

УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

ЗАШТИТА ТАЈНИХ ПОДАТАКА У РЕПУБЛИЦИ СРБИЈИ

ДИПЛОМСКИ РАД

МЕНТОР:

Проф. др Зоран Кековић

КАНДИДАТ:

Богдан Миленковић 396/11

Београд, 2017. године

САДРЖАЈ

УВОД.....	1
1.СИСТЕМ ДРЖАВНЕ БЕЗБЕДНОСТИ.....	3
2.ПОЈАМ ИНФОРМАЦИЈЕ.....	4
3.ПОЈАМ И ВРСТЕ ПОДАТАКА.....	5
3.1.Тајни податак.....	5
3.1.1.Страни тајни податак.....	6
3.1.2.Документ.....	6
5. ОРГАНИЗАЦИЈА ПРИСТУПА ОБРАДИ ТАЈНИХ ПОДАТАКА.....	8
5.1.Овлашћена лица за одређивање тајности података.....	9
5.2. Поступак одређивања тајности података.....	9
5.3.Ознаке и степен тајности података.....	10
5.4. Означивање страних тајних података.....	10
5.5.Временско ограничење трајности података.....	11
5.5.1. Продужење временског рока чувања тајности података.....	11
5.5.2. Периодична процена тајности.....	12
6. КРИТЕРИЈУМИ, ПОСТУПЦИ И МЕРЕ ЗА ЗАШТИТУ ТАЈНИХ ПОДАТАКА.....	13
6.1. Критеријуми заштите тајних података.....	13
6.2. Мере заштите тајних података.....	13
6.3. Чување, преношење и достављање тајних података.....	14
6.4. Дужност обавештавања у случају губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних података и страних тајних података.....	14
7. ПРИСТУП ТАЈНИМ ПОДАЦИМА.....	16
7.1.Приступ тајним подацима без сертификата.....	16
7.2. Поступак за издавање сертификата односно дозволе.....	17
7.3. Подношење захтева.....	18
7.4. Садржина захтева.....	19
7.5. Безбедносна провера.....	19
7.6. Рок за вршење безбедносне провере.....	21
7.7. Безбедносни упитник.....	23
7.8.Одбијање захтева за издавање сертификата односно дозволе.....	25
7.9. Престанак важења сертификата.....	25
8.КОНТРОЛА И НАДЗОР.....	26
8.1. Унутрашња контрола.....	26
8.2. Министарство правде.....	26
8.3. Канцеларија Савета за националну безбедност.....	27
9.СЛОБОДА ПРИСТУПА ИНФОРМАЦИЈАМА И ГЛОБАЛИЗАЦИЈА.....	28
10. ПРАВО НА СЛОБОДАН ПРИСТУП ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА И ЗАШТИТА ТАЈНИХ ПОДАТАКА.....	29
10.1.Ограничења слободе приступа информацијама.....	31
10.2. Устав Републике Србије и право на слободан приступ информацијама.....	31
10.3.Међународна сарадња у области заштите тајних података.....	32
10.3.1.Конвенција 205 Савета Европе о приступу службеним документима.....	33
11. КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА.....	36
11.1.Организациона структура канцеларије.....	37

12. ПРАВНИ ОКВИР ПРИМЕНЕ ПОСТУПАКА И МЕРА ЗА ТАЈНО ПРИКУПЉАЊЕ ПОДАТАКА	39
12.1. Законска терминологија	39
12.2. Посебне доказне радње	40
13. КАЗНЕНЕ ОДРЕДБЕ	43
13.1. Кривично дело	43
13.2. Прекршајна одговорност одговорног лица у органу јавне власти	43
14. ОБАВЕЗЕ КОЈЕ ПРОИЗИЛАЗЕ ИЗ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА.....	45
ЗАКЉУЧАК.....	46
ЛИТЕРАТУРА	48

УВОД

Република Србија у XXI веку, налази се на путу реформи и транзиције у демократски уређено друштво, које спроводи више и мање успешно кроз процедуре приступања европским интеграцијама. Први корак на овом путу представља хармонизација прописа из области безбедности са стандардима Европске Уније и Савета Европе, како у погледу заштите зајамчених људских слобода и права, тако и у смеру остваривања интереса националне, али и регионалне безбедности. Следећи корак представља имплементација ових законских решења у друштво и праксу поступања и организовања државних органа. Један од најзначајнијих пројеката, везаних за реформу система безбедности, са којима се Србија суочава у овим процесима је реформа националног система заштите тајних података. Посматрајући позитивно - правна решења из правног система Републике Србије у области заштите тајних података, можемо закључити, са једне стране, да многобројни прописи из ове области нису усаглашени са савременим општеприхваћеним међународним стандардима и упоредно - правним искуством, што за последицу има неадекватну заштиту националних тајних података, а са друге стране отежану сарадњу у процесу размене тајних података са другим државама и међународним организацијама.

У сваком друштву постоје одређени подаци и информације, које су недоступне јавности и као такве изузете од обавезе увида и давања грађанима, а као такве су проглашене тајним, због чега је током дуге историје човечанства, тајни податак представљао једно од основних средстава моћи у рукама власти. Када говоримо о корацима уређења области тајних података у Републици Србији, морамо имати у виду да је то била област националне безбедности којој је у последњих 20 година било посвећено најмање пажње у законодавној делатности.

Када говоримо о мерама безбедности можемо рећи да су оне скупови радњи, активности и поступака које предузимају сви субјекти система националне безбедности како би из стања свакодневног ангажовања организационих, кадровских, материјалних, техничких и функционалних капацитета прешли у стање веће спремности за извршавање безбедносних послова и задатака који се по сложености и озбиљности разликују од свакодневног - редовног ангажовања. Циљ ових мера јесте да се благовремено спречи наступање појава које могу да угрозе националну безбедност.

У раду су приказани најзначајнији институти Закона о тајности података, уз напомену да се у предстојећем периоду тек треба подзаконским актима детаљније уредити ова област. Осим Закона о тајности података, значајан осврт дат је и на објашњење рада Канцеларије Савета за националну безбедност и заштиту тајних података, као и на право на слободан приступ информацијама од јавног значаја.

1.СИСТЕМ ДРЖАВНЕ БЕЗБЕДНОСТИ

Систем државне безбедности представља правним прописима и политичким одлукама предвиђен и уређен делокруг надлежности, права и дужности безбедносних и обавештајних служби, војске, полиције и других институција у склопу система националне безбедности, који систематски прикупљају, обрађују и презентују обавештајна и безбедносна сазнања и спроводе друге активности по захтеву носилаца државне власти, с циљем да остваре унутрашњу и спољну безбедност земље.

Када говоримо о државној безбедности ту се пре свега мисли на заштиту државног јединства, унутрашње стабилности и правног и политичког система и друштвене заједнице целини. Такав степен заштите постиже се благовременим откривањем и елиминисањем постојећих или предстојећих појава и процеса, који се негативно одражавају на стање безбедности саме државе. По правилу, угрожавање државне безбедности је организовано и конспиративно, односно тајно или потајно(прикривено), док су његови носиоци појединци, групе лица, организације и институције које непосредно организују или спроводе обавештајне или субверзивне активности у земљи или иностранству. Полазећи од тога, појму безбедности државе не припада само заштита државног апарата као хијерархијске организације састављене од индивидуалних и колективних носилаца државне власти, него и заштићеност територије и становништва обухваћених једном државном организацијом.

Јавну безбедност у основи можемо схватити као стање заштићености јавног поретка, односно заштите грађана и њихове имовине. Под јавним поретком подразумевамо укупност јавних интереса зајамчених и заштићених правним системом, без обзира на то да ли је реч о општим (јавни ред и мир и слично) или појединачним правилима (личне слободе и права, имовина и друго). Јавна безбедност се остварује откривањем, спречавањем и сузбијањем кривичних и других кажњивих дела, одржавањем јавног реда и мира, осигуравањем функционисања саобраћаја на путевима, заштитом од пожара и експлозија и вршењем других стручних и административних послова.

2. ПОЈАМ ИНФОРМАЦИЈЕ

Продуктивност савремених система у великој мери зависи од брзине доношења одлука и квалитета управљања. Одлучивање, а тиме и квалитет управљања у потпуности зависе од квалитета информација. Од бројних атрибута информација „квалитет информација у потпуности зависи од скупа релативно независних атрибута:

- *поверљивости* - да информације нису откривене неовлашћеним корисницима;
- *интегритета* - да информације нису неовлашћено измењене;
- *распољивости* – да су информације доступне легитимним корисницима када је то потребно“ (Грубор и сар., 2012: 3).

Квалитет процесираних, складиштених и преношених информација у савременим високо дистрибуираним системима зависи од функционалне повезаности и безбедности система и његовог окружења, односно од имплементираног система заштите.

Безбедност информација или информациона безбедност, примарно подразумевају безбедност информација, а секундарно безбедност објеката, чиме се посредно штите информације. Овакав приступ имплицира да је крајњи циљ безбедности и заштите – заштита информација и података, која се директно или посредно постиже заштитом информационе имовине. Док се у страној литератури користе термини попут (енг. *information security*; нем. *Informations – sicherheit*; рус. *безопасност информации*), код нас су заступљени термини *информациона безбедност* и *безбедност информација*, који увек имплицирају на безбедност информационе имовине у целини.

У пракси постоје бројне дефиниције безбедности информација, зависно од нивоа апстракције. На нивоу државе то је „стање заштићености националних интереса у информационој сфери, одређених скупом личних, пословних и државних интереса“ (Грубор и сар., 2012: 4). Како се безбедност информација обезбеђује заштитом, може се дефинисати и као „заштићеност информација од случајних и намерних активности природног или вештачког карактера, које могу нанети неприхватљиву штету информационој имовини организације“ (Грубор и сар., 2012: 4).

Безбедност информационо – телекомуникационих система је објективна мера стања ризика или стања безбедног, поузданог и неометаног функционисања система, у односу на себе самог и своје окружење. Систем се сматра безбедним, ако је заштићен од утицаја фактора ризика.

3. ПОЈАМ И ВРСТЕ ПОДАТАКА

Када говоримо о подацима у најширем смислу, можемо издвојити неколико подела. Пре свега, подаци могу бити јавни – доступни најширој јавности и публиковани путем различитих медија, који се у стручној јавности називају и „отвореним“ подацима. Затим, подаци могу бити са ограниченим приступом из различитих правних разлога, односно:

1. **Подаци од интереса за Републику Србију**, који представљају сваки податак којим располажу органи јавне власти, у смислу Закона о тајности података, који се односи на територијални интегритет и суверенитет, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње и спољне послове. У формалном смислу овде је реч о подацима који су законом, другим прописом или одлуком надлежног органа деносеном у складу са законом, одређени и означени одговарајућим степеном тајности.
2. **Подаци о личности** представљају сваку информацију која се односи на физичко лице, без обзира на облик у којем је изражен и на носач информација (папир, трака, филм, електронски медијум и слично), без обзира на околност чувања информација, без обзира на начин прибављања (слушањем, гледањем, путем увида у документ и слично) и без обзира на друга својства те информације. Податак о личности је зато сваки податак који се односи на физичко лице ако је оно одређено или одредиво.
3. **Пословне тајне** уређене су посебним прописима и не спадају у област заштите тајних података. Оне проистичу из прописа којима се уређује лекарска, психијатријска и психолошка делатност, адвокатура, свештенички позив и слично.
4. **Професионалне тајне** представљају област која није довољно законски уређена. Постоји само правни основ или један законски члан у прописима о привредним друштвима, а сама обрада и критеријуми су препуштени привредним друштвима да их сами уреде. Нека од становишта упућују на то да би ову област требало уредити слично као и у закону о тајности података, односно по облику и обиму штете која наступа у привредним друштвима неовлашћеним откривањем података.

3.1. Тајни податак

Према Закону о тајности података дефинисан је као „тајни податак је податак од интереса за Републику Србију које је законом, другим прописом или одлуком надлежног органа донесен у складу са законом, одређен и означен одређеним степеном тајности“ (Закон о тајности података, 2009).

Законом су такође одређени и *подаци који се не сматрају тајним подацима*. Према дефиницији Љубомира Стајића „то су сви они подаци који су означени као тајни а за циљ имају прикривање кривичног дела, прекорачење овлашћења или злоупотребу службеног положаја или другог незаконитог акта или поступања органа јавне власти“ (Стајић, 2011: 347).

3.1.1.Страни тајни податак

Одређен је као „податак који Републици Србији повери страна држава или међународна организација уз обавезу да га чува као тајни, као и тајни податак који настане у сарадњи Републике Србије са другим државама, међународним организацијама и другим међународним субјектима, у складу са закљученим међународним споразумом које са страном државом, међународном организацијом или другим међународним субјектом закључила Република Србија“ (Закон о тајности података, 2009).

3.1.2.Документ

Одређен је као „сваки носач података (папир, магнетни или оптички медиј, дискета, усб меморија, смарт картица, компакт диск, микро филм, видео и аудио запис и друго) на коме је записан или меморисан тајни података“ (Закон о тајности података, 2009). Дакле под документом се у овом смислу подразумева сваки физички уређај који садржи тајни податак.

4.ТАЈНА

У најширем смислу, под појмом тајне се подразумева све оно што је непознато. На основу излагања Љубомира Стајића „сва досадашња изучавања појма тајне полазе од тога да је могуће говорити о две основне врсте тајни:

- апсолутној(општој) тајни – непознатој свима (тајне науке,придоде и др.);
- релативној, која представља непознаницу само за неког(одређени круг људи, неко друштво итд.)“ (Стајић, 2011: 345).

Релативна тајна јавља се као продукт различитих интереса одређене групе људи, односно одређених друштвених односа. Тајна је често била злоупотребљавана и коришћена као основ опстанка власти, прикривање незаконитог и неправилног рада носиоца највиших државних функција или расипништва и корупције. Интересантно је и тумачење Дејана Миленковића, који износи став да је „тајност одлика недемократских и затворених система. Међутим, чак и високо развијене демократске земље, настоје да врше своје послове скривено од очију јавности“ (Миленковић, 2003: 44). Јер, како је то речено „свака власт је као печурка и најбоље расте и развија се у мраку“ (Радојковић, 2002: 29). Такво мишљење доминирало је и у правној теорији 20. века. Волтер Багехот, угледни британски теоретичар тог времена, сматрао је да демократија може функционисати „само ако су њени прави владари заштићени од вулгарних испитивања“ (Freedom of information, 2004: 10).

5. ОРГАНИЗАЦИЈА ПРИСТУПА ОБРАДИ ТАЈНИХ ПОДАТАКА

Што се тиче саме организације приступа обради тајних података, она је била организована по ресорном моделу. Наиме постојало је више заокружених нормативних области и то у оквиру: - система одбране; - система спољних послова; - система унутрашњих послова; - Безбедносно-информативне агенције (након издвајања ресора државне безбедности из система унутрашњих послова); - система министарства надлежног за правосуђе(извршење заводских санкција и правосудни органи); - Народне банке Србије; као и осталих органа државне управе.

Сама реформа области заштите тајних података подразумева :

1. реформу националног система безбедности;
2. уставне и законске измене, кроз хармонизацију прописа са прописима и стандардима Европске уније у овој области;
3. едукацију и обуку кадрова који непосредно учествују у креирању и заштити тајних података;
4. евалуацију од стране међународних институција кроз успостављање процеса билатералне сарадње, али и оне везане за Европску унију, НАТО и слично;
5. превођење практичних позитивних и негативних искустава у одговарајућу законску и подзаконску регулативу.

Имајући у виду изнето, можемо закључити да је уређење система заштите тајних података процес који траје, а упоредна искуства држава које су прошле овакве процесе говоре о деценијском периоду. У државама источно-европске оријентације (друштва у транзицији), након распада Варшавског уговора, у пракси организовања националног безбедносног тела за заштиту тајних података карактеристично је постојање два модела, и то се наводе: „централизовани модел (Чешка, Словачка, Бугарска, Македонија, Хрватска...) – који се карактерише формирањем нове службе безбедности, додуше општебезбедносне или безбедносне надлежности“ (Матић, 2012: 9), која представља централну националну извршну власт у области заштите тајних података, са великим бројем запослених и разноврсним надлежностима од контроле рада цивилних и војних служби безбедности до рада са тајним потписима; и као други модел се наводи: „децентрализовани модел (Мађарска, Словенија, Босна и Херцеговина, Црна Гора...) – који представља само једног од носиоца заштите тајних података на националном нивоу“ (Матић, 2012: 9) и карактерише се подељеном надлежношћу са ресорним министарствима и агенцијама, односно представља малобројну стручну агенцију која се бави координацијом свих надлежности државних органа који се баве пословима безбедности и заштитом тајних података.

5.1.Овлашћена лица за одређивање тајности података

Тајност података, под условима и на начин утврђен Законом о тајности података, одређује овлашћено лице. Као овлашћена лица наводе се:

- „председник Народне скупштине;
- председник Републике;
- председник Владе;
- руководилац органа јавне власти;
- изабрани, постављени или именовани функционер органа јавне власти који је за одређивање тајних података овлашћен законом, односно прописом донесеним на основу закона, или га је за то писмено овластио руководилац органа јавне власти;
- лице запослено у органу јавне власти које је за то писмено овластио руководилац тог органа“ (Закон о тајности података, 2009).

5.2. Поступак одређивања тајности података

Поступак одређивања тајности података започиње приликом његовог настанка, односно када орган јавне власти започне обављање посла чији је резултат настанак тајног податка.

Лице које је запослено, односно које обавља одређене послове у органу јавне власти дужно је да, у оквиру својих радних задатака, односно овлашћења, обавести овлашћено лице о подацима који би могли да буду одређени као тајни. При одређивању тајности података овлашћено лице процењује могућу штету по интересе Републике Србије.

Одлука о одређивању степена тајности доноси се на основу процене могуће штете по интересе Републике Србије, и у складу са тим, врши се обележавање документа ознаком тајности предвиђеном овим законом. Ова одлука доноси се у писаном облику са образложењем.

Посебни случајеви одређивања и означавања тајних података наступају када овлашћено лице одређује као тајни податак онај податак који је настао обједињавањем или повезивањем података који само по себи нису тајни, ако тако обједињени или повезани представљају податак који треба заштити из разлога утврђеним овим законом.

5.3.Ознаке и степен тајности података

Документ који садржи тајне податке означава се:

- 1) ознаком степена тајности;
- 2) начином престанка тајности;
- 3) подацима о овлашћеном лицу;
- 4) подацима о органу јавне власти.

Влада прописује начин и поступак означавања тајности података, односно докумената.

Податак садржи следеће степене тајности:

- 1) "ДРЖАВНА ТАЈНА", који се одређује ради спречавања настанка неотклоњиве тешке штете по интересе Републике Србије;
- 2) "СТРОГО ПОВЕРЉИВО", који се одређује ради спречавања настанка тешке штете по интересе Републике Србије;
- 3) "ПОВЕРЉИВО", који се одређује ради спречавања настанка штете по интересе Републике Србије;
- 4) "ИНТЕРНО", који се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио.

Критеријуме за одређивање степена тајности "ДРЖАВНА ТАЈНА" и "СТРОГО ПОВЕРЉИВО" одређује Влада на основу претходно прибављеног мишљења Савета за националну безбедност, док за податке степена тајности "ПОВЕРЉИВО" и "ИНТЕРНО" одређује Влада на основу предлога надлежног министра или руководиоца надлежног органа.

5.4. Означавање страних тајних података

Документ који садржи тајни податак означава се степеном тајности којим је означен у страниј држави или међународној организацији. При означавању степена тајности документа намењених за сарадњу са страним државама, међународним организацијама, односно другим субјектима међународног права могу се користити и одговарајуће ознаке степена тајности на енглеском језику и то:

- 1) "TOP SECRET" одговара ознаци степена тајности "ДРЖАВНА ТАЈНА";
- 2) "SECRET" одговара ознаци степена тајности "СТРОГО ПОВЕРЉИВО";
- 3) "CONFIDENTIAL" одговара ознаци степена тајности "ПОВЕРЉИВО";
- 4) "RESTRICTED" одговара ознаци степена тајности "ИНТЕРНО".

Начин на који је ова материја регулисана, објашњен је у раду „Српска правна ревија“: „такође се може уочити да међународне безбедносне и друге организације у својим регулативама крајње уопштено одређују процедуре размене тајних података и да приликом усклађивања националног законодавства са њиховом регулативом не инсистирају на квалитету података који ће бити предмет размене, већ је то препуштено слободној процени и нивоу успостављене сарадње у области безбедности и одбране, као и у другим областима“ (Јовичић, 2008: 41).

5.5. Временско ограничење трајности података

Тајност података престаје:

- 1) датумом *утврђеним у документу у коме је садржан тајни податак*, односно ако овлашћено лице у поступку одређивања тајности утврди да наступањем одређеног датума престају разлози због којих је податак проглашен за тајни, утврдиће датум престанка тајности и означити га у документу који садржи такав податак
- 2) *наступањем одређеног догађаја утврђеног у документу у коме је садржан тајни податак* утврђује да ли тајност престаје наступањем тог догађаја и означити га у документу који садржи такав податак;
- 3) *истеком законом одређеног рока*; ДРЖАВНА ТАЈНА-30 година, за податак са ознаком СТРОГО ПОВЕРЉИВО-15 година, за податак са ознаком ПОВЕРЉИВО-5 година и за податак са ознаком ИНТЕРНО-2 године;
- 4) *опозивом тајност* се утврђује да податак престаје да буде тајни пре истека предвиђеног рока;
- 5) *ако је податак учињен доступним јавности*. Овлашћено лице може да промени начин који је одређен за престанак тајности податка, ако за то постоје основани разлози, у складу са законом. О промени из става 2. овог члана, овлашћено лице је дужно да о томе, без одлагања, у писаном облику обавести органе јавне власти и лица која су тајни податак добила или имају приступ том податку.

5.5.1. Продужење временског рока чувања тајности података

Уколико и након истека временског рока постоје разлози да се податак и даље чува као тајни, овлашћено лице може продужити временски рок за чување тајности података утврђен за одређене степене тајности.

Како се наводи у Закону о тајности податак „Влада може продужити рок чувања тајности у случајевима:

- 1) када би њихово откривање имало непоправљиве тешке штетне последице по националну безбедност и нарочито битне државне, политичке, економске или војне интересе Републике Србије;
- 2) када је то предвиђено међународним споразумом или другим међународним обавезама Републике Србије;
- 3) када би њихово откривање имало непоправљиве тешке последице по основна људска и грађанска права једног или више лица, или би угрозило безбедност једног или више лица“ (Закон о тајности података, 2009).

5.5.2. Периодична процена тајности

Закон о тајности података наглашава да „овлашћено лице врши периодичну процену тајности, на основу које може извршити опозив тајности, и то:

- 1) за податак означен степеном "ДРЖАВНА ТАЈНА", најмање једном у десет година;
- 2) за податак означен степеном "СТРОГО ПОВЕРЉИВО", најмање једном у пет година;
- 3) за податак означен степеном "ПОВЕРЉИВО", најмање једном у три године;
- 4) за податак означен степеном "ИНТЕРНО", најмање једном годишње“ (Закон о тајности података, 2009).

6. КРИТЕРИЈУМИ, ПОСТУПЦИ И МЕРЕ ЗА ЗАШТИТУ ТАЈНИХ ПОДАТАКА

6.1. Критеријуми заштите тајних података

Када орган јавне власти успоставља систем поступака и мера заштите тајних података према следећим критеријумима:

- степену тајности;
- природи документа у коме је садржан тајни податак;
- процени претње по безбедност тајног податка.

6.2. Мере заштите тајних података

Врсте мера заштите су опште и посебне мере које се предузимају ради спречавања настанка штете, односно мере које се односе на остваривање административне, информатичко-телекомуникационе, персоналне и физичке безбедности тајних података.

Као опште мере заштите тајних података у Закону о тајности података, наводе се:

- „одређивање степена тајности;
- процену претње за безбедност тајног податка;
- одређивање начина коришћења и поступања са тајним податком;
- одређивање одговорног лица за чување, коришћење, размену и друге радње обраде тајног податка;
- одређивање руковооца тајним подацима, укључујући и његову безбедносну проверу у зависности од степена тајности података;
- одређивање посебних зона, зграда и просторија намењених заштити тајних података и страних тајних података;
- надзор над поступањем са тајним податком;
- мере физичко-техничке заштите тајног податка, укључујући и уградњу и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту бан безбедносне зоне;
- мере заштите информационо-телекомуникационих система;
- мере крипто-заштите;
- заштитни режим радних и формацијских места, у оквиру акта о унутрашњем уређењу и систематизацији радних места;
- утврђивање посебних програма образовања и обуке за потребе обављања послова заштите тајних података;

- друге опште мере одређене законом“(Закон о тајности података, 2009).

У циљу ефикасне примене општих мера заштите тајних података, актом Владе утврђују се посебне мере заштите тајних података. Поједине посебне мере заштите могу се ближе уредити актом надлежног министра, односно руководиоца посебне организације, у складу са актом Владе.

6.3. Чување, преношење и достављање тајних података

Тајни подаци чувају се на начин тако да је приступ тим подацима дозвољен само овлашћеним корисницима. Тајни подаци могу се преносити и достављати изван просторија органа јавне власти само уз придржавање прописаних мера безбедности и поступака којима се обезбеђује да податке добије само лице које има сертификат за приступ тајним подацима и које има право да их добије.

Приликом преношења и достављања тајних података изван просторија органа, поступци и мере заштите одређују се према степену тајности тих података, у складу са законом и прописом донетим на основу закона.

Преношење и достављање тајних података коришћењем телекомуникационо-информатичких средстава врши се уз обавезну примену прописаних мера крипто-заштите.

6.4. Дужност обавештавања у случају губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних података и страних тајних података

Када дође до сазнања да је дошло до губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних података и страних тајних података, функционер, запослено лице, односно лице која обавља послове у органу јавне власти, без одлагања обавештава овлашћено лице органа јавне власти.

Лице из члана 35. став 2. овог закона које утврди да је приликом преноса и достављања тајних података изван просторија органа јавне власти, дошло до губитка, крађе, оштећења, уништења или неовлашћеног откривања тајног податка и страног тајног податка, без одлагања обавештава овлашћено лице органа који му је тајне податке и стране тајне податке пренео, односно доставио.

Овлашћено лице дужно је да без одлагања предузме све потребне мере за утврђивање околности због којих је дошло до губитка, крађе, оштећења, уништења или неовлашћеног откривања тајног податка и страног тајног податка, изврши процену проузроковане штете, као и да предузме потребне мере у циљу отклањања штете и спречавања поновног губитка, крађе, оштећења, уништења или неовлашћеног откривања тајног податка и страног тајног податка.

У случају из става 3. овог члана о предузетим мерама овлашћено лице обавештава Канцеларију Савета.

7. ПРИСТУП ТАЈНИМ ПОДАЦИМА

7.1. Приступ тајним подацима без сертификата

Приступ тајним подацима и коришћење података и докумената било ког степена тајности без издавања сертификата, на основу функције и у циљу обављања послова из њихове надлежности имају председник Народне скупштине, председник Републике и председник Владе.

Државни органи које бира Народна скупштина, руководиоци државних органа које бира Народна скупштина, судије Уставног суда и судије, овлашћени су да приступе подацима свих степена тајности који су им потребни за обављање послова из њихове надлежности без безбедносне провере.

Изузетно, лица имају право на приступ тајним подацима који су означени степеном "ДРЖАВНА ТАЈНА" и "СТРОГО ПОВЕРЉИВО" уз претходну безбедносну проверу ако је то потребно за обављање послова из њихове надлежности, ако се ти подаци односе на:

- 1) радње спречавања, откривања, истраге и гоњења за кривична дела, које спроводе надлежни државни органи, до окончања истраге, односно гоњења;
- 2) начин примене посебних поступака и мера у прибављању безбедносних и обавештајних података у конкретном случају;
- 3) припаднике министарства надлежног за унутрашње послове и служби безбедности са прикривеним идентитетом, док је то неопходно ради заштите животних интереса ових лица, односно чланова њихових породица (живот, здравље и физички интегритет);
- 4) идентитет садашњих и бивших сарадника служби безбедности, односно трећих лица, док је то неопходно потребно ради заштите животних интереса ових лица, односно чланова њихових породица (живот, здравље и физички интегритет).

Приступ страним тајним подацима врши се у складу са овим законом, прописима донесеним на основу овог закона, односно у складу са међународним споразумом који је са страном државом, међународном организацијом или другим међународним субјектом закључила Република Србија, а по принципу „потребно да зна“.

7.2. Поступак за издавање сертификата односно дозволе

ПРИМЕРИ ОБРАЗАЦА ЗА ПОДНОШЕЊЕ ЗАХТЕВА И ЖАЛБИ И ШЕМАТСКИ ПРИКАЗ ПОСТУПКА:

назив и седиште органа коме се захтев упућује

ЗАХТЕВ За приступ информацији од јавног значаја

На основу чл.15. ст.1. Закона о слободном приступу информацијама од јавног значаја (Сл.гласник РС бр. 120/04), од горе наведеног органа захтевам:*

обавештење да ли поседује тражену информацију;
увид у документ који садржи тражену информацију;
копију документа који садржи тражену информацију;
достављање копије документа који садржи тражену информацију:**
поштом
електронском поштом
факсом
на други начин:*** _____

Овај захтев се односи на следеће информације:

(навести што прецизнији опис информације која се тражи као и друге податке који олакшавају проналажење тражене информације)

Тражилац информације / име и презиме

У _____,

адреса _____

дана _____ 201__ године

други подаци за контакт _____

_____ потпис

*Означити која законска права на приступ информацијама желите да остварите.

Означити начин достављања копије документа. *Када захтевате други начин достављања обавезно уписати који начин достављања захтевате.

Поступак за издавање сертификата односно дозволе, на који се примењују посебне одредбе закона којим се уређује општи управни поступак, осим ако законом то није другачије одређено, обухвата: услове за издавање сертификата физичком и правном лицу; издавање дозволе страном лицу; подношење захтева и његову садржину; безбедносну проверу. Сертификат издаје надлежни орган утврђен овим законом, на основу писаног захтева физичког лица, ако је подносилац захтева:

- 1) држављанин Републике Србије;
- 2) пунолетан;
- 3) пословно способан;
- 4) неосуђиван на безусловну казну затвора за кривично дело за које се гони по службеној дужности, односно за прекршај предвиђен овим законом;
- 5) прошао одговарајућу безбедносну проверу.

Страно лице као подносилац захтева за издавање сертификата мора испунити следеће услове:

- 1) има регистровано седиште на територији Републике Србије;
- 2) обавља делатност у вези са интересима Републике Србије;
- 3) прође одговарајућу безбедносну проверу;
- 4) није у поступку ликвидације, односно стечаја;
- 5) није кажњен мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мера безбедности забране обављања одређених регистрованих делатности или послова;
- 6) уредно плаћа порезе, односно доприносе.

Од оснивања Канцеларије Савета издато је 775 безбедносних сертификата за прступ тајним подацима:

	2011.	2012.	2013.	2014.	2015.	УКУПНО
ДРЖАВНА ТАЈНА	25	37	35	43	126	266
СТРОГО ПОВЕРЉИВО	13	86	15	45	131	290
ПОВЕРЉИВО	3	3	17	10	186	219
УКУПНО	41	126	67	98	443	775

Страном лицу надлежни орган издаје дозволу ако:

- 1) поседује одговарајући сигурносни сертификат издат од стране државе чији је држављанин, односно у којој има седиште или од стране међународне организације чији је члан;
- 2) обавеза омогућавања приступа тајним подацима проистиче из закљученог међународног споразума.

7.3. Подношење захтева

Захтев за издавање сертификата, односно дозволе подноси се Канцеларији Савета. Ако сертификат захтева руковалац или други запослени у органу јавне власти, захтев се доставља руководиоца органа јавне власти.

Ако се сертификат тражи за правно лице и запослене у правном лицу, захтев подноси законски заступник правног лица.

Захтев за издавање сертификата лицу које ће у вези са извршавањем уговорених послова са органом јавне власти имати приступ тајним подацима, подноси орган јавне власти на који се извршавање уговорених послова односи.

7.4. Садржина захтева

Закон о тајности података, дефинише *Захтев физичког лица* за сертификат садржи: „име и презиме, пребивалиште, послове које обавља, разлоге због којих се тражи сертификат, као и степен тајности података за које се тражи сертификат“ (Закон о тајности података, 2009).

Захтев правног лица садржи: „назив фирме, седиште и делатност правног лица, име и презиме и пребивалиште законског заступника правног лица, разлоге због којих се тражи сертификат, као и степен тајности података за које се тражи сертификат“ (Закон о тајности података, 2009).

7.5. Безбедносна провера

Разликују се безбедносни критеријуми који се односе на заснивање радног односа у одређеним структурама, као и за обављање одређених специфичних дужности у оквиру система (на пример службе криптозаштите, ангажовање на дужностима везаним за војне службе безбедности и слично) од оних који представљају безбедносну сметњу и ризик за руковање са тајним подацима и могу бити специфични за заснивање радног односа у спољним пословима, службама безбедности, полицији, војсци и другим осетљивим радним местима за националну безбедност.

Заједничко питање за све безбедносне провере, било да су оне везане за заснивање радног односа у државним органима, обављање одређених специфичних дужности у истима или су потребне ради приступа тајним подацима своде се на питање провере и процена података од стране полиције и овлашћених органа служби безбедности.

Методолошки се могу поделити на:

- 1) проверу по месту становања и по месту запослења;

2) проверу из јавних и других евиденција и оперативних евиденција којима располажу органи јавне власти, полиција и службе безбедности;

3) проверу података на основу међународне сарадње из евиденција које се налазе у иностранству.

Када је реч о проценама, онда је битно указати на следеће:

- 1) „**процену личности кандидата** за којег се обавља безбедносна провера – личних идентификационих података, његовог друштвеног понашања, личних особина, образовања, положаја у друштву, социјалног окружења и контаката са другим лицима, његове породице и лица са којима живи у заједничком домаћинству, раније осуђиваности и слично. Ова процена се обавља на основу јавних и других података и евиденција које воде државни органи.
- 2) **процена безбедносног ризика** – своди се на податке које оперативним радом прикупљају службе безбедности на основу индикатора угрожавања безбедности, али и процену могућег стања безбедносног ризика које би проверавано лице могло имати на националну безбедност омогућавањем приступа тајним подацима највишег нивоа“ (Матић, 2012: 18).

Приликом обављања провера и процена задире се у област обраде нарочито осетљивих података о личности за потребе безбедности, одбране и слично, тако да може представљати највећи проблем у пракси, дефинисање односа нормирано стање – дискрециона процена надлежног органа. Нарочито осетљиви подаци дефинисани су одредбама члана 16. Закона о заштити података о личности који се односе на „националну припадност; расу; пол; језик; вероисповести; припадност политичкој странци; синдикално чланство; здравствено стање; примање социјалне помоћи; жртву насиља; осуду за кривично дело; и сексуални живот“ (Закон о заштити података о личности, 2008).

Критеријуми за безбедносне сметње и процедуре различити су за:

- 1) основна безбедносна провера, за податке означене степеном тајности "ИНТЕРНО" и "ПОВЕРЉИВО", врши министарство надлежно за унутрашње послове.
- 2) потпуна безбедносна провера, за податке означене степеном тајности "СТРОГО ПОВЕРЉИВО", коју врши Безбедносно-информативна агенција;
- 3) посебна безбедносна провера, за податке означене степеном тајности "ДРЖАВНА ТАЈНА", коју такође врши Безбедносно-информативна агенција;
- 4) Безбедносну проверу за приступ тајним подацима и документима свих степена тајности за лица којима је приступ тајним подацима и документима потребан ради

обављања функција или радних дужности у министарству надлежном за послове одбране и Војсци Србије врши Војнобезбедносна агенција.

7.6. Рок за вршење безбедносне провере

Како наводи Љубомир Стајић „надлежни орган (БИА, МУП и ВБА) дужан је да, од дана пријема попуњеног упитника изврши безбедносну проверу у следећим роковима:

- до 30 дана, за основну безбедносну проверу;
- до 60 дана, за потпуну безбедносну проверу;
- до 90 дана, за посебну безбедносну проверу“ (Стајић, 2011: 354).

Ако се безбедносна провера не изврши у овим роковима, сматра се да не постоји безбедносни ризик приступа тајним подацима подносиоца захтева.

Основна и потпуна безбедносна провера

Неки од основних критеријума за безбедносне ризике и сметње су:

- 1) **Кривична осуђиваност** – питање кривичних дела која се сматрају безбедносном сметњом и ризиком, као и примена одредби Кривичног законика које се односе на брисање правних и других последица кривичне осуде. Осуђиваност представља облик стигматизације осуђених лица и има последице везане за заснивање радних односа уопште, али и за приступ тајним подацима и рад на безбедносно осетљивим радним местима;
- 2) **Кривични поступци у току** – не производе последице, осим у кривично-процесном смислу, међутим ова околност представља безбедносну сметњу и ризик за приступ тајним подацима али и за рад на безбедносно осетљивим радним местима;
- 3) **Прекршајна осуђиваност** -питање обима прекршаја који се сматрају безбедносном сметњом и ризиком, питање последица брисаних прекршајних решења (или пресуда). Знатно блаже последице за заснивање радног односа и за приступ тајним подацима, а одлука је ствар процене надлежног органа;
- 4) **Прекршајни поступци у току** – не производе последице, осим у прекршајно процесном смислу, међутим ова околност представља знатно блажу безбедносну сметњу и ризик за приступ тајним подацима од оне која се односи на кривичне поступке у току, као и за рад на безбедносно осетљивим радним местима;
- 5) **Контакт са страним службама безбедности и обавештајним службама** –могу бити планирани кроз активности државних органа (међународна сарадња, оперативна комбиновање и слично) или самоиницијативни и за рачун ових страних служби (шпијунажа);

- 6) **Учешће у активностима организације чије су деловање и циљеви забрањени** – организације које су забрањене одлукама Уставног суда или других надлежних органа или организације које у старту делују илегално (терористичке организације). Може бити повезано са другим безбедносним сметњама. Постоје и листе УН и ЕУ о овим организацијама. Питање уређења и вођења листе забрањених и илегалних организација је у надлежности Савета за националну безбедност – тзв. „црне листе“;
- 7) **Подаци о одговорности за повреду прописа који се односе на тајност података** – представљају податке којима располажу државни органи и друга правна лица која рукују тајним подацима;
- 8) **Подаци о праву својине или другом стварном праву на непокретностима, подаци о праву својине на другим стварим уписаним у јавни регистар, као и податак о годишњем финансијском извештају за претходну годину у складу са законом којим се уређује рачуноводство и ревизија;**
- 9) **Служба у страним војскама и паравојним формацијама;**
- 10) **Други подаци и чињенице који физичко лице чине подложним утицајима и притисцима који престављају безбедности ризик;**
- 11) **Дуговима насталим услед финансијских задужења или преузетих гаранција.**

Посебна безбедносна провера

Критеријуми за потребе посебне безбедносне провере обухватају, поред оних из потпуне безбедносне провере и проверу чињеница, околности и догађаја из приватног живота подносиоца захтева, најмање у последњих десет година од дана подношења захтева за издавање сертификата, које би, у случају, представљале основ за сумњу у његову поверљивост и поузданост, а нарочито ако су његове активности у спротности са интересима Републике Србије или ако је повезан са страним лицима која могу да угрозе безбедност и међународне интересе Републике Србије.

Допунска безбедносна провера

Уколико се из извештаја о резултатима безбедносне провере, али и из препоруке не може утврдити да ли су испуњени законом прописани услови за издавање сертификата физичком или правном лицу, или је после обављене безбедносне провере дошло до битне измене провераваних података који би могли бити од утицаја на издавање сертификата, Канцеларија Савета ће захтевати од надлежног органа да изврши допунску безбедносну проверу, односно допуну извештаја и израду нове препоруке, најкасније у накнадном року од 30 дана.

7.7. Безбедносни упитник

Ради вршења безбедносне провере, Канцеларија Савета доставља подносиоцу захтева безбедносни упитник. Подносилац захтева попуњава основни безбедносни упитник, а ако се сертификат захтева за тајне податке степена тајности "ДРЖАВНА ТАЈНА" и "СТРОГО ПОВЕРЉИВО", попуњава се посебан безбедносни упитник.

„У основни безбедносни упитник уносе се следећи подаци о подносиоцу захтева:

- 1) име и презиме, као и претходна имена и презимена;
- 2) јединствен матични број грађана;
- 3) датум и место рођења;
- 4) држављанство, претходна држављанства и двојна држављанства;
- 5) пребивалиште и боравиште, као и претходна пребивалишта;
- 6) брачни статус и породично стање;
- 7) подаци о лицима која живе у заједничком домаћинству са лицем на кога се односи безбедносни упитник (њихова имена и презимена, заједно са претходним именима и презименима, њихови датуми рођења, као и однос са провераваним лицем);
- 8) име и презиме, датум рођења и адреса пребивалишта сродника до другог степена сродства у правој и првог степена сродства у побочној линији, усвојиоца, старатеља, очуха, маћехе, односно хранитеља;
- 9) стручна спрема и занимање;
- 10) подаци о претходним запослењима;
- 11) подаци у вези са извршењем војне обавезе;
- 12) подаци о кривичном и прекршајном кажњавању и кривичним и прекршајним поступцима који су у току;
- 13) медицински подаци у вези са болестима зависности (алкохол, опојне дроге и др.), односно душевним болестима;
- 14) контакти са страним службама безбедности и обавештајним службама;
- 15) дисциплински поступци и изречене дисциплинске мере;
- 16) подаци о чланству или учешћу у активностима организација чије су активности или циљеви забрањени;
- 17) подаци о одговорности за повреду прописа који се односе на тајност података;
- 18) подаци о праву својине или другом стварном праву на непокретности, подаци о праву својине на другим стварима уписаним у јавни регистар, као и податак о годишњем порезу на укупан приход грађана за претходну годину;
- 19) претходне безбедносне провере“ (Закон о тајности података, 2009).

„У основни безбедносни упитник за правна лица уносе се следећи подаци о подносиоцу захтева:

- 1) назив фирме и седиште, као и претходни називи фирми и седишта;
- 2) матични број правног лица и пореско-идентификациони број;
- 3) име и презиме заступника;
- 4) датум и место оснивања;
- 5) подаци о организационим јединицама, огранцима, зависним друштвима и другим облицима повезивања;
- 6) порекло оснивачког капитала укључујући и промене у последње три године;
- 7) број запослених;
- 8) број запослених за које се тражи сертификат и врста послова које обављају;
- 9) подаци о осудама за кривично дело, привредни преступ и прекршај правног лица и одговорних лица у правном лицу, као и подаци о поступцима за кривично дело, привредни преступ или прекршај против правног лица који су у току;
- 10) подаци о контактима са страним службама безбедности и обавештајним службама;
- 11) подаци о учешћу у активностима организације чије су активности и циљеви забрањени;
- 12) подаци о одговорности за повреду прописа који се односе на тајност података;
- 13) подаци о претходној безбедносној провери;
- 14) подаци о праву својине или другом стварном праву на непокретностима, подаци о праву својине на другим стварима уписаним у јавни регистар, као и податак о годишњем финансијском извештају за претходну годину у складу са законом којим се уређује рачуноводство и ревизија“ (Закон о тајности података, 2009).

За безбедносну проверу, поред основног, испуњава се и посебан безбедносни упитник. У посебан безбедносни упитник, уносе се подаци о:

- 1) „служби у страним војскама и паравојним формацијама;
- 2) други подаци и чињенице, осим података наведених у чл. 58. и 59. које физичко, односно правно лице чине подложним утицајима и притисцима који представљају безбедносни ризик;
- 3) дуговима насталим услед финансијских задужења или преузетих гаранција“ (Закон о тајности података, 2009).

7.8.Одбијање захтева за издавање сертификата односно дозволе

Канцеларија Савета решењем одбија захтев за издавање сертификата ако се на основу извештаја безбедносне, односно допунске безбедносне провере утврди:

- 1) да је подносилац захтева навео неистините и непотпуне податке у основном, односно посебном безбедносном упитнику;
- 2) да подносилац захтева не испуњава услове за издавање сертификата;
- 3) да подносилац захтева није обезбедио услове за предузимање прописаних мера заштите тајних података;
- 4) да постоји безбедносни ризик од приступа и коришћења тајних података подносиоца захтева. Образложење решења о одбијању издавања сертификата не садржи податке који се сматрају тајним у смислу овог закона, нити навођење извора безбедносне провере.

7.9. Престанак важења сертификата

Сертификат престаје да важи:

- 1) истеком времена за које је издат;
- 2) престанком функције лица;
- 3) престанком обављања дужности и послова из делокруга рада лица;
- 4) на основу решења Канцеларије Савета донетог у поступку провере издатог сертификата;
- 5) смрћу физичког лица или престанком правног лица коме је издат сертификат.

Престанак важења сертификата истеком времена:

- сертификат издат за податак и документ означен степеном тајности "ДРЖАВНА ТАЈНА" важи три године.
- сертификат издат за податак и документ означен степеном тајности "СТРОГО ПОВЕРЉИВО" важи пет година.
- сертификат издат за податак и документ означен степеном тајности "ПОВЕРЉИВО" важи десет година.
- сертификат издат за податак и документ означен степеном тајности "ИНТЕРНО" важи 15 година.

8. КОНТРОЛА И НАДЗОР

Контролу и надзор над применом Закона о тајности података можемо поделити на „послове који се обављају у оквиру:

- унутрашње конторле;
- Канцеларије савета за националну безбедност и заштиту тајних података и
- Министарства надлежног за послове правосуђа“ (Матић, 2012: 14).

8.1. Унутрашња контрола

Унутрашњу контролу спроводи руководилац органа јавне власти. У министарству надлежном за унутрашње послове, министарству надлежном за послове одбране и Безбедносно-информативној агенцији, а по потреби и у другим органима јавне власти, за унутрашњу контролу и друге стручне послове у вези са одређивањем и заштитом тајних података систематизује се посебно радно место или се за обављање ових задатака и послова посебно задужује постојећа организациона јединица у саставу министарства или агенције.

Унутрашњом конторлом обезбеђује се редовно праћење и оцењивање појединих делатности, као и делатности органа јавне власти у целини, у вези са спровођењем овог закона и прописа и мера донетих на основу овог закона.

8.2. Министарство правде

Врши назор над спровођењем овог закона и прописа донетих на основу закона. У складу са Законом, у вршењу надзора, ово министарство:

- прати стање у области заштите тајних података;
- припрема прописе неопходне за спровођење овог закона;
- даје мишљење на предлоге прописа у области заштите тајних података;
- предлаже Влади садржину, облик и начин вођења евиденција тајних података;
- налаже мере за унапређење заштите тајних података;
- подноси кривичне пријаве;
- сарађује са органима јавне власти;
- обавља и друге послове који су предвишени овим законом и прописима донетим на основу овог закона.

Министар надлежан за правосуђе подноси, одбору Народне скупштине надлежном за надзор и контролу у области одбране и безбедности, годишњи извештај о активностима у спровођењу и контроли примене закона. У обављању надзора министарство врши контролу спровођења мера обезбеђења, коришћења, размене и других радњи обраде тајних података, без претходног обавештавања органа јавне власти, овлашћеног лица, руковооца, односно корисника тајног податка.

8.3. Канцеларија Савета за националну безбедност

Канцеларија Савета је стручна служба Владе са својством правног лица, у чијој су надлежности одређени послови спровођења и контроле примене овог закона и надзор над спровођењем Закона о тајности података.

У складу са овим законом, Канцеларија Савета:

- 1) „поступа по захтевима за издавање сертификата и дозвола;
- 2) обезбеђује примену стандарда и прописа у области заштите тајних података;
- 3) стара се о извршавању прихваћених међународних обавеза и закључених међународних споразума између Републике Србије и других држава, односно међународних органа и организација у области заштите тајних података и сарађује са одговарајућим органима страних држава и међународних организација;
- 4) израђује и води Централни регистар страних тајних података;
- 5) предлаже образац безбедносног упитника;
- 6) предлаже образац препоруке, сертификата и дозволе;
- 7) води евиденцију о издатим сертификатима, односно дозволама, као и евиденцију о одбијању издавања сертификата, односно дозвола;
- 8) организује обуку корисника тајних података у складу са стандардима и прописима;
- 9) предлаже Влади план заштите тајних података за ванредне и хитне случајеве;
- 10) опозива тајност податка у складу са одредбама овог закона;
- 11) после престанка органа јавне власти који немају правног следбеника, обавља послове који се односе на заштиту тајних података;
- 12) сарађује са органима јавне власти у спровођењу овог закона у оквиру своје надлежности;
- 13) обавља и друге послове који су предвиђени овим законом и прописима донетим на основу овог закона“ (Закон о тајности података, 2009).

9. СЛОБОДА ПРИСТУПА ИНФОРМАЦИЈАМА И ГЛОБАЛИЗАЦИЈА

Током последњих тридесетак година, следствено концепту социјалне државе и управе система за социјалну регулацију друштвених процеса и усвојеним међународним документима право на слободан приступ информацијама признато је у многим националним законодавствима широм света. Закони који су донети у последњих неколико година, углавном кореспондирају са принципима садржаним у документима Савета Европе, Европске уније, Уједињених нација и препорукама и принципима међународних невладиних организација.

И поред чињенице да је својеврсна „глобализација“ права на слободан приступ информацијама довела до стварања универзалних принципа у овој области, националне државе су оставиле могућност, да у зависности од сопствених унутрашњих специфичности, и у духу традиције националних правних система саме разрађују циљеве закона, круг органа јавне власти на које се односе обавезе пружања информација, круг титулара права на слободан приступ информацијама, садржину захтева и начин остваривања слободе приступа информацијама, моделе заштите и надзора над остваривањем овог права, трошкове неопходне за његово остваривање и друге детаље.

Упоредном анализом великог броја закона, већ у први мах постаје јасно да закони често истичу да остваривању права на слободан приступ информацијама, значајно доприноси развоју демократије и људских права али и да утиче на реформу државе и јавне управе, која у складу са савременим развојем подразумева отвореност, транспарентност, пропорционалност и непосредно и активно учешће грађана у друштвеним процесима. Само коришћење слободе приступа информацијама јесте „модел“ активног учешћа грађана у друштву, у коме је грађанин истовремено и „контролор“ јавног управљања на свим нивоима.

10. ПРАВО НА СЛОБОДАН ПРИСТУП ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА И ЗАШТИТА ТАЈНИХ ПОДАТАКА

„Слобода информација, уобичајно схваћена као право на слободан приступ информацијама у поседу органа јавне власти, данас је широко препозната као људско право“ (Mendel, 2003: 3). Ово право најчешће се дефинише и као „право свакога да од носиоца власти, односно јавних овлашћења, тражи и добије релевантне информације од јавног значаја како би се на делотворан начин омогућио увид у рад и поступање оних субјеката којима су грађани на слободним и демократским изборима поклонили поверење да у њихово име и за њихов рачун врше функцију власти и, у вези с тим, да управљају другим јавним пословима“ (Јелић, 2002). Простије речено, реч је о праву свакога(и физичког и правног лица) да се обавести о подацима којима располажу јавни органи као и други субјекти којима је поверено вршење јавних овлашћења. Слобода приступа информацијама према томе, управо обезбеђује директан надзор грађана над радом и понашањем оних, којима су сами грађани на демократским изборима поклонили поврење. Зато је ово право од великог значаја за превазилажење формалне и успостављање стварне демократије у њеном аутентичном значењу као владавине народа.

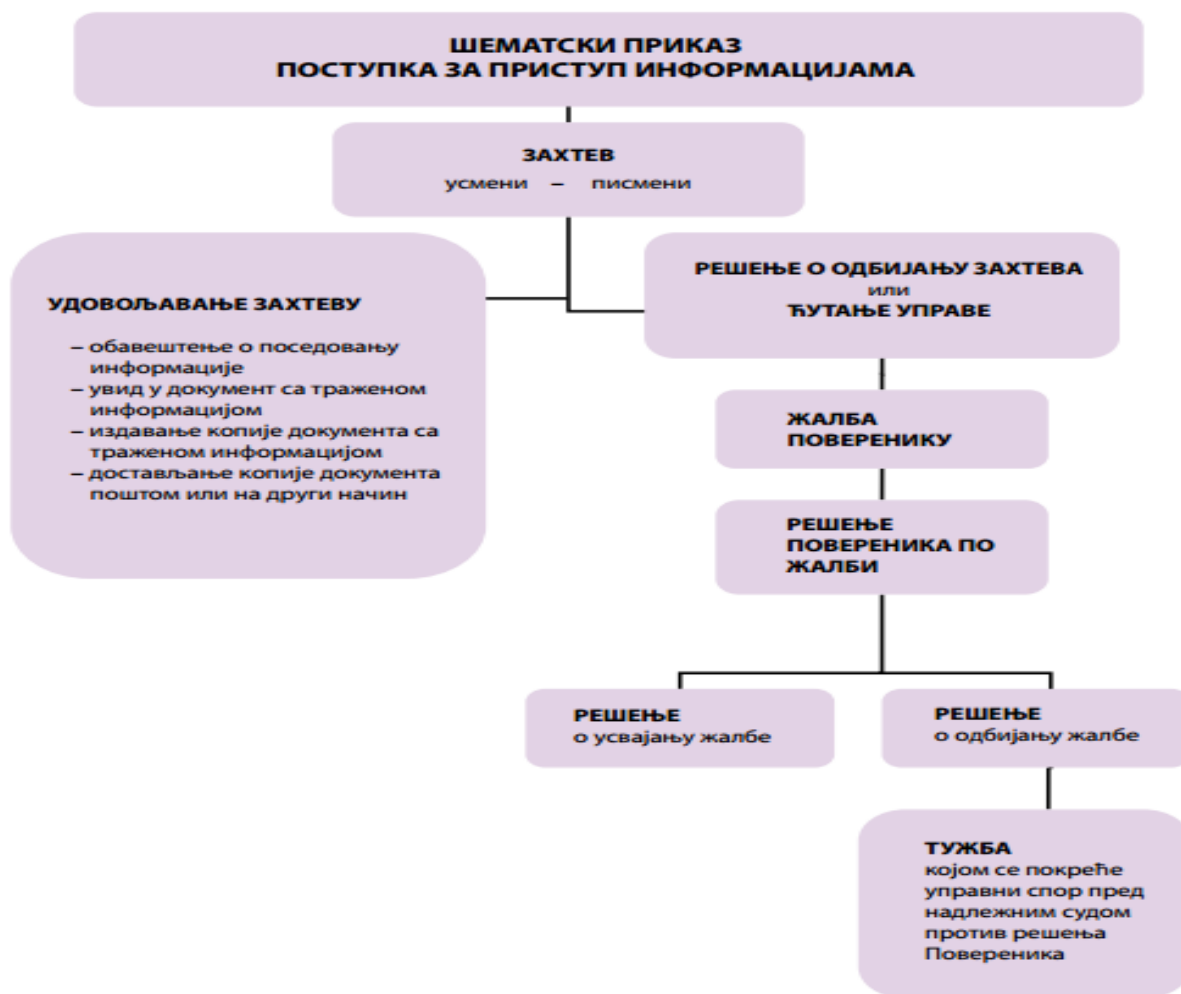
Две области које су нераскидиво повезане са слободом приступа информацијама су тајност информација и заштита података о личности. Злоупотребом тајности и личних података у појединим земљама, али и у Србији често се настоји одржати првобитни концепт правне државе и управе као власти, чиме се угрожавају и основни постулати демократског друштва, као и слободе приступа информацијама. Зато ове две области такође морају да буду системски уређене посебним законима који би били хармонизовани са међународним стандардима у овим областима али и стандардима садржаним у Закону о слободном приступу информацијама од јавног значаја.

Крајем октобра 2008. године, Скупштина Србије је усвојила Закон о заштити података о личности. Међутим, усвојени Закон садржи значајан недостатак, јер иако предвиђа проширење надлежности досадашње институције Повереника за информације и на област заштите података о личности, ограничења надлежности Повереника која су утврђена овим Законом, значајно умањује гаранције заштите података о личности као основног људског права и јачају култ тајности у односу на приступ личним подацима. То свакако није у складу са међународним стандардима, нарочито стандардима Европске уније у овој области.

С друге стране, Република Србија још увек нема Закон о класификацији информација. Уместо оваквог системског закона, данас преко 400 закона и подзаконских аката парцијално или кроз појединачне одредбе регулишу питање тајне. Доношењем једног оваквог закона којим се на целовит начин уређује систем обраде, коришћења, приступа, заштите и контроле тајних информација, односно разрадом наведених принципа и системских решења која су већ у великој мери установљена у међународном праву, Србија би се придружила породици европских и других народа који су овакве законе у прошлости већ донеле.

Питање које се поставља јесте да ли је актуелна власт заиста спремна да озбиљно хармонизује наведене три области или то чини само на декларативном нивоу.

Поступак за приступ информацијама од јавног значаја одвија се на следећи начин: (Миленковић, 2010: 172).



10.1.Ограничења слободе приступа информацијама

Слобода приступа информацијама није апсолутно право. Међутим, приступ информацијама треба да буде правило, а њихова поверљивост изузетак. Сви закони који регулишу остваривање права на приступ информацијама, утврђују својеврсне „листе“ изузетака од приступа. У неким земљама, законом су таксативно набројани сви разлози изузећа. У другим земљама, законодавац је имао потребу да опише шта се све подразумева као разлог изузећа у оквиру одређеног легитимног процеса, чиме су значајни делови закона и посвећени изузецима. Међутим, у упоредном праву углавном доминира принцип општег и растегљивог утврђивања претежних легитимних интереса, из којих се у конкретном случају изводе изузетци од приступа траженим информацијама. Ти легитимни интереси у већини законодавстава као и у препоруци Савета Европе јесу:

- 1) национална и јавна безбедност;
- 2) одбрана и међународни односи;
- 3) тајност у вези са вођењем одређених поступака;
- 4) приватност и заштита података о личности;
- 5) комерцијални и други економски интереси;
- 6) равноправност страна у судском поступку;
- 7) економска и монетарна политика државе;
- 8) поверљивост консултација унутар и између органа власти за време интерне припреме неког документа.

Поред тога, примену Закона о слободном приступу информацијама отежава околност да је овај закон први донет, а да је након њега током 2008. године, донет Закон о заштити података о личности, а тек на крају, током 2009. године, Закон о тајности података, који би заправо требао претходити овим законима и био „кровни“ или „темељни“ закон за примену Закона о слободном приступу информацијама.

10.2. Устав Републике Србије и право на слободан приступ информацијама

Доношењем Устава Републике Србије 2006, право на приступ информацијама постаје и Уставом загарантовано право грађана. Ранији Устав Републике Србије из 1990. године ово право није предвиђао. Право на слободан приступ информацијама, у новом Уставу постало је саставни део права на обавештеност.

Слобода приступа информацијама конзумирана је и изводи се већ кроз члан 46. Устава који јемчи слободу мишљења и изражавања. „Јемчи се слобода мишљења и изражавања, као и слобода да се говором, писањем, сликом или на други начин, траже, примају и шире обавештења и идеје“ (Устав Републике Србије, 2006). За разлику од, на пример, Европске конвенције за заштиту људских права и основних слобода, која под слободом изражавања не предвиђа тражење идеја и информација (што је и основ слободе приступа информацијама), Устав Србије је познаје.

Даље долазимо и до уставног права на обавештеност. Осврт на ово право проитиче из самог изражавања и коришћења обавештења у контексту речи информација. Где је у овом случају право на обавештеност заправо право на информацију. Односно право приступа информацијама. Ово је Уставом регулисано на следећи начин: „Свако има право да истинито, потпуно и благовремено буде обавештен о питањима од јавног значаја и средства јавног обавештавања су дужна да то право поштују. Свако има право на приступ подацима који су у поседу државних органа и организација којима су поверена јавна овлашћења у складу са законом“ (Устав Републике Србије, 2006).

10.3. Међународна сарадња у области заштите тајних података

Међудржавна сарадња у области заштите тајних података одвија се на више нивоа. На првом нивоу, у оквиру међународне мултилатералне сарадње везане за евроатланске интеграције држава западног Балкана, а посебно у оквиру НАТО и програма „Партнерство за мир“, Европске уније и Савета Европе. На другом нивоу, у оквиру различитих регионалних иницијатива везаних за сарадњу у области правосуђа, одбране, полиције и других области, уз напомену да још увек не постоје посебно разрађени регионални механизми сарадње у области размене и заштите тајних података. На трећем нивоу, у оквиру билатералне сарадње држава западног Балкана, кроз потписивање појединачних билатералних споразума и њихову имплементацију у правне системе сваке државе. Значајан помак био би формирање регионалног борда директора надлежних за заштиту и размену тајних података, који би у првој фази обухватао Словенију, Хрватску, БиХ, Србију, Црну Гору и Македонију и који би довео до повећања степена регионалне безбедности кроз повећање конкретних активности „на терену“.

Неке од међународних организација и држава са којим је закључен споразум о сарадњи у области размене и заштите тајних података:

Редни број	Држава	Година закључења
1.	НАТО	2011. година
2.	Европска унија	2011. година
3.	Словачка	2011. година
4.	Бугарска	2011. година
5.	Чешка	2013. година
6.	Словенија	2013. година
7.	Босна и Херцеговина	2013. година
8.	Македонија	2014. година
9.	Шпанија	2014. година
10.	Руска Федерација	2014. година
11.	Пољска	2015. година

Такође су покренути поступци за закључивање споразума са: Португалом, Немачком, Црном Гором, Румунијом, Турском и Мађарском.

10.3.1. Конвенција 205 Савета Европе о приступу службеним документима

Конвенција 205 Савета Европе о приступу службеним документима отворена је за потписивање на 29. Конференцији министара правде земаља чланица Савета Европе. Република Србија је ову Конвенцију потписала и активно учествовала у њеном доношењу.

Први део ове Конвенције садржи основне принципе права на приступ информацијама, који би требало да буду разрађени и садржани у актима држава које су је потписале и ратификовале.

Први принцип односи се на јасно дефинисање појмова попут "Јавна власт" и "службени документ". Под појмом јавне власти се подразумевају влада и јавна управа на националном, регионалном или локалном нивоу; законодавна тела и судска власт, уколико обављају административне функције у складу са националним законом; као и физичка и правна лица којима је поверено вршење управних јавних овлашћења. Такође државе могу укључити све оне елементе који су предвиђени националним законодавством.

Појам „службени документ“ означава све информације у било којем облику које су сачињене од стране органа јавне власти, или које је орган јавне власти примио и којима располаже.

Други принцип најпре одређује титулара права и утврђује да свако има право приступа службеним документима без дискриминације, а затим предвиђа и обавезу држава да у свом националном законодавству предузму све потребне мере како би спровеле одредбе ове Конвенције.

Трећи принцип односи се на изузетке од приступа, чиме и Конвенција ставља до знања да право на приступ информацијама није апсолутно право. Свака држава може ограничити право на приступ службеним документима, али та ограничења морају бити прецизно утврђена законом, неопходна у демократском друштву и сразмерна (пропорционална) циљу заштите: националне безбедности, одбране и међународних односа, јавне безбедности, превенције, истраге и гоњења криминалних активности, дисциплинске истраге, инспекције, контроле и надзора органа власти, приватности и других легитимних приватних интереса, комерцијалних и других економских интереса, економске, монетарне и девизне политике државе, равноправности страна у судском поступку, животне средине, и поверљивости консултација унутар или између органа власти за време интерне припреме неког документа. Приступ службеним документима може бити одбијен ако њихово објављивање угрожава или би могло да угрози наведене интересе, осим ако постоји претежнији јавни интерес за њихово откривање.

Четврти принцип односи се на подношење захтева органу јавне власти. Од тужиоца се не може захтевати да у захтеву образложи разлоге за приступ службеном документу. Тражилац не би требало да буде у обавези да у захтеву наведе разлоге због којих тражи приступ. Државе тражиоцу могу дати и могућност да остане анониман, осим када је идентитет од суштинске важности како би захтев био обрађен. Сам захтев мора да буде лишен непотребних формалности.

Пети принцип се састоји из низа правила која се односе на поступање органа јавне власти по захтеву. Тако, захтев за увид у службени документ требало би да разматра било који орган који у свом поседу има тај документ. Захтев за увид у службени документ требало би да буде разматран на равноправној основи. Ако се тражени службени документ не налази у поседу дотичног органа власти он би требало да, кад год је то могуће, упути подносиоца на надлежни орган. Орган власти требало би да помогне тражиоцу, у мери у којој је то могуће, да идентификује тражени службени документ. Сваки захтев за приступ службеном документу требало би да буде разматран хитно, а одлука да буде донета, саопштена и спроведена што пре, а најкасније у року који мора бити унапред одређен. Орган јавне власти може одбацити захтев, када је он нејасан или ако је очигледно неразуман.

Орган власти који у потпуности или делимично одбије увид у службени документ требало би да образложи то одбијање.

Шестим принципом утврђено је да би приступ информацијама требало да буде обезбеђен на начин који је најповољнији за тражиоца. Ако се ограничење односи на неку од информација из службеног документа, орган власти би ипак требало да дозволи увид у преостале информације које су у њему садржане. На свако изостављање делова документа требало би јасно скренути пажњу.

Седми принцип односи се на трошкове. Како би се сваком обезбедила могућност да оствари право на слободан приступ информацијама, трошкови увида у службени документ требало би да буду минимални. Преглед оригинала службених докумената на лицу места требало би да буде бесплатан. За копију службеног документа од подносиоца захтева може да се тражи надокнада која би требало да буде разумна и не би требало да премашује стварне трошкове органа.

Осми принцип односи се на делотворно правно средство и поступак у случају када је тражиоцу ускраћен приступ информацијама. Тражиоцу информације чији је захтев одбијен (делимично или потпуно), односно одбачен или није размотрен у утврђеном временском року, мора бити омогућен делотворан поступак преиспитивања такве одлуке пред судом или другим независним или непристрасним телом утврђеним законом.

Девети принцип односи се на допунске мере ради обезбеђења остваривања права на приступ информацијама. Ефикасно остваривање права на слободан приступ информацијама подразумева и предузимање допунских мера од стране државе, као на пример да се обавести јавност о њеном праву на приступ информацијама и о томе како се то право може остварити; да се обезбеди да државни службеници буду обучени када је реч о њиховим обавезама и дужностима како би омогућили подносиоцима захтева да остваре своје право, и др.

Последњим, *десетим принципом*, предвиђено је да би највећи део документа у поседу органа јавне власти требало да буде објављен и лако доступан грађанима. На овај начин промовише се транспарентност државне администрације и ефикасност унутар ње. Такође, на овај начин подстиче се информисано учешће јавности у питањима од јавног интереса. Циљ овог начела није да од органа власти тражи да обелодане све информације које су у њиховом поседу, већ их охрабрује да обелодањују оне информације које би омогућиле „обавештено“ учешће грађана у расправама од општег интереса.

11. КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

Уредбом о оснивању Канцеларије Савета за националну безбедност, иста је почела са радом 16. новембра 2009. године под називом Канцеларија Савета за националну безбедност. Ступањем на снагу Закона о тајности података, који се примењује од 01. јануара 2010. године, Канцеларија Савета за националну безбедност, променила је име у Канцеларија Савета за националну безбедност и заштиту тајних података. Канцеларија Савета основана је као служба Владе са својством правног лица.

Основне надлежности које Канцеларије Савета примењује у раду садржане су у :

- Устав Републике Србије;

Законски акти:

- Закон о Влади;
- Закон о основама уређења служби безбедности Републике Србије;
- Закон о тајности података;
- Закон о одбрани;
- Закон о Војсци Републике Србије;
- Закон о полицији;
- Закон о БИА;
- Закон о ВБА и ВОА;
- Закон о информационој безбедности;
- Закон о потврђивању Споразума између Владе Републике Србије и Организације северноатлантског пакта о безбедности информација и кодекса о поступању;
- Закон о државној управи;
- Закон о државним службеницима;
- Закон о платама државних службеника и намештеника;
- Закон о буџету;
- Закон о буџетском систему.

Подзаконски акти:

- Уредба о оснивању Канцеларије Савета за националну безбедност;
- Уредба о обрасцима безбедносних упитника;
- Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима;

- Уредба о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података Канцеларије Савета за националну безбедност и заштиту тајних података и Министарству правде;
- Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима;
- Уредба о начину и поступку означавања тајности података односно документа;
- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима;
- Уредба о посебним мерама надзора за поступање над тајним подацима;
- Уредба о посебним мерама физичко техничке заштите тајних података.

Директор Канцеларије Савета дужан је да Влади Републике Србије поднесе годишњи извештај о активностима у оквиру надлежности Канцеларије Савета. Канцеларија Савета је обавезна да се у обављању послова из свог делокруга придржава начелних ставова и смерница Владе који се односе на безбедносну политику Републике Србије.

Канцеларија Савета преузима тајне податке органа јавне власти који су престали да постоје, а немају правног следбеника, односно задужује други орган јавне власти за чување и коришћење тих података.

Размена тајних података са страним државама и међународним организацијама врши се преко Канцеларије Савета, односно Централног регистра страних тајних података, осим ако законом или закљученим међународним споразумом није другачије одређено.

11.1.Организациона структура канцеларије

Радам Канцеларије Савета руководи директор кога поставља и разрешава Влада, по прибављеном мишљењу Савета за националну безбедност. За обављање послова из надлежности Канцеларије Савета образоване су унутрашње јединице.

Директор Канцеларије Савета је државни службеник на положају који за свој рад одговара Влади и председнику Владе и поставља га Влада на пет година на основу Закона о тајности података, а на предлог председника Владе. Директор Канцеларије Савета доноси акт о унуташњој организацији и систематизацији радних места на који сагласност даје Влада по прибављеном мишљењу Савета за националну безбедност.

На радне односе директора Канцеларије Савета, заменика директора и запослене у Канцеларији Савета на пословима заштите тајних података примењују се прописи који се односе на радне односе државних службеника и намештеника.

Организациона шема Канцеларије Савета за националну безбедност и заштиту тајних података:¹



¹ Информатор о раду Канцеларије Савета за националну безбедност и заштиту тајних података.

12. ПРАВНИ ОКВИР ПРИМЕНЕ ПОСТУПАКА ИМЕРА ЗА ТАЈНО ПРИКУПЉАЊЕ ПОДАТАКА

Правни оквир примене посебних поступака и мера за тајно прикупљање података своје почетке налази у 2002. години, да би се непрестаним унапређивањем, добио одлике јединственог и развијеног правног оквира. Актери који су Влади и праламетну највише помогли у изради истог јесу Заштитник грађана, Повереник за информације од јавног значаја и заштиту података о личности и Уставни суд Србије. Поред њих велику улогу имали су и невладине организације и стручна јавност која се бави проблематиком заштите људских права.

Законом о кривичном поступку из 2001. године, била је уведена само једна мера за тајно прикупљање података- мера надзора и снимања телефонских и других разговора или комуникације и оптичко снимање. У веома кратком временском раздобљу она је допуњена 2002. године у три закона: Закон о изменама и допунама; Закона о кривичном поступку; Закон о службама безбедности Савезне Републике Југославије и Закону о Безбедносно-информативној агенцији. То уређење претрпело је бројне промене, да би данашњи правни оквир своје финално обличје добио у Законику о кривичном поступку из 2011 године.

Позитивноправни оквир, непосредно значајан за примену посебних поступака и мера за тајно прикупљање података чине следећи извори:

- 1) одговарајуће одредбе Устава, Европске конвенције о људским правима и других међународних докумената који обавезују Републику Србију;
- 2) Закон о основама уређења служби безбедности Републике Србије, Закон о БИА и Закон о ВБА и ВОА;
- 3) Закон о полицији и Законик о кривичном поступку.

12.1. Законска терминологија

Посебни поступци и мере тајног прикупљања података, како наводи Катарина Ђокић „нису никаква новина у раду безбедносних актера, али у последњих неколико година привлаче велику пажњу јавности“ (Ђокић, 2014: 6). Уређени су седмој глави Законика о кривичном поступку у оквиру дела који се зове тајности "Посебне доказне радње". Разликују се у већој мери од општих, зато што код њих у већој мери посеже у људска права.

Док их је Закон о полицији означио као "мере потраге применом специјалне истражне технике утврђене законом којим се уређује кривични поступак", односно "мере

циљане потраге"(Закон о полицији, 2005). У Закону о основама уређења служби безбедности Републике Србије користи се термин "посебни поступци и мере за тајно прикупљање података"(Закон о основама уређења служби безбедности, 2007). Закон о Безбедносно-информативној агенцији дефинише их као "посебне мере којима се одступа од неповредивости тајне писама и других средстава опшетња"(Закон о Безбедносно – информативној агенцији, 2014).

Оно због чега примена посебних поступака и мера изазива пажњу јесте чињеница да се њиховом применом индивидуална права и слободе ограничавају. Ова идеја је неспојива са савременим концептом демократије, али с друге стране њена примена у великој мери може спречити развој тероризма, организованог криминала и других облика угрожавања јавне и националне безбедности. Тајност посебних поступака и мера је оно што их разликује од других поступака који примењују органи кривичног гоњења. У било ком случају ови поступци сматрају се легитимним уколико се одвијају у законски дефинисаним оквирима, а како би се очували јавни ред и поредак који је предуслов за уважавање права појединаца.

Узимајући у обзир наведено, посебне поступке и мере можемо дефинисати као „специјална овлашћења безбедносних органа и органа кривичног гоњења за тајно прикупљање података, којима се изузетно, на одређено време и без сазнања грађана, а на основу одлуке суда и под законски прописаним условима, одступа од уставом зајамчених индивидуалних права“(Милосављевић, 2015: 11).

Према сврси прикупљања података, ове мере и поступци могу се класификовати на оне:

- 1) „којима је циљ вођење кривичног поступка;
- 2) којима је циљ превентивно деловање ради заштите националне безбедности и који се примењују на основу закона о службама безбедности“(Милосављевић, 2012: 59).

12.2. Посебне доказне радње

Законик о кривичном поступку утврдио је шест посебних доказних радњи:

- „тајни надзор комуникације;
- тајно праћење и снимање;
- коришћење симулованих послова;
- рачунарско претраживање података;
- примењивање контролисане испоруке;

- ангажовање прикривеног иследника“(Законик о кривичном поступку, 2011).

Тајни надзор састоји се у праћењу и снимању комуникације која се обавља телефоном, надзор, електронске и друге адресе осумњиченог и заплене писама и пошиљки. Њену примену одобрава судија на образложени предлог јавног тужиоца. Трајање надзора временски је ограничено на три месеца, али може бити продужено за још толико. У ратним условима или у случају организованог криминала надзор је могуће продужити још два пута у истом трајању. Престаје у тренутку када нестану разлози за његову примену. У спровођењу надзора ангажовани су полиција, БИА и ВБА, а о извршеном надзору сачињавају дневни извештај који се доставља судији и јавном тужиоцу на њихов захтев. Орган који спровори мере тајног надзора у току њиховог трајања, може проширити надзор и на друге адресе и видове комуникације.

Тако је Милосављевић, мере за *Тајно праћење и снимање* које односи на осумњиченог, поделио на оне за:

- „откривања контаката или комуникације осумњиченог на јавним местима и местима на којима је приступ ограничен или у просторијама, осим у стану;
- утврђивања истоветности лица или лоцирање лица или ствари“(Милосављевић, 2012: 14).

Оно што може бити предмет тајног надзора и снимања јесу места и просторије, превозна средства само ако је вероватно да ће се осумњичени ту појавити или користити та превозна средства. Примену ове радње такође одобрава судија на претходни захтев јавног тужиоца.

Прислушкивање, тајно праћење, фотодокументовање, снимање разговора спада у ред класичних и веома распрострањених мера које користе полиција и службе безбедности. С обзиром на савремено схватање људских права, примена ових мера је знатно ограничена.

Симуловани послови односе се на симуловану куповину, продају или пружање пословних улога, као и на симуловано давање и примање мита. Једна од карактеристика ове радње лежи у томе да приликом њеног спровођења, друго лице не сме бити навођено да изврши кривично дело.

Рачунарско претраживање података односи се на оне податке који су већ обрађени и који се пореде са онима који већ постоје о осумњиченом и кривичном делу.

Контрлисан испорука примењује се у циљу прикупљања података о личности и откривање осумњичених, а њоме се дозвољава да нелегалне и сумњиве пошиљке буду испоручене како на територији Републике Србије, тако и ван ње. Контрлисану испоруку спроводи полиција или други надлежни органи које именује јавни тужилац. Уколико та пошиљка напушта територију Републике Србије, онда се испорука спроводи у садејству са надлежним органима заинтересованих држава.

Прикривени иследник користи се у случају да прикупљање података неком од претходим доказних радњи није довело до жељених сазнања. Приликом ангажовања прикривеног иследника, неопходно је доставити податке који садрже детаљан опис циљних група, трајања и места операције, као и средстава која ће се користити.

Прикривеног иследника ангажује министар унутрашњих послова, директор БИА или директор ВБА или лице које они овласте, а трајање ангажовања ограничено је на годину дана уз могућност продужења на још шест месеци. Прикривени иследник одређује се шифром или псеудонимом, а када то захтевају услови, могуће је издати исправе са измењеним подацима.

13. КАЗНЕНЕ ОДРЕДБЕ

13.1. Кривично дело

У Закону о тајности података казнене одредбе обухватају кривично дело и два прекршаја: Ко неовлашћено непозваном лицу саопшти, преда или учини доступним податке или документа који су му поверени или до којих је на други начин дошао или прибавља податке или документа, а који представљају тајне податке са ознаком тајности "ИНТЕРНО" или "ПОВЕРЉИВО", одређене према овом закону, казниће се затвором од три месеца до три године.

Ако је дело из става 1. овог члана учињено у односу на податке означене, у складу са овим законом, степеном тајности "СТРОГО ПОВЕРЉИВО", казниће се затвором од шест месеци до пет година.

Ако је дело из става 1. овог члана учињено у односу на податке означене, у складу са овим законом, степеном тајности "ДРЖАВНА ТАЈНА", учинилац ће се казнити затвором од једне до десет година.

Ако је дело из ст. 1. до 3. овог члана учињено из користољубља или ради објављивања или коришћења тајних података у иностранству или је извршено за време ратног или ванредног стања, учинилац ће се казнити за дело из става 1. овог члана затвором од шест месеци до пет година, за дело из става 2. затвором од једне до осам година, а за дело из става 3. затвором од пет до петнаест година.

Ако је дело из ст. 1. до 3. овог члана учињено из нехата, учинилац ће се казнити за дело из става 1. овог члана затвором до две године, за дело из става 2. затвором од три месеца до три године, а за дело из става 3. затвором од шест месеци до пет година.

У судској пракси још није забележен ни један случај примене кривичног дела или прекршаја на основу Закона о тајности података, јер још увек нису донете одговарајуће уредбе које би у целости омогућиле примену овог дела закона.

13.2. Прекршајна одговорност одговорног лица у органу јавне власти

Новчаном казном у износу од 5.000 до 50.000 динара казниће се за прекршај одговорно лице у органу јавне власти ако:

- 1) податак и документ који се очигледно не односе на заштићене интересе, означи као тајне;
- 2) овлашћење за одређивање тајности података пренесе на треће лице;
- 3) означи тајне податке садржане у документу неодговарајућим степеном тајности;
- 4) донесе одлуку о одређивању тајности податка без образложења;
- 5) не опозове тајност податка после наступања датума или догађаја после кога престаје тајност податка;
- 6) не опозове тајност податка после истека законског рока за престанак тајности податка;
- 7) не спроведе периодичну процену тајности податка;
- 8) не опозове тајност податка на основу решења Повереника за информације од јавног значаја и заштиту података о личности или одлуке надлежног суда;
- 9) промени степен тајности документа супротно одредби члана 27. овог закона;
- 10) пропусти да органе јавне власти обавести о промени степена тајности и опозиву тајности;
- 11) не пропише, организује и надзире опште и посебне мере заштите тајних података који одговарају степену њихове тајности;
- 12) лицу коме је издат сертификат за приступ тајним подацима не да на потписивање изјаву о томе да је упознато са прописима који уређују заштиту тајних података;
- 13) тајне податке достави правним и физичким лицима супротно одредби члана 46. овог закона;
- 14) не води евиденцију решења о сертификату за приступ тајним подацима;
- 15) решење за приступ тајним подацима не чува у посебном делу кадровског досијеа;
- 16) не организује унутрашњу контролу над заштитом тајних података;
- 17) не предузме мере да се образује, води и обезбеђује посебан регистар страних тајних података.

Прекршајна одговорност руковоаца тајних података из члана 100. Закона о тајности података:

- 1) Новчаном казном у износу од 5.000 до 50.000 динара казниће се за прекршај руковалац тајних података који не предузима мере заштите тајних података.

14. ОБАВЕЗЕ КОЈЕ ПРОИЗИЛАЗЕ ИЗ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА

Закон о тајности података унео је у правни систем Републике Србије један нов систематски приступ утемељен на безбедносним, правним и техничким стандардима који се примењују у Европској унији, НАТО, али и земљама у окружењу које су га имплементирале у своје правне системе. Сам Закон о тајности података је наметнуо одређене обавезе органима јавне власти које се огледају у следећем:

- 1) израда подзаконске регулативе о одређивању критеријума за степен тајности ИНТЕРНО и ПОВЕРЉИВО;
- 2) израда подзаконске регулативе која се односи на поједине посебне мере заштите;
- 3) усаглашавање прописа са Законом о тајности података који се односе на рад са тајним подацима (канцеларијско пословање и слично);
- 4) измене међународних споразума који подразумевају размену тајних података и формирање посебних регистара за те намене;
- 5) измене аката о унутрашњој организацији и систематизацији или формацији, увећањем степена тајности коме лице има присуп у обављању својих послова;
- 6) израда аката о преносу тајних података, примени општих и посебних мера и слично;
- 7) одређивање руковођа тајних података у органу јавне власти и формирање регистарског система за рад са тајним подацима Републике Србије;
- 8) организовање система перманентне едукације из области заштите тајних података;
- 9) вођење слижбених евиденција у складу са Законом о тајности података;
- 10) успостављање непосредне сарадње и комуникације са Канцеларијом Савета за националну безбедност и заштиту тајних података;
- 11) унутрашње регулативе о информатичкој сигурности/безбедности.

ЗАКЉУЧАК

Демократизација друштва у савременим условима нарочито се односи на државе у транзицији и она мора да буде заснована на принципима правне и социјалне државе, транспарентности и отвореног друштва, што подразумева реафирмацију јавне сфере.

„Пут од хиљаду миља почиње првим кораком.“ Република Србија чини велике напоре да на законодавном пољу среди област креирања и обраде тајних података, при томе реформишући и сектор безбедности(и одбране) у целости. Први корак је учињен доношењем Закона о тајности података, а следећи би требао бити посвећен доношењу законског текста о информатичкој сигурности или безбедности. Након тога следи подзаконско уређење ове области, са којим се касни због сложености и комплексности ове материје, као и његова практична примена, а вероватно и одговарајуће измене законских текстова у складу са праксом и међународним стандардима. Сама имплементација Закона о тајности података омогућава успостављање сарадње на највишем нивоу између система одбране Републике Србије и НАТО, Европске уније, али и на билатералном нивоу, омогућавајући припадницима Министарства одбране и Војске Србије(али и других државних органа и правним лицима) учешће у различитим међународним активностима које подразумевају приступ одређеним тајним подацима.

У савременој пракси (и теорији у Србији), за потребе обављања заштите тајних података поред контраобавештајне заштите, приступи су и следећи садржаји: 1) физичко обезбеђење; 2) техничко обезбеђење; 3) заштитни режим формацијски места и безбедносне провере; 4) заштита од пожара и експлозија; 5) заштита од елементарних непогода; 6) заштита у ванредним околностима; 7) заштита у склопу боравка странаца; 8) заштита информационих и телекомуникационих система; 9) процедуре стварања и утврђивања нивоа заштите тајних података; 10) преношење тајних података; 11) чување, складиштење и употреба тајних података; 12) уништавање тајних података; 13) конторла спровођења мера. Поред тога, потребно је указати да од примене ово закона није изузет ни један орган државне власти, ни правно лице, које рукује тајним подацима, односно да у његовој практичној примени нема изузетака.

Поред тога, један од циљева закона је и омогућавање транспарентности рада свих државних органа када су у питању различите области њиховог деловања, кроз значајније смањивање примене дискреционих права, приликом обраде било које врсте података.

На крају треба напоменути, да проблематика која се односи на архивирану грађу државних органа са ознаком тајности, као ни питање отварања тзв. „тајних досијеа“ није у надлежности овог закона, који би требао да уреди рад само са тајним подацима који се креирају од момента његовог доношења.

ЛИТЕРАТУРА

1. Грубор, Г., и Милосављевић, М. (2012). *Основе заштите информација, методолошко-техничке основе*. Београд.
2. Ђокић, К., (2014). *Парламенти на специјалном задатку: надзор над применом посебних мера за тајно прикупљање података*. Београд: Београдски центар за безбедносну политику.
3. *Закон о заштити података о личности*. (2008). Службени гласник РС, бр. 97/2008.
4. *Закон о тајности података*. (2009). Службени гласник РС, бр. 104/2009.
5. *Закон о полицији*. (2005). Службени гласник РС, бр. 101/05.
6. *Закон о основама уређења служби безбедности Републике Србије*. (2007).
7. *Законик о кривичном поступку*. (2011). Службени гласник РС, бр. 72/11.
8. *Закон о Безбедносно-информативној агенцији*. (2014). Службени гласник РС, бр. 65/14.
9. Јелић, З., (2002). *У сусрет законском регулисању слободног приступа информацијама*. Београд: Економика.
10. Јовичић, И., (2008). *Српска правна ревија – Правна реформа безбедносних служби*. Београд: Правни форум.
11. Матић, Г. (2012). *Систем заштите тајних података*. Београд: Организација за европску безбедност и сарадњу, Мисија ОЕБС у Србији: Канцеларија Савета за националну безбедност и заштиту тајних података.
12. Миленковић, Д., (2003). *Слободан приступ информацијама као фундаментално људско право*. Београд: Комитет правника за људска права.
13. Миленковић, Д., (2010) *Приручника за примену закона о слободном приступу информацијама од јавног значаја*. Београд.
14. Милосављевић, Б., (2012). *Правни оквир и пракса примене посебних поступака и мера за тајно прикупљање података у Републици Србији*. Београд.
15. Mendel, T., (2003). *Freedom of information(a comparative legal survey)*. New Delhi.
16. Радојковић, М., (2002). *За слободан приступ информацијама*. Београд: Призма – Центар за либерално – демократске студије.
17. Службени гласник РС, бр. 116/07.
18. Стајић, Јб. (2011). *Основи система безбедности*. Нови Сад: Правни факултет.
19. *Training manual for public officials - Freedom of information*. (2004). Лондон.
20. *Устав Републике Србије*. (2006).