrivaju pretnje po javno zdravlje i život. (Transparency International, 2014). Ovi razlozi su kako se vidi, pored zahteva koji se odnose na ostvarivanje zagarantovanih prava i direktno povezani sa čisto političkim pitanjima. Potreba u demokratskom društvu se često određuje kroz negaciju, odnosno naglašavanjem, kada u demokratskom društvu nije neophodno da dođe do ograničavanja. To bi bili slučajevi, ako se time ionako ne mogu zaštiti interesi nabrojani u zakonu, ako se njihova zaštita može podjednako ostvariti i na drugi način, ili ako se time uskraćuje sloboda pristupa u većoj meri od onoga što je dovoljno za zaštitu navedenih interesa (Milenković, 2010).

Da li se ograničavanjem mogu ili ne zaštiti pobrojani interesi, ili da li se njihova zaštita može ostvariti podjednako bez ograničavanja ovog prava su hipotetička pitanja koja zavise od mnogo faktora, naročito kada je reč o sistemu bezbednosti. Kako transparentnost ovde dolazi u kontakt sa bezbednošću, čak i uz pretpostavku visoke stručnosti, jasno je da ovde ostaje dosta slobodnog prostora za različita tumačenja. U principu će od političkopravnih polazišta naklonjenijih otvorenosti ili tajnosti zavisiti ishod sučeljavanja prava pristupa informacijama i zaštite nekog od pretežnijih interesa.

7. ZAKON O TAJNOSTI PODATAKA REPUBLIKE SRBIJE- OTVORENA PITANJA.

Zakon o tajnosti podataka Republike Srbije (Službeni glasnik, 104/2009) je usvojen 2009. godine, a stupio je na snagu 1.1.2010. godine. Prvo što se može zapaziti je anahronost u donošenju zakona, koji čine normativnu trijadu koja reguliše sferu podataka i informacija. Zakon o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009, 36/2010) je prvi donet još 2004. godine. Zatim je usledilo donošenje Zakona o zaštiti podataka o ličnosti (Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012) 2008. da bi Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009) bio poslednji donet. Ova obrnuta logika regulisanja ovako važne oblasti, kao što su podaci, nije redak slučaj za države u tranziciji, koje nakon rušenja autokratskog režima, izložene brojnim inostranim uticajima i pritiscima, nastoje da nadoknade izgubljeno vreme i požure sa "demokratizacijom", makar to bilo i samo deklarativno, čak u dosta slučajeva i štetno po suštinsko uvođenje reda i izgradnju funkcionalnog pravnog i političkog sistema. Brojni problemi, sa kojima sa kojima se susreo još pri nastajanju, a i kasnije prilikom implementacije u pravni sistem Srbije su u velikoj meri faktički, do danas, onemogućili njegovu primenu u punom obimu.

Prvi i najuočljiviji problem sa kojim se zakon susreo je taj što predstavlja prvi propis, nakon dugog niza godina koji reguliše oblast tajnih podataka uopšte. Brojni propisi kojima su organi uređivali ovu oblast nasleđeni su još iz SFRJ, na principu autonomne regulative u svakom od resora (Ministarstvo unutrašnjih poslova, Ministranstvo vanjskih poslova, Ministarstvo odbrane, Vlada). Mnogi ga zato smatraju krovnim zakonom. To se može tumačiti samo sa aspekta uloge, koju mu je zakonodavac namenio, a to je da na jednistven način reguliše nastanak i zaštitu tajnih podataka, kao i da se odredi centralno telo za rad, sa stranim tajnim podacima, što predstavlja međunarodni standard u ovoj oblasti, a ne i po pitanju hijerarhijskog odnosa prema drugim zakonima u ovoj oblasti-Zakonu o zaštiti podataka o ličnosti (Službeni glasnik RS, 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012) i Zakonu o slobodnom pristupu informacijama od javnog značaja (Službeni glasnik RS, 120/2004, 54/2007, 104/2009 i 36/2010). Ovi zakoni moraju biti usklađeni u potpunosti i tako obezbediti pretpostavke za ostvarivanje demokratskih načela transparentnosti organa javne vlasti, potrebe zaštite interesa nacionalne bezbednosti i prava pojedinca da mu se garantuje zaštita podatka o ličnosti.

„Naime, članom 14. zakona određena su četiri stepena tajnosti („Državna tajna", „Strogo poverljivo", „Poverljivo" i „Interno"), pri čemu je nedvosmisleno rečeno da se za određivanje stepena tajnosti mogu koristiti samo navedeni stepeni. Dakle, ne i neki drugi. Isto se odnosi i na organe nedležne za sprovođenje, kontrolu i nadzor nad primenom zakona, što znači da je zakon nedvosmislen, nije predviđena mogućnost da se meterija koja se odnosi na tajnost podataka drugačije uređuje posebnim zakonom. U tom smislu, Zakon o tajnosti podataka u suštini predstavlja „krovni zakon" u tojoblasti, što znači da bi drugi zakoni morali biti usklađeni sa njim kada uređuju pitanja vezana za tajnostpodataka." (Petrović, 2014. p. 67)

U međuvremenu, iako van svih rokova, doneti su gotovo svi podzakonski akti predviđeni u zakonskom tekstu kako bi se omogućila realna primena samih normi Zakona o tajnosti podataka:

-Uredba o obrascima bezbednosnih upitnika („Službeni glasnik RS" , 30/10).

-Uredba o sadržini, obliku i načinu dostavljanja sertifikata za pristup tajnim podacima („Službeni glasnik RS" , 54/10).

-Uredba o određivanju poslova bezbednosne zaštite određenih lica i objekata (Službeni glasnik RS" , 72/10)

-Uredba o uvećanju plate državnih službenika i nameštenika koji obavljaju poslove u vezi sa zaštitom tajnih podataka u Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka i Ministarstvu pravde („Službeni glasnik RS", 79/10).

-Uredba o sadržini, obliku i načinu vođenja evidencija za prstup tajnim podacima („Službeni glasnik RS", 89/10).

-Uredba o načinu i postupku označavanja tajnosti podataka, odnosno dokumenata („Službeni glasnik RS", 8/11).

-Uredba o posebnm merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima („Službeni glasnik RS", 53/11)

-Uredba o posebnim merama nadzora nad postupanjem sa tajnim podacima („Službeni glasnik RS", 90/11).

-Uredba o posebnim merama fizičko-tehničke zaštite tajnih podataka („Službeni glasnik RS", 97/11).

-Uredba o bližim kriterijumima za određivanje stepena tajnosti "Državna tajna" i "Strogo poverljivo" („Službeni glasnik RS", 46/13).

-Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” i “ Interno” u Bezbednosno informativnoj agenciji („Službeni glasnik RS“, 70/13).
- Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” i “ Interno” u Kancelariji saveta za nacionalnu bezbednost I zaštitu tajnih podataka („Službeni glasnik RS“, 86/13).
- Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” i “ Interno” u Ministarstvu unutrašnjih poslova („ Službeni glasnik RS“, 105/13).
-Uredba o posebnim merama zaštite tajnih podataka koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa („Službeni glasnik RS“, 63/13).
-Pravilnik o službenoj legitimaciji i načinu rada lica ovlašćenih za vršenje nadzora nad sprovođenjem zakona („Službeni glasnik RS“ , 85/2013).
-Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” i “ Interno” u organima javne vlasti („Službeni glasnik RS“, 79/14).
- Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” i “ Interno” u Ministarstvu odbrane. („Službeni glasnik RS“, 66/14).
- Uredba o postupku javne nabavke u oblasti bezbednosti („Službeni glasnik RS“, 82/14).

Pravna, politička priroda i želja zakonodavca da u ovoj oblasti donese novi propis kojim na celovit i unifikovan način određuje šta i na koji način može biti tajna i tako približi ovu oblast propisima EU i oslobodi se čitave grupe različitih propisa, koji su autonomno regulisali tajnost podataka, mnogo je više od same normativne aktivnosti, jer kao prethodnicu podrazumeva reformu sistema bezbednosti i celokupne državne uprave Republike Srbije. Da bi njegova primena i idejna rešenja bila realno sprovodljiva neophodno je mnogo rada na sistemu bezbednosti, od prilagođavanja državnih organa na rad u demokratskim uslovima i prisustvo civilne kontrole, preko restrukturiranja i nastanka novih tela u ovom sistemu do promene pravila i navikavanja angažovanih službenika državne uprave na drugi sistem rada.

Kako ovaj zakon donosi novine u smislu jedinstvene tajne klasifikacije, potrebno je usvojiti izmene i dopune ili potpuno nove zakonske tekstove u nizu oblasti, koje regulišu pitanje tajnosti na drugi način. Takođe rešenja zakona vezana za mere zaštite tajnih podataka u daljoj razradi, putem podzakonskih akata predstavljaju materiju informacione bezbednosti koja još uvek nije regulisana državnom strategijom ili drugim opštim pravnim aktom.

Složenost ovakvog posla prirodno ne može proći bez teškoća i neophodnog vremena, koje je potrebno za usklađivanje sistema bezbednosti i državne uprave, koji po prirodi ne spadaju u najfleksibilnije i otvorenije za prihvatanje novina u načinu rada. Kao dodatni problem se pojavljuje praksa ponašanja i međusobnih odnosa organa javne vlasti koja se ogleda u visokom stepenu zatvorenosti i nedostatka koordinacije. Takav ignorantski odnos organa izvršne vlasti prema zakonskom tekstu potkrepljen je time što je i sam zakonodavac, nakon usvajanja ovog zakona i formalno usvojenog novog sistema stepenovanja tajnih podataka u kasnije usvojenim zakonskim tekstovima zadržao primenu starih pojmova (službena tajna).

Imajući u vidu opsežnost opisanog posla i vreme koje ono podrazumeva, teško je shvatljiva ideja tvoraca zakona, da za sam zakonski tekst, kao pretpostavku svoje primene podrazumeva donošenje velikog broja pratećih podzakonskih akata i time učini implementaciju ovog zakona još komplikovanijom. *„Još u vreme donošenja zakona upozoravao sam da je veliki problem to što je za njegovu primenu neophodno doneti enormno veliki broj podzakonskih akata. Potreba za donošenjem preterano velikog broja podzakonskih akata kao pretpostavke za primenu zakona, uvek je, generalno, problem. A u uslovima našeg legislativnog procesa u kome je docnja Vlade i drugih subjekata nadležnih za donošenje podzakonskih akata postala gotovo pravilo, to je još veći problem"* (Šabić, 2014, p.34).

Brojni problemi u primeni ovog zakona nagoveštavaju da je realno očekivati da se izmene i dopune, ako ne i novi zakonski tekst nađu u skorije vreme u skupštinskoj proceduri. Ipak i ovavkvo rešenje, iako ne idealno je ipak prvi korak u regulisanju jedne važne oblasti koja je dugi niz godina bila zapuštena i prepuštena nasleđenoj praksi i propisima SFRJ, SRJ, a negde i potpunom zanemarivanju.

Zakon o tajnosti podataka (Službeni glasnik, 104/2009) ima složenu strukturu, izrađenu po ugledu na češki zakon, ali za razliku od češkog zakona, koji je znatno obimniji, zbog toga što većinu pitanja iz ove materije stavlja na zakonski nivo, ovde se radi o dosta sažetijem zakonskom tekstu koji prati velik broj podzakonskih akata. Mana ovog zakona je svakako i upotreba previse apstraktnih pravila i pojmova, koja zahteva određeni nivo pravničkog znanja, odnosno poznavanja materije koja se uređuje.

U regulisanju ovako osetljivih oblasti, radi lakšeg razumevanja normi poželjno je izdvajanje onih normi, koje imaju značaj načela u ovoj oblasti, a ne njihovo samo usputno pominjanje kroz članove koji u prvi plan stavljaju druge stvari.

Struktura zakona se može podeliti po oblastima regulisanja, pa će u skladu sa tim kroz postavljanje određenih pravnih dilema i uporedno pravnu analizu ovaj rad pratiti tu podelu i kroz kritički pristup, koji bi išao od prigovora vezanih za neke formulacije, odnosno formalnopravne nedostatke do razmatranja drugačijih suštinskih materijalno pravnih rešenja vezanih za položaj i nadležnost organa i kontrolu nad sprovođenjem samog zakona.

7.1. Podatak koji se može odrediti kao tajni.

Prvo pitanje koje se logično postavlja, kada se govori o regulisanju tajnosti podataka je, koje kriterijume treba da ispunjava jedan podatak, da bi od strane organa javne vlasti mogao biti označen kao tajni. Definisanje ovog pitanja ima mnogo veći značaj od samog formalnopravnog određivanja uslova ili definicije, jer se preko njega može osetiti političko pravno opredeljenje vlasti u vaganju između principa transparentnosti rada državnih organa i tajnosti, odnosno odnosa između transparentnosti i zaštite nacionalne, odnosno državne bezbednosti. Odgovor na ovo pitanje uglavnom daje sam zakon, u prvim članovima, gde suštinski definiše razloge, zbog kojih postoji potreba označavanja podataka kao tajnih, kao i uslove koji moraju biti ispunjeni da bi se podatak smatrao podobnim da se na njega stavi oznaka tajnosti.

Suština tajnosti podataka je da se zaštite određeni bezbednosno značajni podaci, čijim bi otkrivanjem i upoznavanjem neodređenog broja lica sa njima bila ugrožena bezbednost države, saveza, unije. To su informacije i podaci koji se posredno ili neposredno odnose na najvažnije nacionalne interese koje država štiti izgradnjom i koordinacijom službi koje čine sistem bezbednosti. Polazna tačka kod definisanja tajnog podatka je uglavnom zaštita državnih odnosno nacionalnih interesa.

„... nacionalni interes je operacionalizacija osnovnih potreba nacije ili države i neposredno se ili posredno odnosi na njihovu bezbednost... Vitalni nacionalni interesi (poput samoočuvanja, zaštite suvereniteta, teritorijalnog i nacionalnog integriteta, vojne bezbednosti)

retko su kad predmet pregovaranja i radi njihove zaštite nacija i država su spremne da angažuju sve raspoložive snage" (Mijalković, 2011, pp. 154-155).

Uporednom analizom normativnih akata koji regulišu ovu materiju, lako je utvrditi da se u uvodnim delovima zakona nalaze odredbe, koje propisuju koje se to informacije mogu označiti kao tajne i na koji način se to vrši. Tu se sreću uglavnom slične formulacije i rešenja. Često se napominje neposredno da su to informacije čije bi neovlašćeno otkrivanje ili zloupotreba ugrozili nacionalnu bezbednost, uz nabrajanje oblasti iz kojih takvi podaci mogu poticati, odakle se posredno zaključuje da se radi o osetljivim i bezbednosno važnim informacijama. Tako se u izvršnoj uredbi Sjedinjenih Država (https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information) definiše da su to informacije čije bi neovlašćeno otkrivanje, sa osnovanom izvesnošću prouzrokovalo štetu, po nacionalnu bezbednost, a ako se odnose na oblasti kao što su vojni planovi i operacije, informacije inostranih vlada, obaveštajne aktivnosti

Švedski zakon o tajnosti i pristupu javnim informacijama (http://www.government.se/information-material/2009/09/public-access-to-information-and-secrecy-act/) navodi da se kao tajne moraju označiti informacije koje su od velike važnosti za nacionalnu bezbednost.

„*...podaci iz djelokruga državnih tijela u području obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva ukoliko su podaci od sigurnosnog interesa za Republiku Hrvatsku."* (Zakon o tajnosti podataka Republike Hrvatske ,Narodne Novine RH, 108/96).

Češki zakon o tajnosti (http://www.nbu.cz/en/legislation/), tajnu informaciju definiše kao svaku onu, čije bi neovlašćeno otkrivanje ili zloupotreba moglo naneti štetu ili nepovoljno uticati na interese Češke republike. Da bi potom definisao interese Češke republike (očuvanje ustavnog poretka, suvereniteta i teritorijalnog integriteta, unutrašnje bezbednosti, ispunjavanje međunarodnih obaveza i odbrana zemlje, zaštita ekonomije i zaštita života i zdravlja građana), a potom i štetu po interese. (http://www.nbu.cz/en/legislation/). Zakonodavac se ovde odlučio da krene od definisanih državnih interesa kojima se nanosi šteta ukoliko dođe do otkrivanja tajnih podataka neovlašćenim licima. Nanošenje štete ovim interesima nije ništa drugo, osim ugrožavanja nacionalne bezbednosti, a podaci koji se klasifikuju vezani su za ove najviše

interese, te predstavljaju činjenice od značaja za bezbednost. Češki zakonodavac se odlučio za složeniji pristup i zakon koji u potpunosti, do tančina (u nekim delovima čak detalja koji generalno ne spadaju u zakonsku materiju), reguliše sve aspekte nastanka i zaštite tajnih podataka uz uvođenje centralnog nacionalnog tela za rad sa tajnim podacima kao posebne službe bezbednosti (NSA ovlašćenja i zadaci), razmene podataka sa drugim članicama NATO i EU (http://www.nbu.cz/en/legislation/)

Ovo je primer opširnog zakona koji na sveobuhvatan način pokušava da reguliše tajnost i zaštitu tajnih podataka. Takav pristup je jedan od načina za uvođenje jedinstvenog sistema rada svih državnih organa, ne ostavljajući prostora za različita tumačenja i odstupanja kod onih na koje se zakon odnosi. Izrada kataloga tajnih podataka koji predstavlja ili deo zakona, ili njegov prateći akt, uz sistematizaciju po oblastima u kojima se tajnost primenjuje je još jedan od pokazatelja da u post-komunističkim državama, pored pravnih dilema vezanih za odmeravanje interesa, procenu moguće štete po nacionalne interese, koje spadaju u pravna pitanja visokog nivoa apstraktnosti, mora da se radi i na edukaciji i disciplinovanju administracije (Transparency International, 2014). Uz to, uspostavljanje centralnog nacionalnog tela za rad, sa tajnim podacima sa kapacitetima i ovlašćenjima jedne čitave nove službe opštebezbednosnog karaktera je jedno od mogućih adekvatnih rešenja za implementaciju novih propisa i načina rada, naročito kada su u pitanju zemlje u tranziciji.

Zakon o tajnosti podataka Republike Srbije (Službeni glasnik RS, 104/2009), na sličan način kao češki zakon kao polaznu tačku uzima interese Republike Srbije. U članu 8. definiše kao podatke, koji mogu biti podobni da budu označeni kao tajni, one koji su od interesa za Republiku Srbiju, a koji se odnose na teritorijalni integritet i suverenost, zaštitu ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalnu i javnu bezbednost, odbranu, unutrašnje poslove i spoljne poslove, a čijim bi otkrivanjem neovlašćenom licu nastala šteta, po interese Republike Srbije, ako je potreba zaštite interesa Republike Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja. Zatim u stavu 2. istog člana navodi oblasti na koje se naročito podatak odnosi. Odmah se može primetiti da se sintagma "podatak od interesa za Republiku Srbiju" pojavljuje mnogo puta, ali ni jedan član ne definiše interese Republike Srbije, kao što je to slučaj u češkom zakonu (http://www.nbu.cz/en/legislation/). Član 8. takođe kao uslov navodi da se klasifikacija može vršiti, ako je potreba zaštite interesa Republike Srbije (koji nisu definisani u ovom zakonu) pretežnija od interesa za slobodan pristup informacijama od javnog značaja. Interes javnosti

da zna, kao i izuzeci od prava na slobodan pristup definisani su u Zakonu o slobodnom pristupu informacijama od javnog značaja („Sl. glasnik RS“, br. 120/2004, 54/2007, 104/2009 i 36/2010). Zakonopisac ovom prilikom, na samom početku zakona, gde je potrebno na jasan i koncizan način utvrditi osnovno pitanje (šta to uopšte može biti označeno kao tajni podatak), umesto da odnos sa pravom pristupa informacijama od javnog značaja utvrdi u formi načela, koristi materijalnopravnu odredbu, kojom upućuje na drugi zakonski tekst. tj. ukazuje na potrebu preduzimanja tripartitnog testa odmeravanja interesa javnosti da zna i drugih suprotstavljenih interesa. Može se primetiti da Zakon o tajnosti („Službeni glasnik“, broj 104/2009) već u prvom delu nije ispunio jedan od osnovnih međunarodnih principa iz ove oblasti, a to je da zakonski tekst, koji uvodi ograničenje ustavnih prava mora biti jasan i nedvosmislen kako bi svakom čitaocu mogao da omogući tumačenje koje informacije mogu biti označene kao tajne i izuzete od prava da budu dostupne javnosti.

Ako se uzme u obzir da je 2009. usvojena i Strategija nacionalne bezbednosti („Službeni glasnik, broj 88/2009) u kojoj su definisane nacionalne vrednosti i interesi, zatim da su usvojeni zakoni kojima se krenulo u reformu sistema bezbednosti i odbrane - Zakon o osnovama uređenja službi bezbednosti republike Srbije (Službeni glasnik RS, 116/2007 i 72/2012) , Zakon o Bezbednosno-informativnoj agenciji (Službeni glasnik RS, 42/2002, 111/2009, 65/2014-odluka US i 66/2014), Zakon o vojnobezbednosnoj i vojnoobaveštajnoj agenciji (Službeni glasnik RS, 88/2009, 55/2012. Odluka US i 17/2013) i stvaranjem tela za koordinaciju i obavljanje zadataka iz oblasti nacionalne bezbednosti (Savet za nacionalnu bezbednost) jasno je da je i kod nas prihvaćen savremeni koncept nacionalne bezbednosti, koji podrazumeva sveobuhvatnost pojma odnosno podrazumeva bezbednost države, čitavog društva kao i učešće u globalnoj bezbednosti.

„Nacionalna bezbednost danas obuhvata bezbednost društva (bez obzira na etničko, versko, rasno i ideološko opredeljenje njegovih članova) i bezbednost države ali i njihovo participiranje u međunarodnoj i globalnoj bezbednosti." (Mijalković, 2011, p.160)

„Ovi podaci se u praksi najčešće odnose na nacionalnu bezbednost u najširem smislu te reči, počev od opasnosti da će biti ugrožena bezbednost zemlje pa sve do mogućnosti da će biti ugroženo otkrivanje nekog krivičnog dela."(Popović, 2009, p. 4).

Razlozi iz kojih zakonopisac nije odredio pojam tajnog podatka, vezujući ga za ugrožavanje nacionalne bezbednosti, već je išao na određenje ovog pojma, preko prilično konfuznog određivanja "interesa Republike Srbije" mogli bi se tražiti možda u prebrzom pokušaju reforme sistema bezbednosti i nedovoljnoj usklađenosti zakona, koji su doneti u ovoj oblasti sa realnom situacijom. Pojam"interes Republike Srbije", koji je pri tom, u samom zakonu široko i neprecizno formulisan i vezivanje pojma tajnog podatka za procenu pretežnosti dva interesa od kojih je jedan definisan u drugom zakonskom tekstu, donosi već u prvim članovima ovom zakonu visok nivo apstraktnosti koji po pravilu u tumačenju zahteva zavidan nivo pravničkog znanja, što kada se uzmu u obzir i neke kasnije odredbe, kao i kumulativna primena podzakonskih propisa koji detaljnije razrađuju pravila same klasifikacije, ozbiljno dovodi u pitanje mogućnost pravilne procene i tumačenja, a samim tim i realne primene rešenja ovog zakona u praksi.

„Tumačenje je sastavni deo procesa saznanja pravne norme i to jedan od najvažnijih (ako ne i najvažniji) delova tog procesa... da bi pravna norma , dakle delovala, potrebno je da je subjekt na čije se ponašanje ona odnosi najpre sazna... norma je pravilno saznata tek ako je pravilno, tačno protumačena... Stoga je potrebno obratiti pažnju na pravilno tumačenje i pripremu ljudi za ovo, osobito kada su u pitanju državni organi..." (Košutić, Lukić, 2007, p. 259).

Pri izradi zakona, po uzoru na zakone drugih država, mora se poći od detaljne analize sličnosti i kompatibilnosti širih društvenih i političkih uslova, kao i mogućnosti tih pravnih sistema. Preuzimanje jednog modela regulisanja, a zatim njegove izmene i dorađivanje u domaćem pravnom sistemu mogu dovesti do ozbiljnih problema u funkcionisanju pravnog sistema. Pravni transplanti su u praksi pokazali da čak i uz pretpostavku vrhunskog pravničkog znanja i analize, svoje nedostatke mogu pokazati tek “oživljavanjem” normi i njihovom primenom u pozitivnom pravu jedne države.

7.2. Ko i kako stvara tajne podatke?

Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009) u članu 9. propisuje ko su ovlašćena lica za određivanje tajnosti podataka. Kao ovlašćena lica zakon navodi:

1. *predsednika Narodne skupštine;*
2. *predsednika Republike*;
3. *predsednika Vlade;*
4. *rukovodioca organa javne vlasti;*
5. *izabrani, postavljeni ili imenovani funkcioneri javne vlasti koji je za određivanje tajnih podataka ovlašćen zakonom, odnosno propisom donetim na osnovu zakona ili ga je za to pismeno ovlastio rukovodilac organa javne vlasti;*
6. *Lice zaposleno u organu javne vlasti koje je za to pismeno ovlastio rukovodilac tog organa;*

U prvom delu Zakona o tajnosti podataka (Službeni glasnik RS, 104/2009), stoji da su stepeni tajnosti za označavanje tajnog podatka:

"DRŽAVNA TAJNA"
"STROGO POVERLJIVO"
"POVERLJIVO"
"INTERNO"

Ovi stupnjevi tajnosti su pored mnogih država standard i u EU i NATO. Pored svrsishodnosti, koju je pokazala podela na četiri stupnja tajnosti, prihvatanje ove podele olakšava razmenu tajnih dokumenata sa državama članicama EU i NATO jer se odvija po automatizmu i ne zahteva dodatni posao procene stepena tajnosti stranog podatka u domaćem pravnom sistemu. Tako zakon predviđa ekvivalente u domaćim stepenima tajnosti i to:

TOP SECRET-DRŽAVNA TAJNA
SECRET-STROGO POVERLJIVO
CONFIDENTAL-POVERLJIVO
RESTRICTED-INTERNO

Postupak stvaranja tajnih podataka podrazumeva da pri određivanju stepena tajnosti lice koje je ovlašćeno za klasifikaciju proceni moguću štetu po interese Republike Srbije i na osnovu te procene donese odluku o stavljanju oznake tajnosti na dokument. Test povrede interesa obično ima dve komponente, težinu povrede interesa i verovatnoću da takva povreda nastupi**.** (Transparency International, 2014). Što su ova dva faktora veća to potreba zaštite podatka nalaže viši nivo stepenovanja.

Kada se radi o stepenima tajnosti "DRŽAVNA TAJNA" i "STROGO POVERLJIVO**"** oni se primenjuje radi sprečavanja nastanka neotklonjive teške štete po interese Republike Srbije, odnosno radi sprečavanja nastanka teške štete po interese Republike Srbije. Kod stepena tajnosti "POVERLJIVO" odnosno "INTERNO" radi se o sprečavanju nastanka štete po interese Republike Srbije, odnosno štete za rad, obavljanje zadataka i poslova organa javne vlasti. Bliži kriterijumi za klasifikaciju tajnih podataka sadržani su u uredbama koje je Vlada donela, sa popriličnim zakašnjenjem u odnosu na zakonom predviđen rok od 6 meseci (Uredbe o bližim kriterijumima za određivanje stepena tajnosti "državna tajna" i "strogo poverljivo" i "poverljivo" i "interno"). Uredbe nastoje da reše dilemu tumačenja pravnih standarda, kao što su pojmovi neotklonjiva teška šteta i teška šteta.

Odluka o označavanju podatka stepenom tajnosti se donosi u pisanom obliku, sa obrazloženjem. Kao što je već pomenuto, kod razmatranja tripartitnog testa koji predviđa Zakon o slobodnom pristupu informacijama od javnog značaja („Službeni glasnik", broj 120/2004, 54/2007, 104/2009 i 36/2010) ovakvo rešenje je prilično diskutabilno, sa aspekta usporavanja procedure i obimnosti dokumentacije. *„Nesumnjivo je da bi ovakav pristup doveo do hiperprodukcije prateće dokumentacije u vezi sa aktom kojim se određuje tajni podatak."* (Stanković, 2014. p. 102).

Vlada je relativizovala ovu zakonsku obavezu time što u uredbama, u kojima razrađuje bliže kritetijume za označavanje tajnih podataka određenim stepenom tajnosti pominje samo odluku o određivanju stepena tajnosti, koja se donosi na osnovu predviđenih kriterijuma i uz prethodnu procenu moguće štete po interes Republike Srbije. Iz ovakvog rešenja sledi da organi javne vlasti neće prilikom svake odluke o označavanju tajnih podataka donositi poseban upravni akt o toj odluci, već da je ta odluka zbirnog karaktera, te da predstavlja katalog tajnih podataka koji bi trebalo da nose odgovarajuću oznaku tajnosti. (Stanković,

2014, p.102) .Kao potkrepljenje ovog stava je i proces izrade kataloga podataka, koji treba da budu označeni odgovarajućim stepenima tajnosti u ministarstvima kao i izrada lista „POTREBNO DA ZNA“. Organi javne vlasti rade na implementaciji propisa vezanih za tajnost podataka, donošenjem unutrašnjih akata, na osnovu uredaba Vlade. Iako je jasno da se radi o logičnom rešenju, koje je u praksi primenljivo i ovde se vidi da postoji raskorak između zakonski definisanog pravila i rešenja koja se u praksi primenjuju[11].

Rešenje sa izradom kataloga tajnih podataka, koje podrazumeva i izradu registra je naročito pogodno za izbegavanje preširoke primene tajnosti i rad administracije koja nije naviknuta, ni obučena za direktnu primenu zakonskih rešenja. Ovakvi katalozi imaju funkciju pravilnika ili vodiča za označavanje određenim stepenom tajnosti jer razrađuju zakonska pravila objašnjavajući konkretno koji podatak zaslužuje koji stepen tajnosti. (Transparency International, 2014).

Tako češki zakon o tajnosti (http://www.nbu.cz/en/legislation/) u članu 139. predviđa da nacionalni organ za rad sa tajnim podacima (NSA[12]), treba da predloži vladi listu informacija koje treba da budu klasifikovane, koju vlada usvaja dekretom, a koja služi za razvrstavanje informacija u jedan od nivoa tajnosti predviđenih zakonom. Kako domaće zakonodavstvo u ovoj oblasti ne predviđa postojanje centralnog nacionalnog tela za rad sa tajnim podacima koje bi sastavilo katalog sa tipologijom oblasti i činjenica koji daje odgovor na pitanje šta treba označiti kao tajno i kojim stepenom tajnosti, a slični katalozi nisu još uvek sačinjeni u svakom od resora pojedinačno, primena zakona je ozbiljno dovedena u pitanje.

Ovlašćenje za označavanje podataka stepenima tajnosti spada u rang najviših ovlašćenja, s obzirom da se njegovom primenom ograničava ustavno pravo građana. Ovo je i razlog što će se ovakvo nabrajanje lica sa ovlašćenjem za označavanje tajnih podataka naći u gotovo svim

[11] Zakon o tajnosti podataka (“Službeni glasnik RS” 104/2009) u čl. 11. stav 4. Jasno definiše da se odluka o određivanju stepena tajnosti donosi na osnovu propsanih kriterijuma u pisanom obliku sa obrazloženjem. Ovakvo zakonsko rešenje koje zahteva određenu formu (pismenu) iako nelogično sa aspekta praktične primene bitno je izmenjeno podzakonskim aktima. Treba obratiti pažnju i na to da bi predviđeni podzakonski akti trebalo da razrade sasvim drugo pitanje (definisano drugim članovima zakona).

[12] NSA- National security authority- pojam vezan za NATO i EU sisteme tajnih podataka koji podrazumevaju centralizaciju kada su u pitanju organi država članica koji se bave zaštitom i razmenom tajnih podataka. Potrebno je razlikovati ovlašćenje od NSA- obaveštajne agencije američke Vlade.

normativnim tekstovima koji uređuju ovo pitanje u različitim nacionalnim pravnim sistemima. Međunarodni standardi podrazumevaju da ovakvo ovlašćenje bude predviđeno zakonom, pa je mišljenje da bi i organi, koji su u zakonu označeni kao ovlašćena lica za određivanje tajnosti podataka trebalo da budu oni koji svoja ovlašćenja i moć crpu na osnovu akata parlamenta. Pravilo je da tvorac tajnog dokumenta određuje njegovu upotrebu, drži ga u svom posedu, vodi evidenciju, sprovodi mere zaštite, odlučuje o ukidanju oznake tajnosti, pravi kopije, prevodi dokument, omogućava pristup podacima. Delegiranje ovih ovlašćenja je stoga strogo kontrolisano. Podrazumeva se primena principa *delegatus delegare non potest*,[13]

U Zakonu o tajnosti podataka (Službeni glasnik RS, 104/2009), na osnovu člana 9. na prvi pogled može da se zaključi da se zakonodavac opredelio za taksativno nabrajanje ovlašćenih lica, za označavanje tajnih podataka. Precizno navođenje lica koja mogu klasifikovati tajne podatke je pogodno rešenje naročito za "mlade" administracije, koje nisu dovršile proces tranzicije i one koje se po prvi put sreću sa novim pravilima vezanim za jedinstven sistem označavanja tajnih podataka. Međutim, lista našeg zakonodavca je jasna samo do četvrte tačke, kada počinju problemi i nejasnoće. U zakonu se koristi pojam organ javne vlasti, čime se označava „*državni organ, organ teritorijalne autonomije, organ jedinice lokalne samouprave, organizacija kojoj je povereno vršenje javnih ovlašćenja kao i pravna lica koje osniva državni organ ili se finansira u celini, odnosno u pretežnom delu iz budžeta*."(Zakon o tajnosti, Sužbeni glasnsik RS, 104/2009). Zakonodavac dakle pored državnih organa u listu ovlašćenih, za označavanje tajnih podataka svrstava i organe lokalne samouprave i pravna lica, koja su osnovana od strane državnog organa ili se finansiraju iz budžeta. Ovo su u principu pravna lica koja obavljaju delatnosti od značaja za odbranu i bezbednost. Regulisanje ovog pitanja je oblast industrijske bezbednosti, koja uređuje pristup i razmenu tajnih podataka između države i preduzeća. I pored ovako formulisanog ovlašćenja za klasifikaciju odakle se samo nazire oblast industrijske bezbednosti, zakon ostaje nem po pitanju dalje razrade ovih pravila.

Ono što je odmah uočljivo je to da se nigde ne definiše ko može označiti podatke kojim stepenom tajnosti. Podela na četiri stepena tajnosti i postoji zbog različitog značaja podataka i

[13] Princip podrazumeva da ovlašćenje može dati samo onaj ko svoje ovlašćenje crpe sa izvora u ovom slučaju iz samog zakona. Dalji prenos ovlašćenja od strane lica na koje je ovlašćenje preneto od strane originernog imaoca ovlašćenja nije moguće.

eventualnih posledica koje nastaju njihovim otkrivanjem ili zloupotrebom. Nije sporno da bi ovde važilo pravno načelo, ko može više-može i manje , pa bi lica koja imaju ovlašćenje da označe podatke višim stepenom, mogla i nižim, ali ovde ostaje nejasno ko ima kakva ovlašćenja, odnosno dokle ko može ići u označavanju tajnih podataka. Jezičkim tumačenjem ove norme proizlazi da najvišim stepenom tajnosti mogu označavati podatke i lica koja su za to ovlašćena podzakonskim aktom, lica na koja se prenese ovlašćenje rukovodioca organa javne vlasti, organi lokalne samouprave i organizacije kojima su poverena javna ovlašćenja. Kako je u prethodnom poglavlju već razmatrano, podatak koji se može označiti kao tajni je onaj od interesa za Republiku čijim otkrivanjem neovlašćenom licu nastaje šteta, ako je potreba zaštite interesa države pretežnija od interesa za slobodan pristup informacijama od javnog značaja. Ovde je jasno je da je pred licem koje treba da stavi oznaku tajnosti na određeni podatak poprilično težak zadatak procene pretežnosti interesa, a zatim i moguće štete po interes države. Složenost ovakvog zadatka, sama po sebi isključuje iz mogućnosti upotrebe najvišh stepeni tajnosti, širok krug državnih službenika i funkcionera. Ovakvo rešenje da se ne ide u bliže određenje ovlašćenja po stepenima tajnosti ostavlja otvoreno i pitanje da li onda zakon uopšte taksativno navodi lica ovlašćena za označavanje tajnih podataka, ili se radi o navođenju lica, odosno funkcija od kojih originerno može poteći takvo ovlašćenje.[14]

Zakon o tajnosti podataka Republike Slovenije (http://nato.gov.si/eng/documents/classified-info-act/) naglašava da podatke mogu klasifikovati lica ovlašćena za to, gde spadaju rukovodioci agencija, imenovani, postavljeni funkcioneri ovlašćeni za klasifikaciju na osnovu zakona ili ovlašćenja rukovodioca i drugi zaposleni sa takvim ovlašćenjem. Ovo se može tumačiti kao generalna odrednica ko, prema strukturi administracije ima ovlašćenje za označavanje tajnih podataka. U sledećem članu već je jasno naglašeno koje funkcije mogu klasifikovati najvišim nivoom “TOP SECRET”(predsednik države, predsednik Vlade, ministri, direktori agencija povezanih sa ministarstvima, predsednik parlamenta i komisije za nadzor nad službama bezbednosti, određeni vojni komandanti, diplomatsko-konzularni predstavnici i rukovodioci vladinih službi koji su direktno odgovorni premijeru), (http://nato.gov.si/eng/documents/classified-info-act/).

[14] Ovakvo rešenje sreće se u američkom zakonodavstvu koje reguliše pitanje tajnosti podataka na sasvim drugačiji način od regulisanja ove oblasti u kontinentalnom pravu. Imajući to u vidu može se zaključiti da je domaći zakonodavac izostavio regulisanje ovg važnog pitanja

U Hrvatskoj, stepenima tajnosti “VRLO TAJNO” i “ TAJNO” mogu označavati podatke, „*Predsjednik Republike Hrvatske, predsjednik Hrvatskog sabora, Predsjedik Vlade Republike Hrvatske, ministri, Glavni državni odvjetnik, načelnik Glavnog stožera Oružanih snaga i čelnici tijela sigurnosno-obavještajnog sustava RH te osobe koje oni za tu svrhu ovlaste.“* **(**Zakon o tajnosti Republike Hrvatske**,** Narodne Novine,79/07, 86/12**).**

Ovakvo rešenje u domaćem zakonodavstvu, vezano za određivanje ovlašćenih lica za označavanje tajnih podataka je veliki propust, koji otvara niz problema u tumačenju i primeni ne samo konkretnog člana zakona, već stvara problem u tumačenju jednog od osnovnih pitanja kada je reč o tajnosti podataka uopšte.

Kada je u pitanju stepen tajnosti "INTERNO" i tu zakon sadrži jednu spornu odredbu. Kao tajni podatak se označava onaj podatak koji je od interesa za Republiku Srbiju, čijim otkrivanjem neovlašćenom licu nastaje šteta po interese Republike. U primeni stepena tajnosti “INTERNO” , navedeno je da se ovaj stepen tajnosti upotrebljava za sprečavanje štete za rad organa javne vlasti, koja za posledicu može imati smanjenje operativnih i funkcionalnih sposobnosti organa javne vlasti odnosno ugrožavanje saradnje organa javne vlasti sa organima drugih država, međunarodnih organizacija i drugih međunarodnih subjekata. Prilično bi široko trebalo poimati štetu za rad i obavljanje zadataka poslova organa javne vlasti, da bi se ona mogla tumačiti kao šteta po najviše interese države. Ovakve formalne nedoslednosti u okviru zakonskog teksta dokaz odsustva pravne analize i diskusije prilikom njegovog donošenja.

Oznaka tajnosti “INTERNO” odgovara oznaci tajnosti “RESTRICTED” u stranim zakonodavstvima odnosno u sistemu tajnosti NATO i EU. Pod ovom oznakom podrazumevaju se podaci, čije bi neovlašćeno otkrivanje nepovoljno uticalo na interese, bilo država, bilo vojnog pakta, odnosno ekonomske zajednice. Kod definisanja kada se upotrebljavaju niži stepeni tajnosti, a naročito stepen “INTERNO” neophodna je posebna pažnja, jer je ovo najkritikovaniji segment primene tajnosti, koji može se reći predstavlja “sivu zonu” između otvorenih i tajnih podataka. To su po pravilu podaci, koji ne spadaju sami po sebi u kategoriju podataka koji bi trebalo da budu označeni stepenom tajnosti, ali svakako predstavljaju osetljive podatke koje državni organi, bilo iz objektivnih razloga, bilo po svom mišljenju nastoje da zaštite od slobodnog pristupa javnosti. Po karakteru najsličniji su podacima koji su u prethodnom period spadali pod pojam “službena tajna”.

Podataka koji spadaju u ovu kategoriju, po pravilu, ima najviše jer ih stvara gotovo ceo administrativni aparat države, pa će kod ovih podataka biti i najviše pogrešnog označavanja i zloupotrebe. Ovo je razlog što se u pojedinim nacionalnim pravnim sistemima ova kategorija podataka štiti na drugi način, a ne primenom pravila o tajnosti popdataka. Ovako definisan stepen tajnosti "INTERNO" susrešće se sa brojnim problemima, prilikom zahteva za slobodan pristup informacijama, jer nije na adekvatan način određeno u kojim se slučajevima primenjuje i o kom stepenu ugrožavanja interesa se ovde radi. Prilikom korišćenja pravnih standarda, u vidu pojmova “neotklonjiva teška šteta” i “teška šteta”, koji po obimu idu iznad pojma štete koji je definisan u uvodnom delu samog zakona, nejasno je zašto se nije definisao i odgovarajući pojam koji bi išao ispod obima pojma “šteta”, a koji bi adekvatnije definisao kriterijume primene ovog stepena tajnosti.

7.3. Pristup tajnim podacima

Podatak koji je označen određenim stepenom tajnosti se od tog trenutka nalazi u posebnom režimu postupanja sa njim, njegove zaštite i mogućnosti uvida u njegovu sadržinu. Pravila koja regulišu postupanje sa tajnim dokumentima se donose u cilju zaštite podataka koje oni sadrže. To ipak ne znači da tajnim dokumentima niko više neće moći da pristupi i da saznanje o njegovoj sadržini ostaje privilegija samo lica koja su ga stvorila.

Sa aspekta procene rizika po bezbednost tajnih podataka, što se krug lica koja pristupaju podacima širi i što je više kopija tajnog podatka, povećava se opasnost od “curenja” informacija izvan kruga ovlašćenih lica i potencijalnog nastanka štete. Da bi se ostvario pristup tajnim podacima, podrazumeva se postojanje poverenja u lica koja vrše pristup, odnosno uverenje da se radi o pouzdanim licima. Bezbednosna provera fizičkih i pravnih lica je segment opštih bezbednonsnih mera, koje se primenjuju radi zaštite tajnih podataka, odnosno postupak koji se koristi za utvrđivanje lojalnosti, pouzdanosti i autentičnosti lica u svrhu izdavanja ili produženja bezbednosne dozvole i može se definisati kao personalna bezbednost (Matić, 2012).

Personalna bezbednost predstavlja primenu mera koje osiguravaju da pristup tajnim podacima bude odobren samo onim licima kojima je pristup potreban, koja su prema potrebi prošla odgovarajuću bezbednosnu proveru za odgovarajući stepen i koja su upoznata sa svojim odgovornostima i obavezama (Odluka saveta EU-2013/488/EU).

Kao što je određivanje ovlašćenih lica za označavanje tajnih podataka bitno sa aspekta pravne sigurnosti, ispravne primene zakonskih pravila i sprečavanja zloupotreba ili preširoke klasifikacije, podjednako važno pitanje vezano za tajnost podataka je ko sve ima pristup podacima, na koje je stavljena oznaka tajnosti. Pored nosilaca ovlašćenja da na podatke stave oznaku tajnosti, koji su po prirodi stvari upoznati sa sadržinom tajnih dokumenta, u broj lica koja su upoznata sa tajnim podatkom spadaju i ona koja imaju pravo da se upoznaju sa sadržinom već nastalih tajnih dokumenata. Po pravilu ovaj broj je mnogo veći od broja lica ovlašćenih za označavanje tajnih podataka. Uređenje ovog pitanja je od suštinske važnosti za ostvarivanje same svrhe tajnosti jer od njegovog definisanja zavisi broj onih koji će saznati sadržinu tajnih dokumanata.

Zakon o tajnosti podataka (Službeni glasnik RS, 104/2009) u tu svrhu definiše pojam korisnika tajnog podatka. To je domaće ili strano fizičko ili pravno lice kome je izdata bezbednosna dozvola za pristup tajnim podacima, kao i funkcioneri organa javne vlasti kojima je na osnovu zakona zagarantovano pravo pristupa i korišćenja tajnih podataka, bez izdavanja sertifikata. To su predsednik Narodne skupštine, predsednik republike i predsednik Vlade.

Državni organi koje bira narodna skupština, rukovodioci takvih državnih organa, sudije Ustavnog suda i sudije ovlašćeni su na pristup podacima svih stepena tajnosti, koji su im potrebni za obavljanje poslova iz njihove nadležnosti, bez bezbednosne provere, osim za podatke označene stepenom tajnosti "DRŽAVNA TAJNA" i "STROGO POVERLJIVO", koji se odnose na: radnje sprečavanja, otkrivanja istrage i gonjenja za krivična dela do okončanja istrage, na primene postupaka i mera u pribavljanju bezbednosnih i obaveštajnih podataka, na pripadnike službi bezbednosti i ministarstva unutrašnjih poslaova sa prikrivenim identitetom, identitet sadašnjih i bivših saradnika službi bezbednosti odnosno trećih lica. U slučaju da je pristup ovakvim podacima potreban za obavljanje poslova iz nadležnosti ovih državnih organa, izuzetno, sprovodi se bezbednosna provera i za vršioce nabrojanih funkcija (Zakon o tajnosti podataka, „Sl. glasnik RS", 104/2009).

Članovi odbora Narodne skupštine nadležnog za nadzor i kontrolu u sektoru odbrane i bezbednosti imaju pravo na pristup i uvid u podatke u vezi sa vršenjem svojih funkcija.

Funkcioneri i zaposleni u organima javne vlasti imaju pristup tajnim podacima stepena tajnosti “INTERNO”.

Domaći zakon predviđa u tu svrhu izdavanje dozvole-sertifikata za pristup tajnim podacima. Sertifikat izdaje Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka[15] i ono podrazumeva da podnosilac zahteva (fizičko/pravno lice) mora ispuniti određene uslove. Za fizička lica ti uslovi podrazumevaju da se radi o punoletnom, poslovno sposobnom domaćem državljaninu, koji nije osuđivan na bezuslovnu kaznu zatvora, za krivično delo koje se goni po službenoj dužnosti, odnosno za prekršaj predviđen zakonom i da je to lice prošlo bezbednosnu proveru. U zavisnosti od stepena tajnosti bezbednosna provera može biti osnovna za tajne podatke sa oznakom “INTERNO” i “ POVERLJIVO”, potpuna bezbednosna provera za tajne podatke sa oznakom “STROGO POVERLJIVO” i posebna bezbednosna provera za podatke sa oznakom “DRŽAVNA TAJNA”. Samu bezbednosnu proveru, u zavisnosti od stepena tajnosti i radnog mesta lica za koje se ona vrši sprovode službe bezbednosti ili ministarstvo unutrašnjih poslova. Ova provera služi da se izvrši procena bezbednosnog rizika vezanog za pristup i korišćenje tajnih podataka, od strane određenog lica. Na osnovu izveštaja sa preporukom ovlašćenih službi, koje vrše bezbednosnu proveru, Kancelarija Saveta odlučuje o izdavanju sertifikata u roku od 15 dana od prijema ovog izveštaja. (Zakon o tajnosti podataka, „Sl. glasnik RS“, 104/2009)

Domaći zakonodavac je i u ovom slučaju propustio da na samom početku uređivanja oblasti pristupa tajnim podacima na jasan način u skladu sa međunarodnim standardima definiše pojam pristupa i osnovna načela ovog važnog pitanja. Regulisanje ove oblasti počinje sa odredbom da najviši državni organi mogu pristupiti tajnim podacima bez sertifikata.

Pristup tajnim podacima je složeno pravno i bezbednosno pitanje ove oblasti. U programu personalne bezbednosti američkog ministarstva odbrane pristup tajnim podacima je određen kao *"ovlašćenje i mogućnost upoznavanja sa tajnim podacima. Lice može imati pristup tajnim podacima boravkom na mestu gde se podaci čuvaju ako ga bezbednosna pravila koja se odnose na zaštitu tih podataka u tome ne sprečavaju"*
(http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf).

[15] U daljem tekstu Kancelarija Saveta.

Iz ovako definisane radnje pristupa tajnim podacima vidi se da postoji razlika da li pristup tajnom podatku vrši zaposleni sa bezbednosnom dozvolom kome je to neophodno u cilju obavljanja posla , koji u principu nije vezan za same tajne podatke ili se radi o licu čije se radne aktivnosti odnose na sam rad sa tajnim podacima. Ovo otvara pitanje upotrebe lica, sa specijalističkim znanjima, iz oblasti povezanih sa merama zaštite tajnih podataka (prvenstveno iz oblasti informacionih tehnologija) na koje bi trebalo da se odnose drugačija pravila i režim bezbednosne provere, ali i poseban test stručnog znanja, neophodnih za rad sa tajnim podacima, kao što je to slučaj u Češkoj. Iz više aspekata sagledano, svaki od ovih pristupa tajnim podacima ima svoje specifičnosti, koje sa sobom nose razlike u primeni bezbednosnih pravila. Iz brojnih bezbednosnih pravila i standarda vezanih za pristup tajnim podacima neka se izdvajaju i trebalo bi da imaju značaj načela:

1. Princip "POTREBNO DA ZNA" je ovde jedno od načela na kojima počiva tajnost informacija u celini. Ono znači da bi pristup tajnim podacima trebalo da bude omogućen samo onim licima kojima je to neophodno u vršenju njihovog posla. Praktično, to podrazumeva da niko neće na osnovu same funkcije ili položaja odnosno stepena bezbednosne dozvole imati mogućnost da bude upoznat sa sadržinom nedefinisane količine tajnih podataka. Da bi se pravo na pristup odobrilo neophodno je postojanje opravdanog interesa za pristup tajnom podatku. Ovo je osnovno bezbednosno pravilo kada je reč o tajnim podacima jer se njegovom primenom sprečava potencijalna šteta koju mogu naneti ovlašćena lica ukoliko otkriju tajne informacije. O tome da li neko ima opravdan interes da bude upoznat sa sadržinom tajnih podataka, radi obavljanja svojih dužnosti, odluku donosi onaj organ koji je stavio oznaku tajnosti na podatak. Posedovanje dozvole (sertifikata) za pristup tajnim podacima je samo polovina puta do samog uvida u tajne podatke. Tek primenom principa "POTREBNO DA ZNA" dobija se jasna slika ko sve zaista ima pravo na pristup tajnim podacima (http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf).O primeni ovog principa se konstantno vodi računa, s obzirom da se ovde radi o licima koja već imaju bezbednosnu dozvolu za pristup tajnim podacima određenog nivoa, pa s toga treba sa naročitom pažnjom razmotriti da li žele pristup samo onim podacima neophodnim za obavljanje njihovih poslovnih zadataka ili idu preko te potrebe. Od ovog principa, da je pristup tajnim podacima moguć na osnovu kumulativno ispunjena dva uslova- posedovanja bezbednosnog sertifikata i pretpostavke opravdanog interesa za upoznavanje sa sadržinom tajnih podataka, u našem sistemu izuzeti su određeni državni organi, za koje se ne vrši bezbednosna provera. Zakonodavac propisuje da Predsednik Narodne skupštine, predsednik

Republike i predsednik Vlade imaju pravo pristupa tajnim podacima, u cilju obavljanja poslova iz njihove nadležnosti, bez izdavanja sertifikata, dakle bez vršenja bezbednosne provere. Sam izbor na ove najviše državne funkcije izuzima ova lica od vršenja bezbednosnih provera. Od vršenja bezbednosne provere odnosno izdavanja sertifikata izuzima državne organe koje bira narodna skupština, rukovodioce tih organa, sudije ustavnog suda i sudije dok od ovog pravila izostavlja narodne poslanike. Ovo rešenje, iako kritikovano u delu stručne javnosti ima opravdanje, s obzirom na način izbora za narodne poslanike, koji podrazumeva glasanje za stranačke liste, a ne neposredno za samu ličnost.

Svako pravljenje izuzetka od pravila kumulacije uslova za pristup treba da bude ograničeno. Vršenje određene državne funkcije jeste pretpostavka pouzdanosti određenog lica ali s obzirom da svaki pojedinac u svom životu biva izložen brojnim uticajima, sam ima lične interese i ostvaruje kontakte sa različitim krugom ljudi, takva pretpostavka lojalnosti ne sme biti apsolutna. Takođe izričito nije navedeno da li i kako nezavisni organi vrše pristup tajnim podacima. Iako u praksi oni imaju pristup tajnim podacima, jasno nabrajanje funkcija koje imaju pristup tajnim podacima čini propis bitno jasnijim i razumljivijim, a ova potreba naročito dolazi do izražaja kada se pravi izuzetak od opšteg principa.

2. Princip "NEOPHODNO PODELITI SA". Ovaj princip reguliše razmenu tajnih podataka između rezličitih državnih organa, odnosno pristup tajnom podatku na horizontalnom nivou. Ovo je vrlo bitno pitanje tajnosti podataka, jer se njegovim dobrim funkcionisanjem otklanjaju štetne posledice primene tajnosti do kojih može doći ukoliko organi nisu upoznati sa delovanjem drugih državnih organa. Put ka ostvarivanju kvalitetne međusobne saradnje državnih organa, u oblasti rukovanja tajnim podacima je uvođenje registarskog sistema tajnih podataka. Ovaj sistem centralnog registra je sastavni deo NATO pravila o poverljivim dokumentima, a prihvaćen je i od EU, kao dokazano dobar sistem za pristup i razmenu tajnih podataka. Iskustva primene u dva ovako velika nadnacionalna sistema bi trebalo primeniti i na nacionalnom nivou, ne samo zbog politike evro integracija i eventualnog pristupanja NATO paktu, već zbog stvaranja uređenog i funkcionalnog nacionalnog sistema za rad sa tajnim podacima. U razmeni tajnih podataka između različitih državnih organa svakako bi trebalo da važi i princip kontrole od strane kreatora tajnog podatka koji je sastavni deo ovih stranih bezbednosnih standarda. To bi značilo da organ koji stavlja oznaku tajnosti na podatak ima apsolutnu kontrolu, po pitanju daljeg rada i pristupa tajnom dokumentu, razmene takvog dokumenta ili uklanjanja oznake tajnosti. Uz ovakvo ovlašćenje ide i odgovornost počevši od

primene pravila za nastanak tajnih doumenata, primene pravila potrebno da zna i potrebe obaveštavanja drugih državnih organa kojima je ovakav podatak potreban.
O uspostavljanju centralnog registra nacionalnih tajnih podataka i pravilima razmene tajnih podataka između organa javne vlasti zakon o tajnosti podatka gotovo da nema odredbi.

Sledeće pitanje koje otvara prostor za analizu je izdavanje privremenog sertifikata. Radi izvršenja neodložnih poslova i zadataka organa javne vlasti u cilju sprečavanja ili otklanjanja štete direktor Kancelarije Saveta može i pre završetka bezbednosne provere izdati privremeni sertifikat, na isnovu uvida u bezbednosni upitnik, ako se oceni da ne postoje sumnje u pogledu bezbednosti. (Zakon o tajnost podataka, Službeni glasnik RS, 104/2009). Ovakvo diskreciono ovlašćenje direktora Kancelarije Saveta ne ide u prilog rešenju po kome je Kancelarija Saveta stručna služba Vlade sa svojstvom pravnog lica. Bezbednosnu proveru lica vrše ministarstvo unutrašnjih poslova i službe bezbednosti, pa se postavlja pitanje na koji način direktor Kancelarije Saveta može na osnovu uvida u upitnik sa sigurnošću da izda dozvolu za pristup tajnim podacima, bez sprovođenja svih mera koje nalažu kriterijumi personalne bezbednosti. I šta bi se u tom slučaju dogodilo, ukoliko službe dostave negativnu bezbednosnu procenu, a takvo lice već izvrši pristup i izazove eventualnu štetu.

Pitanje pristupa i razmene tajnih podataka je jedno od ključnih pitanja koje pokazuje da li sistem tajnosti i zaštite tajnih podataka funkcioniše ili ne. Jedna tako važna oblast ove materije zahteva detaljnije i jasnije zakonsko uređenje, odnosno zakonski tekst koji pored toga što je dostupan i javan ispunjava i druge međunarodne principe pravnog regulisanja ove oblasti, a to je da bude razumljiv svakom čitaocu, a ne samo dobrim poznavaocima ove oblasti, da bude jasan, precizan i pogodan za tumačenje kako onima koji treba da ga primenjuju u svom radu tako i najširoj javnosti (Open Society Foundations, Open Society Initiatives, 2013).

7.4. Nadzor i kontrola nad primenom zakona

Tumačenjem odredbi Zakona o tajnosti podataka („Službeni glasnik RS, 104/2009) može se utvrditi da kontrolu nad primenom zakona vrše rukovodioci organa javne vlasti ili lica koja oni za to ovlaste, Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka dok je nadzor nad vršenjem zakona poveren Ministarstvu pravosuđa.

Unutrašnju kontrolu vrše rukovodioci organa javne vlasti, lica koja oni za to ovlaste ili postojeća organizaciona jedinica u okviru ministarstva ili agencije. O licu zaduženom za vršenje unutrašnje kontrole obaveštava se Kancelarija Saveta radi njegovog obučavanja. Cilj ove kontrole je redovno praćenje i ocenjivanje delatnosti organa javne vlasti u vezi sa sprovođenjem ovog zakona i propisa i mera donetih na osnovu ovog zakona. Sam postupak kontrole je propisn uredbom o posebnim merama nadzora nad postupanjem sa tajnim podacima („Službeni glasnik RS“, 90/11). Tu se detaljno utvrđuje način i oblik vršenja ovog vida kontrole, gde je određeno da se unutrašnjom kontrolom proverava sprovođenje mera zaštite tajnih podataka posebno vezano za određivanje stepena tajnosti podatka i sve druge mere, koje spadaju u oblasti personalne, fizičke, administrativne, informacione bezbednosti tajnog podatka. O izvršenoj kontroli sačinjava se zapisnik.

Prva stvar, koja je ovde odmah uočljiva je da unutrašnju kontrolu vrši rukovodilac organa javne vlasti ili lice koje on za to ovlasti. Osvrtom na član 9. Zakona o tajnosti podataka („Sl. glasnik RS“ ,br. 104/2009) koji definiše ko su lica ovlašćena za označavanje tajnih podataka dolazimo u situaciju da rukovodilac organa javne vlasti ,koji je sam po zakonu ovlašćen da označi podatak kao tajan, kontorliše posebno primenu zakona vezanu za određivanje stepena tajnosti podatka, dakle kontroliše sam svoj prethodni rad. Smisao uspostavljanja unutrašnje kontrole je da rukovodioci organa zbog složenosti i obima zadataka koje oni vrše s vremena na vreme izvrše uvid i kontrolu nad primenom propisa u tim organima kako bi se otklonile nepravilnosti i propusti i sankcionisali oni zaposleni koji su postupali protivno pravilima. Dakle viša instanca vrši kontrolu nižih u okviru istog organa. Ova odredba o vršenju unutrašnje kontrole od strane rukovodioca organa javne vlasti imala bi smisla samo ukoliko je ovlašćenje za označavanje tajnih podataka preneto na drugo lice u samom organu. Ako je za to ovlašćen sam rukovodilac, koji je označio podatak određenim stepenom tajnosti postavlja se pitanje mogućnosti utvrđivanja nepravilnosti sa njegove strane.

Drugi subjekt koji kontroliše primenu zakona je Kancelarija Saveta. U članu 87. Zakona o tajnosti podataka („Sl. glasnik RS“, br. 104/2009) definisane su nadležnosti Kancelarije Saveta među kojima nije na jasan način definisano na koji način ona tu kontrolu vrši. Osim odredbi da obezbeđuje primenu standarda i propisa u oblasti tajnih podataka i ovlašćenja za opoziv tajnosti u skladu sa zakonom, ne bi se moglo reći da se iz ovog zakonskog nabrajanja ovlašćenja mogu naći ovlašćenja za vršenje kontrole drugih organa javne vlasti u primeni propisa u ovoj oblasti. Član 24. Zakona o tajnosti podataka („Sl. glasnik RS“ ,br. 104/2009)

jedini izričito navodi da Kancelarija Saveta vrši postupak kontrole prilikom koje može da zahteva vanrednu procenu tajnosti podatka od strane ovlašćenog lica i na osnovu te procene sama izvršiti opoziv tajnosti.

Položaj Kancelarije Saveta koja je stručna služba Vlade sa svojstvom pravnog lica u startu onemogućava njeno vršenje kontrole nad organima javne vlasti i primenu ovakvih mera. Da bi se sprovodila kontrola rada državnih organa u određenoj oblasti neophodno je da organ koji kontroliše ima i inspekcijska ovlašćenja koja primenjuje kao vid unutrašnjeg upravnog nadzora (Tomić, 2009). Kada se govori o kontroli primene Zakona o tajnosti (Službeni glasnik RS, 104/2009), ona upravo podrazumeva neposredan uvid u rad i pridržavanje zakonom predviđenih mera. Kao stručna služba Vlade, Kancelarija Saveta ne može raspolagati ovakvim ovlašćenjem pa je njen položaj u ovom smislu vrlo diskutabilan.

Nadzor nad sprovođenjem zakona je zato ipak stavljen u nadležnost ministarstva pravde odnosno grupe za nadzor nad tajnošću podataka u okviru ministarstva, kao organa javne vlasti koji poseduje pravni kapacitet za vršenje ovakvog ovlašćenja. Ministarstvo je u procesu vršenja nadzora ima niz ovlašćenja kao što su:1) praćenje stanja u oblasti zaštite tajnih podataka; 2) priprema propise neophodne za sprovođenje zakona; 3) daje mišljenje na predloge propisa u oblasti zaštite tajnih podataka; 4) predlaže Vladi sadržinu, oblik i način vođenja evidencije tajnih podataka i propise kojima se uređuje obrazac bezbednosnog upitnika, sertifikata i dozvole; 5) nalaže mere za unapređivanje zaštite tajnih podataka; 6) kontroliše primenu kritetijuma za označavanje stepena tajnosti i vrši druge poslove kontrole u skladu sa zakonom; 7) podnosi krivične prijave, zahteve za pokretanje prekršajnog postupka i predlaže pokretanje drugog postupka zbog povrede odredaba oog zakona; 8) sarađuje sa organima javne vlasti u sprovođenju ovog zakona u okviru svoje nadležnosti; 9) obavlja i druge poslove koji su predviđeni ovim zakonom i propisima donetim na osnovu njega. (Zakon o tajnosti podataka, „Sl. glasnik RS“ ,br. 104/2009).

O kontroli i sprovođenju zakona ministar pravde podnosi godišnji izveštaj odboru Narodne skupštine za nadzor i kontrolu u oblasti odbrane i bezbednosti. Lica ministarstva koja vrše ovaj nadzor, shodnom primenom propisa o inspekcijskom nadzoru. Upravo ovo je bila tačka sporenja stručne javnosti i predlagača, vazano za predlog zakona o tajnosti, u kome je nadzor nad sprovođenjem zakona bio u rukama Kancelarije Saveta. Ovakvo ovlašćenje može da ima

samo centralizovani nacionalni organ za rad sa tajnim podacima (NSA), kao što je slučaj češkog organa bezbednosti.

Problem u praktičnoj primeni ovih nadzornih ovlašćenja od strane grupe za nadzor nad tajnošću podataka ministarstva pravde je personalni i tehnički kapacitet. Vršenje inspekcijskih ovlašćenja u ovakvoj oblasti i materiji zahteva dobro organizovanu, opremljenu i obučenu službu koja mora poznavati rad sa tajnim podacima, način primene pravnih pravila i specifičnosti sistema bezbednosti. I ovo je jedan od razloga zašto bi adekvatnije rešenje bilo formiranje centralizovanog nacionalnog organa za rad sa tajnim podacima koji bi imao kapacitet nivoa službe, sa posebnim odsecima i većim brojem zaposlenih stručnih lica i raspolagao izvršnim ovlašćenjima u radu sa tajnim podacima.

8. KANCELARIJA SAVETA ZA NACIONALNU BEZBEDNOST I ZAŠTITU TAJNIH PODATAKA

Stručna služba Vlade, sa svojstvom pravnog lica ustanovljena Zakonom o osnovama uređenja službi bezbednosti Republike Srbije (Službeni glasnik RS, 116/2007 i 72/2012), kao služba Vlade, koja obavlja stručne i administrativne poslove za potrebe Saveta. Osnovana je uredbom Vlade- Uredba o osnivanju Kancelarije Saveta za nacionalnu bezbednost (Službeni glasnik RS, 12/2009), a stupanjem na snagu Zakona o tajnosti podataka (Službeni glasnik RS, 104/2009) naziv joj je promenjen u Kancelariju Saveta za nacionalnu bezbednost i zaštitu tajnih podataka. Nastala je u sklopu reforme sistema bezbednosti i dodeljena joj je tehnička uloga podrške Savetu za nacionalnu bezbednost.

Rad sa tajnim podacima, saradnja sa međunarodnim telima i organizacijama i težnja ka evrointegracijama zahtevaju ispunjenje određenih standarda u radu sa tajnim podacima, koji podrazumevaju označavanje jednog organa koji će imati potrebna ovlašćenja i odgovornosti na polju stvaranja, obrade i razmene tajnih podataka.

Reforma oblasti tajnih podataka podrazumeva unifikovanje stupnjeva tajnosti, radi lakše razmene, i formiranje nacionalnog bezbednosnog tela (NSA) za saradnju i razmenu stranih tajnih podataka. Ovo su osnovni principi NATO i EU standarda u oblasti zaštite i bezbednosti tajnih podataka.

„*U formiranju ovakve nacionalne organizacije postoje dva modela: 1) Centralizovani model koji karakteriše formiranje nove službe bezbednosti koja je centralna nacionalna izvršna vlast u oblasti tajnih podataka; 2) Decentralizovani model u kome ova organizacija predstavlja samo jednog od nosilaca zaštite tajnih podataka na nacionalnom nivou sa podeljenom nadležnošću sa resornim ministarstvima i agencijama odnosno predstavlja malobrojnu stručnu agenciju koja se bavi koordinacijom svih nadležnih državnih organa koji se bave poslovima bezbednosti i zaštitom tajnih podataka*." (Matić, 2012, p. 9).

Zakonom o tajnosti podataka (Službeni glasnik RS, 104/2009), Kancelarija Saveta je dobila ulogu kontrole i nadzora nad sprovođenjem zakona. U njenoj nadležnosti su se našli sledeći poslovi:

1) Postupa po zahtevima za izdavanje sertifikata i dozvola; 2) Obezbeđivanje primene standarda i propisa u oblasti zaštite tajnih podataka; 3) Staranje o izvršenju prihvaćenih međunarodnih obaveza i zaključenje međunarodnih sporazuma između Republike Srbije i drugih država odnosno međunarodnih organa i organizacija u oblasti zaštite tajnih podataka i saradnja sa odgovarajućim organima stranih država i međunarodnih organizacija; 4) Izrada i vođenje Centralnog registra stranih tajnih podataka; 5) Predlaganje obrasca bezbednosnog upitnika; 6) Predlaganje obrasca preporuke sertifikata i dozvole; 7) Vodjenje evidencije o izdatim sertifikatima odnosno dozvolama kao i evidencije o odbijanju izdavanja sertifikata odnosno dozvola; 8) Organizacija obuke korisnika tajnih podataka u skladu sa standardima i propisima; 9) Predlaganje Vladi plana zaštite tajnih podataka za vanredne i hitne slučajeve; 10) Opozivanje tajnosti podataka u skladu sa zakonom; 11) Obavljanje poslova zaštite tajnih podataka za organe vlasti koji posle prestanka nemaju pravnog sledbenika; 12) Saradnja sa organima javne vlasti u sprovođenju ovog zakona; 13) Obavljanje drugih poslova predviđenih ovim zakonom i propisma na osnovu ovog zakona. (Zakon o tajnosti podataka, „Sl. glasnik RS“ ,br. 104/2009).

Potpisivanjem individualnog akcionog plana partnerstva sa NATO-IPAP [16] (http://www.mfa.gov.rs/sr/images/ipap/ipap.pdf) predviđeno je jačanje kapaciteta Kancelarije Saveta u ljudstvu, tehnici i administraciji (proširivanje NSA ovlašćenja) i osnivanje pomoćnih tela kancelarije u oblasti bezbednosti informacija INFOSEC: Organa za bezbednosnu akreditaciju (SAA), Nacionalnog organa za bezbednost komunikacija (NCSA) i nacionalnog organa za distribuciju (NDA). (http://www.mfa.gov.rs/sr/images/ipap/ipap.pdf) Predviđa se da regionalna saradnja bude aktivno nastavljena kroz potpisivanje bilateralnih sporazuma kojih trenutno Republika Srbija ima sa osam država.

U analizi koji je model organizacije nacionalnog tela za rad sa tajnim podacima adekvatniji, treba poći od analize nedostataka sadašnjeg položaja i prednosti koje nudi drugo rešenje. Prvo što je već pomenuto je sporna odredba o vršenju nadzora i kontrole nad sprovođenjem zakona, koju ne može vršiti telo sa statusom stručne službe Vlade koje ne poseduje inspekcijska ovlašćenja, niti može vršiti unutrašnju upravnu kontrolu. Istovremeno u praksi se suočavamo

[16] IPAP- Individualni akcioni plan partnerstva Republike Srbije i Organizacije Severno-Atlantskog Ugovora (NATO) je najviši vid saradnje država koje nisu članice saveza sa NATO-om.

sa potpunim odsustvom kontrole nad sprovođenjem ovog zakona, jer grupa ministarstva pravde nema potrebne tehničke i ljudske kapacitete za ovaj složen i obiman posao. Odsustvo adekvatne kontrole u ovoj sferi vodi kako mogućnosti zloupotrebe tajnosti tako i potencijalnom ugrožavanju nacionalne bezbednosti usled neovlašćenog pristupa ovakvim materijalima.

Rad sa stranim tajnim podacima podrazumeva izradu centralnog registra tajnih podataka koji je formirala i vodi Kancelarija Saveta. Ovi standardi u radu sa stranim tajnim podacima su se u praksi pokazali kao funkcionalna i dobra rešenja, pa bi trebalo razmisliti o sličnom principu i u nacionalnom sistemu rada sa tajnim podacima. Kapacitet Kancelarije Saveta će zbog rada sa stranim tajnim podacima svakako biti proširivan pomoćnim službama, čime će se stvoriti jedna celovita služba za rad i razmenu stranih tajnih podataka i paralelno glomazan nacionalni resorni i agencijski aparat diskutabilne tehničke i personalne osposobljenosti.

Registarski model rada sa tajnim podacima se pokazao kao veoma pogodno rešenje. U zavisnosti od položaja i modela nacionalnog bezbednosnog tela za rad sa tajnim podacima registar može biti centralizovan ili decentralizovan.
(http://www.arhivinfo.org.rs/radovi2012/radovi/Zastita%20tajnih%20podataka.pdf).
Centralizovani registar nacionalnih tajnih podataka olakšao bi kontrolu nastanka, razmene, prestanka tajnosti, čime bi se smanjile mogućnosti zloupotreba i“curenja” tajnih podataka u javnost. Trenutno su u fazi izrade registri, kao i katalozi tajnih podataka, u svakom resoru pojedinačno. Kvalitet ovako disperzovanog registra i potreba razmene tajnih podataka između organa javne vlasti idu u prilog potrebi centralizovanja ovakvog registra na nivou Republike. Stvaranje ovakvog registra i stručnost, pri izradi kataloga tajnih podataka od koga, kako je već zaključeno, zavisi sam nastanak tajnih podataka zahtevaju da ovaj obiman posao bude poveren jednom telu koje poseduje neophodan tehnički i stručni kapacitet za izvršenje ovako obmnog i osetljivog zadatka.

Sistem zaštite tajnih podataka podrazumeva primenu opštih i posebnih mera zaštite. Ove mere bi trebalo da budu razvrstane u oblsti kao što su personalna bezbednost, fizička bezbednost, administrativna bezbednost, industrijska bezbednost i informaciona bezbednost. (http://www.arhivinfo.org.rs/radovi-2012/radovi/Zastita%20tajnih%20podataka.pdf) Norme koje bi trebalo da regulišu ove segmente sistema zaštite tajnih podataka u svom zbiru daju

jasan pregled obimnosti i složenosti poslova zaštite tajnih podataka i potrebe posedovanja visoke stručnosti u samom sprovođenju konkretnih mera zaštite.

Savremeni uslovi rada i primena tehnike poseban akcenat stavljaju na informacionu bezbednost, prvenstveno na sisteme kriptozaštite i TEMPEST.[17] Ovi zadaci moraju biti povereni posebnim službama adekvatne tehničke i kadrovske osposobljenosti, što je prilično otežano u decentralizovanom modelu rada sa tajnim podacima. Kako je izdavanje sertifikata za pristup tajnim podacima i vođenje registra izdatih dozvola već u rukama Kancelarije Saveta, logično bi bilo da se ovoj službi povere i poslovi informacione bezbednosti i vođenja centralnog registra nacionalnih tajnih podataka. Postojanje zavidnog nivoa bezbednosne kulture i poznavanja bezbednosnog sistema, koje omogućava pravilnu procenu značaja podatka za nacionalnu bezbednost, pa samim tim i pravilno klasifikovanje, u zavisnosti od procene rizika za bezbednost podatka (upravljanje rizikom kao procesom) se mnogo adekvatnije sprovodi u stručnoj sveobuhvatnoj agenciji nego u svakom organu javne vlasti pojedinačno.

Centralizovan rad sa tajnim podacima omogućava lakšu i bolju primenu principa "POTREBNO DA ZNA", ali i isto tako važnog principa "NEOPHODNO PODELITI SA" čime se postiže lakša saradnja državnih organa i sprečavaju negativni aspekti tajnosti u smislu propusta koji mogu nastati usled zaklanjanja podataka od drugih organa odnosno dupliranja poslova. Veća kontrola razmene nacionalnih tajnih podataka sa inostranstvom postiže se ako se ta razmena odvija uz odobrenje ili preko nacionalnog tela za zaštitu tajnih podataka nego po resornom principu.

Tajni podaci iz prošlosti koji nose stare oznake tajnosti, za koje nije predviđena automatska klasifikacija već zadržavanje stare oznake tajnosti do procene njihovog značaja i eventualno određivanja stepena tajnosti po novom sistemu je izuzeno složen i obiman posao koji takođe da bi uopšte ikada bio dovršen, mora biti poveren stručnoj i opremljenoj službi sa potrebnim kapacitetima za izvršenje tog zadatka.

[17] TEMPEST–Telecomunications Electronics Material Protected from Emanating Spurious Transmissions. Zaštita elektronskih podataka od neovlašćenog pristupa do koga može doći tako što određeni komunikacioni uređaji odašilju elektromagnetne talase na osnovu kojih se može utvrditi sadržaj podataka sa uređaja.

Postojanje centralizovanog organa smanjuje i potrbu za brojnim podzakonskim akatima i onemogućava primenu različitih standarda u državnim organima čime se oni izuzimaju iz obaveze da se bave ovim poslom koji im nije u primarnoj nadležnosti i rasterećuju od potrebe imenovanja odgovornih lica za rad sa tajnim podacima kao i izrade kataloga tajnih podataka. Preuzimanjem dela zaposlenih sa potrebnim iskustvom iz ovih resornih jedinica i agencija omogućava se poznavanje radnih potreba svakog od organa, uz istovremeno filtriranje tih zahteva kroz profesionalnu bezbednosnu procenu koja se odnosi na značaj podatka po interese države i njihovu izloženost riziku. Promena statusa ove službe omogućila bi joj i donošenje akata u ovoj oblasti, kojima bi se direktno uticalo na primenu odgovarajućih standarda struke u ovoj oblasti.

Nedostaci ovakvog rešenja bi bili pozicioniranje nove službe bezbednosti, u već razuđenom i nedefinisanom sistemu bezbednosti. Problem ostvarivanja kontrole nad drugim činiocima ovog sistema po pitanju tajnih podataka podrazumevao bi rad na izmenama većine zakona iz ove oblasti. Uz to ovakva organizacija nosi sa sobom rizik uvećavanja već glomaznog administrativnog aparata koji stvara budžetski problem. Čini se ipak da glavnu prepreku ovakvom urđenju predstavlja uloga političkog faktora koji je u značajnoj meri prisutan, kada je u pitanju sistem nacionalne bezbednosti. Takva situacija ne ide sasvim u prilog mogućnosti sprovođenja ovakvog ponuđenog rešenja u skorije vreme.

Povećavanje kapaciteta Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka je neminovnost i proces koji će u svakom slučaju ići u smeru centralizovanja u radu sa tajnim podacima vezanih za proces pridruživanja EU, pa će samim tim već postojati kapacieteti i infrastruktura unutar ovog organa da preuzme na sebe prava i obaveze po pitanju centralnog (NSA) organa po pitanju rada sa nacionalnim tajnim podacima.

Ovakvo ponuđeno rešenje u ovoj tezi je razmatrano prvenstveno, sa pravnog i organizacionog aspekta sa kojih se čini kao bolje i adekvatnije u smislu stručnosti rada i poboljšanja funkcionisanja celokupnog sistema nacionalnih tajnih podataka. Politički aspekt u ovoj oblasti je sasvim odvojeno pitanje koje može biti predmet neke druge stručne analize.

9. ZAKLJUČAK

Tajnost je fenomen čija primena u demokratskoj državi dovodi do ograničavanja zagarantovanih prava, naročito prava na pristup informacijama od javnog značaja. Nacionalna bezbedost nalaže da određeni podaci moraju biti zaštićeni, tako što će na njih biti stavljena oznaka tajnosti. Kako je transparentnost demokratsko načelo, ograničavanje javnosti nalaže da se u tom slučaju prmene standardi koji se ogledaju u postojanju zakonskog teksta kojim se na jasan i precizan način svako može upoznati sa odgovorima na pitanja koji podaci mogu biti označeni kao tajni? Ko ih može označiti? Kakav tretman ti podaci imaju? I kakve su posledice suprotnog postupanja? Na ovaj način se postiže harmonija interesa i sprečava sukob prava u pravnom sistemu. Država merama zaštite važnih podataka štiti nacionalnu bezbednost čime prvenstveno ostvaruje javni interes svakog građanina i društva kao celine.

Zakon o tajnosti podataka („Sl. glasnik RS“ ,br. 104/2009), posle dugog perioda prilično haotčnog postupanja sa tajnim podacima, uvodi jedinstven sistem pravila po kojima se može izvršiti označavanje podataka kao tajnih uz propisivanje četiri stepena tajnosti. Ovaj zakonski tekst predstavlja prvi i najteži korak procesa reforme celokupne državne uprave, a naročito sistema nacionalne bezbednosti koji u budućnosti mora biti jasno definisan i funkcionalno uređen. Ovaj prvi korak je načinjen, a put evrointegracija Republike Srbije zahteva dalji rad na izgradnji funkcionalne pravne regulative u sferi tajnih podataka i njhove zaštite koja je usklađena sa prihvaćenim međunarodnim principima. Nedostaci ovog zakona zahtevaju brojne izmene i dopune ili čak nov zakonski tekst, koji će na osnovu utvrđenih manjkavosti iz prethodnog perioda predstavljati „drugi korak“ u oživljavanju propisanih pravila u praksi. Funkcionalna rešenja stranih pravnh sistema bi mogla da budu vrsta uzora za poboljšanje domaćih pozitivnopravnih normi koje moraju biti plod podrobne pravne analize, a nikako pukog preuzimanja i transplantacije u pravni sistem koji nije sposoban da takva rešenja iznese.

Zaštita nacionalne bezbednosti bi trebalo da bude osnov koji diktira pravila kojima se uređuje tajnost podataka, a svako dodatno širenje okvira njene primene zahteva detaljno zakonsko precizranje pojmova, a nikako primenu pojmova visokog stepena apstraktnosti koji zahtevaju pravničko znanje i otvaraju mogućnost različitih tumačenja.

Praktično sprovođenje ovako složenog pravnog pitanja koje je produkt pravila bezbednosti predstavlja težak zadatak za mlade demokratske sisteme koji moraju, barem u prvom periodu,

biti povereni centralizovanoj nacionalnoj službi za rad sa tajnim podacima koja ima tehničke i kadrovske kapacitete dovoljne za sprovođenje ove važne i osetljive pravne regulative.

Promene zakonskog teksta koji normira tajnost podataka se očekuju u narednom periodu, pa je cilj ove teze da omogući upoznavanje čitalaca sa suštinskim problemima aktuelnih zakonskih rešenja, međunarodnim standardima u ovoj oblasti, potrebi definisanja nacionalne bezbednosti kao okvira u kome tajnost ima legitimitet i organizovanju organa javne vlasti na takav način koji bi omogućio efikasno sprovođenje takvih normi u praksi.

10. LITERATURA

KNJIGE

Bok, S., 1983, *Secrets: On the etics of concealment and revevation*, New York, Vintage Book, a division of Random House INC.

Grčić, M., 1979, *Politička teorija države*, Beograd, Zavod za udžbenike i nastavna sredstava.

Huntington, S., 1973, *Political order in chalenging societises*, London, Yale University Press, Ltd.

Holloway, D., 1994, *Stalin and the Bomb: The Soviet Union and Atomic Energy 1939—1956*, New Haven and London, Yale University Press.

Košutić, B.P., Lukić, R.D., 2007, *Uvod u pravo*, Beograd, Pravni fakultet Univerziteta u Beogradu, Centar za publikacije, Javno preduzeće „Službeni glasnik".

Marković, R., 2008, *Ustavno pravo i političke institucije*, Beograd, Pravni fakultet Univerziteta u Beogradu, Javno preduzeće „ Službeni glasnik".

Mijalković, S., 2011, *Nacionalna bezbednost*, Beograd, Kriminalističko-policijska akademija.

Milenković, D., 2010, *Priručnik za primenu zakona o slobodnom pristupu informacijama od javnog značaja*, Beograd, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

Parezanović, N., 1995, *Osnovi računarskih sistema*, Beograd, IP „Nauka".

Simeunović, D., 2009, *Uvod u političku teoriju*, Beograd, Institut za političke studije.

Simeunović, 2002, *Teorija politike I deo*, Beograd, Udruženje nauka i društvo .

Stajić, Lj., 2010, *Osnovi sistema bezbednosti sa osnovama istraživanja bezbednosnih pojava*, Pravni fakultet Novi Sad, Novi Sad, 2010.

Tomić, Z. R., 2009, *Opšte upravno pravo*, Beograd, Pravni fakultet Univerziteta u Beogradu, Javno preduzeće „Službeni glasnik" .

Weber, M., 1946, *Essays in sociology*, New York, Oxford University Press.

ISTRAŽVANJA

Brown, P., Gutmann, J., Voigt, S., 2014, *Let the sunshine in: Why countries adopt freedom of information acts*, University of Hamburg, Institute of Law and Economics.

Curtin D., 2014, *Challenging Executive Dominance in European Democracy*, University of Amsterdam, Amsterdam Law School Legal Studies Research Paper No. 2013-77; Amsterdam Centre for European Law and Governance Research Paper No. 2013-09 .

Sulchofer, S., 2010, *Secrecy and Democracy: Who controls Informations in National security state?*, Public Law & legal theory research paper series, working paper no. 10-53 , University School of Law, New York.

Van der Sloot, B., 2014, *Privacy in the post NSA era, Time for a Fundamental Revision,* Institute for Information Law (IViR), University of Amsterdam.

ČLANAK IZ ČASOPISA

Aftergood, S., 2012, Reducing Goveernment Secrecy: Finiding What Works, *Yale Law&policy* 27:339.

Edmunds, T., 2007, Prilagođavanje demokratiji: Misli o „tranziciji" u Srbiji i na zapadnom Balkanu, *Bezbednost zapadnog Balkana*, oktobar 2007- mart 2008 (7-8), 4-9

Epps, D., 2008, Mechanisms of secrecy, *Harward Law Review*, 121:1560-1562, 1562-1564.

Fenster, M., 2014, The implausibility of secrecy, *Hastings law journal*, 65:309,325-333.

Johst, K., 2005, Government Secrecy, *CQ Researcher*, Volume 15 (42), 1005-10028.

Popović, Đ., 2009, Komentar zakona o tajnosti, *Bezbednost Zapadnog Balkana*, Oktobar-decembar 2009 (15), 3-10.

Pozen, D. E., 2010, Deep secrecy, *Stanford Law Review*, 62(2),257.

Simmel, G., 1906, The Sociology of Secrecy and of Secret societies, *American journal of sociology*, The University of Chicago Press, Volume 11(4), 441-498.

KORPORATIVNA IZDANJA

Open Society Foundations, Open Society Initiatives, 2013, The Global Principles on National Security and the Right to Information (Tshwane principles), New York, Open Society Foundations, Open Society Initiatives.

Transparency International UK, 2014, Classified Information A review of current legislation across 15 countries & EU, London, Transparency International UK.

ZBORNICI RADOVA

Gajin, S., 2012, Razvoj i međusobno usklađivanje normativnih okvira pristupa informacijama od javnog značaja i zaštite tajnih podataka, 7-17 , P*ristup informacijama od javnog značaja i zaštita tajnih podataka*, Beograd, 2012.

Matić, G., 2012, Zakon o tajnosti podataka (prikaz pojedinih novih instituta), 7-24, *Sistemi zaštite tajnih podataka, Zaštita tajnih podataka u Srbiji, Sloveniji, Bosni i Hercegovini i Crnoj Gori*, Beograd, 2012.

Matić, G., 2014, Praktični aspekti primene zakona o tajnosti podataka iz 2009. godine, 11-24, *Primena zakona o tajnosti podataka, 10 najznačajnijih prepreka,* Beograd ,2014.

Stanković, M., 2014, Neki praktični problem u primeni zakona o tajnosti podataka, 100-106, *Primena zakona o tajnosti podataka, 10 najznačajnijih prepreka*, Beograd, 2014.

Šabić, R., 2012, Otvorena pitanja primene zakona o slobodnom pristupu informacijama od javnog značaja u period nakon usvajanja zakona o tajnosti podataka, 24-29, *Pristup informacijama od javnog značaja i zaštita tajnih podataka*, Beograd, 2012

Šabić, R., 2014, Pet godina „primene" zakona o tajnosti podataka, 33-39, *Primena zakona o tajnosti podataka, 10 najznačajnijih prepreka*, Beograd, 2014.

Vodinelic, V., 2012, Normiranje informacionog trougla,18-23, *Pristup informacijama od javnog značaja i zaštita tajnih podataka*, Beograd, 2012.

Vodinelić, V., 2014, Otvaranje dosijea političkih policija: između podataka o ličnosti, tajnih podataka i podataka od javnog značaja, 40-45, *Primena zakona o tajnosti podataka, 10 najznačajnijih prepreka,* Beograd ,2014.

ČLANCI SA KONFERENCIJA

Rumsfeld, D.H., 2002, There are known knowns, *US Department of Defense News Briefing*, The Pentagon, February 12.

INTERNET

(http://www.arhivinfo.org.rs/radovi-2012/radovi/Zastita%20tajnih%20podataka.pdf)

Zakon o tajnosti podataka Republike Slovenije http://nato.gov.si/eng/documents/classified-info-act/)

Sweden Public Acess to Information and Secrecy Act http://www.government.se/information-material/2009/09/public-access-to-information-and-secrecy-act/

Czech Republic Act N. 412 of 21 September 2005 on the Protection of Classified Information http://www.nbu.cz/en/legislation/

Odluka Ustavnog suda U 149/01 http://www.sirius.rs/praksa/9465

Odluka saveta EU (2013/488/EU) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2013.274.01.0001.01.ENG

US Executive Order 13526- Classified National Security Information https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

DOD 5200.2-R Personal Security program http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

PRAVNI AKTI

Službeni glasnik Republike Srbije, 98/2006, Ustav Republike Srbije, Beograd, JP „Službeni glasnik“.

ZAKONI

Službeni glasnik Republike Srbije, 120/2004, 54/2007, 104/2009 i 36/2010, Zakon o slobodnom pristupu informacijama od javnog značaja, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije , 97/2008, 104/2009-dr. zakon, 68/2012- odluka US i 107/2012, Zakon o zaštiti podataka o ličnosti, Beograd, „Službeni glasnik“.

Službeni glasnik Republike Srbije, 104/2009, Zakon o tajnosti podataka, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 44/2010, 60/2010, 60/2013-odluka US i 62/2014, Zakon o elektronskim komunikacijama, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 116/2007 I 72/2012, Zakon o osnovama uređenja službi bezbednosti Republike Srbije, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 72/2011, Zakon o zaštiti poslovne tajne, Beograd, JP „Službeni glasnik“.

Službeni list SFRJ, 44/76-1329, Krivični zakonik, Beograd, JP „Službeni list SFRJ“.

Službeni list SRJ, 35/92-651, Krivični zakonik, Beograd, JP „Službeni list SRJ“.

Službeni glasnik Republike Srbije, 88/2009, 55/2012. Odluka US i 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 42/2002, 111/2009, 65/2014-odluka US i 66/2014, Zakon o bezbednosnoinformativnoj agenciji, Beograd, JP „Službeni glasnik“.

Narodne Novine Republike Hrvatske, 79/07, 86/12 Zakon o tajnosti podataka Republike Hrvatske, Zagreb, DD. „Narodne Novine“.

Službeni glasnik Bosne i Hercegovine, 54/05, Zakon o tajnosti podataka BiH, Sarajevo, JP NIO „Službeni list“.

UREDBE

Službeni glasnik Republike Srbije, 12/2009, Uredba o osnivanju Kancelarije Saveta za nacionalnu bezbednost, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 31/2001, 131/2001, Uredba o stavljanju na uvid određenih dosijea o građanima Republike Srbije u Službi državne bezbednosti, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 30/10, Uredba o obrascima bezbednosnih upitnika, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 54/10, Uredba o sadržini, obliku i načinu dostavljanja sertifikata za pristup tajnim podacima, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 72/10, Uredba o određivanju poslova bezbednosne zaštite određenih lica i objekata, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 79/10, Uredba o uvećanju plate državnih službenika i nameštenika koji obavljaju poslove u vezi sa zaštitom tajnih podataka u Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka i Ministarstvu pravde, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 89/10, Uredba o sadržini, obliku i načinu vođenja evidencija za prstup tajnim podacima, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 8/11, Uredba o načinu i postupku označavanja tajnosti podataka, odnosno dokumenata, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 53/11, Uredba o posebnm merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 90/11, Uredba o posebnim merama nadzora nad postupanjem sa tajnim podacima, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 97/11, Uredba o posebnim merama fizičko-tehničke zaštite tajnih podataka, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 46/13, Uredba o bližim kriterijumima za određivanje stepena tajnosti “Državna tajna” I “Strogo poverljivo”, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 70/13, Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” I “ Interno” u Bezbednosno informativnoj agenciji, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 86/13, Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” I “ Interno” u Kancelariji saveta za nacionalnu bezbednost I zaštitu tajnih podataka, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 105/13, Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” I “ Interno” u Ministarstvu unutrašnjih poslova, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije , 79/14, Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” I “ Interno” u organima javne vlasti, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 63/13, Uredba o posebnim merama zaštite tajnih podataka koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 66/14, Uredba o bližim kriterijumima za određivanje stepena tajnosti “Poverljivo” i “ Interno” u Ministarstvu odbrane, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 82/14, Uredba o postupku javne nabavke u oblasti bezbednosti, Beograd, JP „Službeni glasnik“.

PRAVILNICI, ODLUKE

Službeni glasnik Republike Srbije, 85/2013, Pravilnik o službenoj legitimaciji i načinu rada lica ovlašćenih za vršenje nadzora nad sprovođenjem zakona, Beograd, JP „Službeni glasnik“.

Službeni glasnik Republike Srbije, 88/2009, Strategija nacionalne bezbednosti, Beograd, JP „Službeni glasnik“.