

*Радојица С. Лазућ*

*Академија за националну безбедност, Београд*

## **ЗАШТИТА ТАЈНОСТИ ПОДАТАКА – ОД ПРАВНОГ ОСНОВА ДО ПРАКТИЧНЕ ПРИМЕНЕ**

### **Сажетак**

У сваком друштву, било оно демократско или не, постоје одређени подаци, који нису доступни јавности. Они су изузети од могућности остваривања увида грађана у њихове садржаје и као такви проглашени су тајним. Током развоја људског друштва тајни подаци, политичке, економске, безбедносне и друге природе, били су моћно средство у рукама власти. Тачна и поуздана информација и податак су одувек били од посебног значаја за постизање жељених циљева. Циљ рада је критичка анализа проблема заштите тајности података од правног основа па све до практичне стране овог веома сложеног проблема.

Доношењем новог Закона о тајности података на јединствен начин устројена је ова област у Републици Србији. Иако је имплементација наведеног закона текла веома споро, јер су одређена решења тешко примењива у пракси, ипак, он представља веома значајни помак у овој области. Дакле, у овом раду су анализирани правни прописи, процедуре за остваривање приступа тајним подацима (сертификација), које су успостављене тим законом, као и у којој мери се, до сада, његова примена остварила у пракси.

Кључне речи: тајни податак, заштита података, сертификација, размена података, Канцеларија Савета, службе безбедности

## 1. УВОД

Савремено друштво, према Урлиху Беку, представља *друштво ризика* које он дефинише „као друштво науке, комуникационих и информационих средстава, сложених конгломерата група и моћи наспрам природе и између људи.“<sup>1)</sup> Од самог настанка људског друштва човек је настојао да одређене врсте важних информација, до којих је дошао на најразличитије начине, сачува од других лица и друштвених група. Да би их сачувао и обезбедио себи примат, било у политичкој, војној, економској или некој другој сфери, морао је да устроји одређену методологију и правила, како у прикупљању, исто тако и у чувању таквих података. У том смислу развијале су се и одговарајуће процедуре у обезбеђивању заштите свих врста прикупљених података. Свакако треба нагласити да слободан приступ информацијама представља једно од веома значајних права грађана и основ демократског друштва.<sup>2)</sup> Наравно са друге стране приватност и заштита података представљају једно од основних вредности грађана у демократском друштву, што је признато Европском конвенцијом о људским правима и Универзалном декларацијом о људским правима.<sup>3)</sup>

Како бисмо разумели значење термина „податак“ и „тајни податак“ потребно је, најпре, појаснити шта ти појмови представљају, као и на који начин неко одлучује који податак потпада под режим заштите.

Постоји мноштво тумачења везаних за значење ових термина. Тако за Обрена Ђорђевића „податак је назив за скуп међусобно повезаних делатности које сачињавају јединствену целину“,<sup>4)</sup> а тајни подаци „представљају посебне вредности датог друштва“, чија заштита је „одређена законом или наредбом надлежног државног органа“.<sup>5)</sup> Према истом аутору, одговорни субјекти за њи-

---

1) Миша Стојадиновић, Виолета Рашковић Таловић, „Изазови развоја демократије у савременом друштву: политичко насиље и теорија (не)праведног рата“, *Српска политичка мисао*, vol. 51, бр. 1, Институт за политичке студије, Београд, 2016, стр. 49-64.

2) Дејан Миленковић Војин Ракић, *Слободна приступ информацијама и јавна управа*, Комитет правника за људска права, Београд, 2005.

3) Опширније о овоме видети: George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoerhman, Daniel Le Métayer, Rodica Tîrtea, Stefan Schiffner, *Privacy and Data Protection by Design – from policy to engineering*, December 2014, European Union Agency for Network and Information Security (ENISA), 2014.

4) Више о томе видети: Обрен Ђорђевић, *Лексикон безбедности*, Партизанска књига, Београд, 1986, стр. 280.

5) Исто, стр. 378.

хову заштиту предузимају потребне мере да их непријатељ или непозвана лица не сазнају. То су, углавном, подаци политичке, војне и економске врсте, а који су значајни за одбрану, безбедност и привреду земље.<sup>6)</sup>

За Мила Бошковића податак представља чињеницу или обавештење на основу којих се о нечему може закључивати или одлучивати,<sup>7)</sup> док тајни подаци (који могу бити политичке, војне, економске или безбедносне природе) представљају чињенице чије би одавање или изношење у јавност могло проузроковати штету у одређеној области, пословном субјекту, организацији, органу или држави. Исти аутор наглашава да се критеријуми о тајности, заштити и чувању података утврђују законима, интерним и другим прописима у складу са законом, а да се неовлашћено одавање квалификује као кривично дело.<sup>8)</sup> Свакако треба обратити пажњу и на улогу медија у овоме јер они представљају главни извор информација грађана.<sup>9)</sup>

За нас је најрелевантније значење садржано у Закону о тајности података.<sup>10)</sup> На основу поменутог закона „податак од интереса за Републику Србију је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и сувереност, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове“.<sup>11)</sup> Према одредбама истог закона „тајни податак је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности“.<sup>12)</sup>

У смислу овог закона, тајним податком не сматра се податак који је означен као тајна ради прикривања кривичног дела, преко-

---

6) Исто, стр. 378.

7) Више о томе видети: Мило Бошковић, *Криминолошки лексикон*, Матица српска, Нови Сад, 2015, стр. 370.

8) Исто, стр. 512.

9) Миша Стојадиновић, „Значај медија за развој културе мира“, *Медији и култура мира на Балкану* (приредили: Бранислав Стевановић, Александра Костић, Љубиша Митровић), Филозофски факултет – Универзитет у Нишу, Центар за социолошка истраживања, Ниш, 2010, стр. 371-384.

10) Закон о тајности података Народна скупштина Републике Србије усвојила је 11. децембра 2009. године. Објављен је у *Службеном гласнику РС*, бр. 104/09. а почео је да се примењује од 1. јануара 2010. године.

11) Види: члан 2. тачка 1. Закона о тајности података, *Службени гласник РС*, бр. 104/09.

12) Види: члан 2. тачка 2. истог закона.

рачења овлашћења или злоупотребе службеног положаја или другог незаконитог акта или поступања органа јавне власти.

Када се говори о њиховој тајности и заштити од непожељних корисника, треба рећи да није сваки податак који ствара одређена институција такве важности да мора бити заштићен. Из тих разлога ова материја се уређује посебним законима. И поред тога, сведоци смо да и најважнији и строго чувани подаци, понекад и на волшебан начин, процуре у јавност. Најразличитија истраживања спроведена у овој области показала су да највећи број података, који представљају било који облик тајности, произведен је у државним институцијама, укључујући ту и сектор безбедности.

Службе безбедности у Републици Србији и пре усвајања и почетка спровођења овог закона, поштујући раније донешене правне прописе, имале су посебан режим у стварању и чувању података и информација у своме поседу. „Свака држава својим законским прописима јамчи заштиту одређених података или одређених сазнања о нечему. Сватко је дужан чувати било коју од ових тајни и то без обзира на начин сазнања тајних података или стјеццања могућности увида у тајне податке.“<sup>13)</sup>

Применом новог Закона о тајности података поменути режим прилагођен је и устројен са актуелним правним нормама.<sup>14)</sup>

## 2. ЗНАЧАЈ НОВОГ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА

Одређивање и заштита тајности података, начин поступања са тајним подацима и посебне заштитне мере чувања, су питања која све до краја 2009. године у Србији нису била уређена једним законом који успоставља основне принципе правног уређења у овој области. Одредбе, које се тичу тајности података, биле су садржане у више закона којима су регулисане различите области, од Закона о одбрани, преко закона који регулишу рад служби безбедности, закона којим су регулисане активности Министарства спољних послова, све до Закона о полицији, као основног закона у области унутрашњих послова.

13) Бранко Перан, Мирко Горета, Кристина Вуковишић, „Појам и врсте тајни“, *Зборник радова Велеучилишта у Загребу*, бр. 3-4/2015.

14) Више о томе види: члан 11. Закона о безбедносно-информативној агенцији, *Службени гласник РС*, бр. 42/02, 111/09, 65/14 – Одлука УС и 66/14; члан 31. и 32. Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији, *Службени гласник РС*, бр. 88/09, 55/12 – Одлука УС и 17/13; *Информатор о раду БИА – ажуриран 4. јануара 2017. године*, стр. 44–45, Internet, <http://www.bia.gov.rs/download/dokumenta/Informator.pdf>, 02/03/2017; Радојица Лазих, *Контрола служби безбедности*, Академија за националну безбедност, ЈП *Службени гласник*, Београд, 2014, стр. 65–66.

Мрежу прописа којима су регулисана нека питања која се тичу тајности података, поред ових закона, чине и бројни подзаконски акти – правилници, уредбе, инструкције и упутства. Сви ти прописи, углавном, нису међусобно били усклађени, тако да се из њих врло тешко, или готово немогуће, могло закључити, на којим правним принципима се заснивала цела ова област.<sup>15)</sup>

Такав правни недостатак натерао је законодавца да систем одређивања и заштите тајности података уреди једним законом, којим су установљени основни принципи за проглашавање докумената тајним, за класификацију, поступање, чување, али и надзор над спровођењем свих законом уређених мера.

У складу са позитивним правним прописима коју уређују ову област Законом о тајности података, као и подзаконским актима и прописима, државне институције у обавези су да примењују опште и посебне, нормативне, физичко-техничке и логистичке, појединачне и комбиноване, мере заштите података, који су у поседу институције, без обзира на облик и начин вођења тих података. Ове мере, поред осталог, обухватају следеће: одређивање руковоца подацима; одређивање посебних зона зграда и просторија намењених заштити података; мере физичко-техничке заштите, укључујући и уградњу техничких средстава заштите; утврђивање безбедносне зоне и заштиту ван безбедносне зоне; посебне мере заштите које се примењују приликом транспорта документације, а које се предузимају ради спречавања губљења, крађе или уништења.

Нормативне мере заштите, које се примењују на основу Закона о тајности података, обухватају поред организационих и кадровске ресурсе. На основу тих мера подацима могу приступити само лица која поседују одговарајућа овлашћења. Уколико се ради о подацима који поседују одређени степен тајности, лице мора имати лиценцу, односно сертификат за приступ тој врсти тајних података, што подразумева и одговарајућу безбедносну проверу и потписану изјаву о обавези чувања тајности података. Физичко-техничке мере заштите података обухватају техничку заштиту објеката и просторија, уз примену свих средстава заштите (електронска, механичка, противпожарна и сл.).

За спровођење Закона о тајности података било је потребно испунити читав низ предуслова, што захтева не само одређено време и усклађивање других прописа, већ и успостављање неких органа без чијег ефективног деловања није било могуће спроводити такав закон. Поред тога, било је потребно радити и на изградњи

15) Ђорђе Поповић, „Коментар закона о тајности“, *Безбедност Западног Балкана*, октобар – децембар 2009, стр. 4-5.

капацитета државних органа који су значајни за спровођење и контролу у поступку примене Закона о тајности података.<sup>16)</sup>

У том смислу, веома значајна улога, која је садржана у Закону о тајности података, одређена је Канцеларији Савета за националну безбедност, којој је усвајањем поменутог закона придодата и обавеза да се стара о заштити тајних података.

Канцеларија Савета за националну безбедност и заштиту тајних података (у даљем тексту: Канцеларија Савета)<sup>17)</sup> 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.

Влада поставља и разрешава директора и заменика директора Канцеларије Савета, по прибављеном мишљењу Савета за националну безбедност, са мандатом на пет година.<sup>18)</sup> Директор Канцеларије Савета подноси Влади Годишњи извештај о активностима у оквиру надлежности Канцеларије Савета. Размена тајних података са страним државама и међународним организацијама врши се преко Канцеларије Савета, осим ако посебним законом или закљученим међународним споразумом није друкчије одређено.

Извештај који садржи бројчане показатеље о размени тајних података са страном државом или међународном организацијом, орган јавне власти доставља Канцеларији Савета најмање једном

16) У Годишњем извештају Канцеларије Савета за националну безбедност и заштиту тајних података за 2014. годину истиче се да је Безбедносно-информативна агенција током 2014. године готово у потпуности имплементирала одредбе Закона о тајности података и била први орган јавне власти у Републици Србији који је прешао на нов систем одређивања и заштите тајних података. На плану заокруживања нормативног оквира из ове области, Агенција је: донела Одлуку о одређивању тајних података Безбедносно-информативне агенције, са листама тајних података Агенције, одредила лица овлашћена за одређивање тајних података у Агенцији и прописала радна места на којима припадници Агенције имају приступ тајним подацима у складу са принципом „Потребно да зна“. Исти извор наводи, да је у извештајном периоду, Агенција је са страним партнерима разменила укупно 1183 информације које су третирали тероризам, транснационални организовани криминал и недозвољену пролиферацију оружја, војну опрему и робе двоструке намене; *Zakon o tajnosti podataka. Analiza Centra za evroatlantske studije*, Internet, [https://www.ceas-serbia.org/images/2015-i-pre/CEAS\\_analiza\\_-\\_Zakon\\_o\\_tajnosti\\_podataka\\_maj\\_2015.pdf](https://www.ceas-serbia.org/images/2015-i-pre/CEAS_analiza_-_Zakon_o_tajnosti_podataka_maj_2015.pdf), 02/03/2017.

17) Канцеларија Савета за националну безбедност образована је у складу са чланом 8. Закона о основама уређења служби безбедности Републике Србије, *Службени гласник РС*, бр. 116/07 и 72/12, а на основу Уредбе Владе Републике Србије о оснивању Канцеларије Савета за националну безбедност од 6. фебруара 2009. године, *Службени гласник РС*, бр. 12/09. Даном ступања на снагу Закона о тајности података наставаља са радом под називом Канцеларија Савета за националну безбедност и заштиту тајних података.

18) Види: члан 3. и 4. Уредбе о оснивању Канцеларије Савета за националну безбедност.

годишње. Канцеларија Савета обавештава страну државу, односно међународну организацију о безбедности страних тајних података добијених у међународној размени. Канцеларија Савета прима обавештења од стране државе, односно међународне организације о безбедности тајних података које је Република Србија предала у међународној размени.

### 3. СТЕПЕН И РОКОВИ ТАЈНОСТИ ПОДАТАКА

Одредбама Закона о тајности података дефинисана су четири степена тајности докумената.<sup>19)</sup> То су:

„ДРЖАВНА ТАЈНА“ – са роком тајности од 30 година;

„СТРОГО ПОВЕРЉИВО“ – са роком тајности од 15 година;

„ПОВЕРЉИВО“ – са роком тајности од 5 година;

„ИНТЕРНО“ – са роком тајности од 2 године.

Уредбом о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА“ и „СТРОГО ПОВЕРЉИВО“<sup>20)</sup> регулисано је да се тајни податак може одредити и означити степеном тајности „ДРЖАВНА ТАЈНА“ ако би његовим откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала неотклоњива тешка штета по интересе Републике Србије, која за последицу може имати: 1) непосредно и изузетно озбиљно угрожавање територијалног интегритета и суверености Републике Србије; 2) непосредно и изузетно озбиљно угрожавање уставног поретка и демократских принципа Републике Србије; 3) масован губитак људских живота или изузетно озбиљну претњу по живот или здравље људи или имовину великог обима; 4) изузетно озбиљну и дугорочну штету по економске интересе Републике Србије; 5) изузетно озбиљно угрожавање националне и јавне безбедности, одбране или активности безбедносних и обавештајних служби; 6) изузетно озбиљно угрожавање интереса кривичног гоњења, сузбијања кривичних дела и функционисања правосуђа; 7) изузетно озбиљно угрожавање оперативних и функционалних способности Војске Србије и других снага одбране Републике Србије; 8) изузетно озбиљно угрожавање међународног положаја Републике Србије и сарадње са другим државама, међународним организацијама и другим међународним субјектима.

19) Види: члан 14. Закона о тајности података, *Службени гласник РС*, бр. 104/09.

20) Уредба је објављена у *Службеном гласнику РС*, бр. 46/2013 од 24.05.2013. године, ступила је на снагу 01.06.2013, а примењује се од 01.09.2013. године.

Истом Уредбом дефинисано је да се тајни податак може одредити и означити степеном тајности „СТРОГО ПОВЕРЉИВО“ ако би његовим откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала тешка штета по интересе Републике Србије, која за последицу може имати: 1) изузетно озбиљно угрожавање територијалног интегритета и суверености Републике Србије; 2) изузетно озбиљно угрожавање уставног поретка и демократских принципа Републике Србије; 3) губитак људских живота у већем броју или претњу по живот или здравље људи или неко друго важно добро већег броја лица; 4) тешку штету по средњорочне економске интересе Републике Србије; 5) озбиљно угрожавање активности безбедносних и обавештајних служби; 6) озбиљно угрожавање интереса кривичног гоњења, сузбијања кривичних дела и функционисања правосуђа; 7) озбиљно угрожавање оперативних и функционалних способности Војске Србије и других снага одбране Републике Србије; 8) озбиљно угрожавање међународног положаја Републике Србије и сарадње са другим државама, међународним организацијама и другим међународним субјектима; 9) озбиљно погоршање ситуације које изазива међународне тензије.

Уредбама о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у органима јавне власти,<sup>21)</sup> у Министарству одбране,<sup>22)</sup> у Министарству унутрашњих послова<sup>23)</sup> и у Безбедносно-информативној агенцији<sup>24)</sup> одређени су подаци који потпадају под наведени степен тајности.

Степеном тајности „ПОВЕРЉИВО“ У Уредби, која се односи на Безбедносно-информативну агенцију, може се одредити и означити податак, ако би његовим откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по интересе Републике Србије, која за последицу може имати: 1) угрожавање територијалног интегритета и суверености Републике Србије; 2) угрожавање уставног поретка и демократских принципа Републике Србије; 3) губитак људских живота или претњу по живот или здравље људи или имовину; 4) штету по економске интересе Републике Србије; 5) угрожавање националне и јавне безбедности, одбране или активности безбедносних и обавештајних служби; 6) угрожавање интереса кривичног гоњења, сузбијања

21) Уредба је објављена у *Службеном гласнику РС*, бр. 46/2013 од 24.05.2013. године, ступила је на снагу 01.06.2013, а примењује се од 01.09.2013. године.

22) Види: *Службени гласник РС*, бр. 66/2014.

23) Види: *Службени гласник РС*, бр. 105/2013.

24) Види: *Службени гласник РС*, бр. 70/2013.

кривичних дела и функционисања правосудја; 7) угрожавање оперативних и функционалних способности Војске Србије и других снага одбране Републике Србије; 8) угрожавање међународног положаја Републике Србије и сарадње са другим државама, међународним организацијама и другим међународним субјектима.<sup>25)</sup>

У истој Уредби тајни податак може се одредити и означити степеном тајности „ИНТЕРНО“, ако би његовим откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по рад, односно обављање задатака и послова Агенције, која за последицу може имати: 1) смањење оперативних и функционалних способности Агенције; 2) угрожавање сарадње Агенције са безбедносним и обавештајним службама других држава, међународних организација и другим међународним субјектима; 3) нарушавање поверења грађана у законитост и стручност рада Агенције.<sup>26)</sup>

Продужење наведених рокова законодавац је предвидео у случајевима ако после истека постоје разлози да се податак и даље чува као тајни. Влада или овлашћено лице може једном продужити рок за престанак тајности најдуже за временски период утврђен за поједине степене тајности.<sup>27)</sup>

#### 4. ИЗДАВАЊЕ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА

У складу са овим законом, Канцеларија Савета поступа по захтевима за издавање сертификата и дозвола; обезбеђује примену стандарда и прописа у области заштите тајних података; 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; израђује и води Централни регистар страних тајних података; предлаже образац безбедносног

---

25) Види: члан 3. Уредбе о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Безбедносно-информативној агенцији, *Службени гласник РС*, бр. 70/2013.

26) Види: члан 4. Уредбе о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Безбедносно-информативној агенцији, *Службени гласник РС*, бр. 70/2013.

27) Види: члан 20. Закона о тајности података, *Службени гласник РС*, бр. 104/09.

упитника; предлаже образац препоруке, сертификата и дозволе; води евиденцију о издатим сертификатима, односно дозволама, као и евиденцију о одбијању издавања сертификата, односно дозвола; организује обуку корисника тајних података у складу са стандардима и прописима; предлаже Влади план заштите тајних података за ванредне и хитне случајеве; опозива тајност податка у складу са одредбама овог закона, после престанка органа јавне власти који немају правног следбеника; обавља послове који се односе на заштиту тајних података; сарађује са органима јавне власти у спровођењу овог закона у оквиру своје надлежности; обавља и друге послове који су предвиђени овим законом и прописима донетим на основу овог закона.

Република Србија, приликом израде Закона о тајности података, те употпуњавања пакета закона о заштити података, водила је рачуна о стандардима и захтевима у области система тајности података који се односе на саме органе Европске уније и заштиту тајних података у поседу органа Европске уније, нарочито на заштиту информација до којих је Европска унија дошла у комуникацији са другим међународним организацијама и државама чланицама у циљу дефинисања правног оквира и осигурања спровођења докумената у овој области.

На основу захтева поступак сертификације физичког или правног лица за приступ националним и страним тајним подацима одређеног степена тајности покреће Канцеларија Савета.

Поступак сертификације, односно издавања сертификата за приступ тајним подацима, подразумева процедуру вршења одговарајуће безбедносне провере, по чијем окончању и извештају са препоруком Канцеларија Савета поступа. Зависно од степена тајности података, постоје три врсте безбедносне провере: 1) основна безбедносна провера, за податке означене степеном тајности „ИНТЕРНО“ и „ПОВЕРЉИВО“; 2) потпуна безбедносна провера, за податке означене степеном тајности „СТРОГО ПОВЕРЉИВО“; 3) посебна безбедносна провера, за податке означене степеном тајности „ДРЖАВНА ТАЈНА“.

Законом је регулисано да безбедносну проверу за приступ тајним подацима и документима степена тајности „ДРЖАВНА ТАЈНА“ и „СТРОГО ПОВЕРЉИВО“ врши Безбедносно-информативна агенција. За приступ тајним подацима и документима означеним степеном тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ безбедносну проверу врши Министарство унутрашњих послова. Приступ тајним подацима и документима свих степена тајности за лица за-

послена на дужностима у Министарству одбране и Војсци Србије врши Војнобезбедносна агенција. Такође, безбедносну проверу за приступ тајним подацима и документима степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ за лица запослена на пословима у Безбедносно-информативној агенцији, обавља Безбедносно-информативна агенција. Безбедносну проверу за приступ тајним подацима и документима степена тајности „СТРОГО ПОВЕРЉИВО“ за лица која су запослена у Министарству унутрашњих послова врше припадници тог министарства.<sup>28)</sup>

Надлежни државни орган, на основу поднетог захтева, односно безбедносног упитника у обавези је да основну безбедносну проверу изврши у року од 30 дана, потпуну безбедносну проверу најдуже до 60 дана, док је 90 дана предвиђени рок за завршетак посебне безбедносне провере.

Неопходно је нагласити да сертификација представља само персонални елемент система заштите тајних података, као и да је потребно задовољити и остале елементе поменутог система у циљу адекватног и превентивног деловања.<sup>29)</sup>

Деловање сектора безбедности, углавном се базира на тајним подацима, па је из тих разлога, сасвим разумљиво, да прикупљањем, обрадом и анализом таквих података настају материјали, процене за конкретне активности и поступања, која се односе на актуелне безбедносне претње.

Приступ тајним подацима могућ је на начин и под условима само утврђеним прописима донетим на основу овог закона и међународним споразумима. Овлашћеним лицима за одређивање тајности податка сматрају 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 донетим на основу закона или га је за то писмено овластио руководилац органа јавне власти, као и лице запослено у органу јавне власти које је за то писмено овластио руководилац тог органа.

---

28) Види: члан 54. истог закона.

29) Види: Бојан Стаменковић, „Потрага за уверењем“, *Свет безбедности*, број 3/14, Београд, 2014, стр. 79.

## 5. РАЗМЕНА ПОДАТАКА СА СТРАНИМ ДРЖАВАМА И МЕЂУНАРОДНИМ ОРГАНИЗАЦИЈАМА

У складу са Законом о тајности података, размена тајних података са страним државама и међународним организацијама врши се преко Канцеларије Савета, осим ако посебним законом или закљученим међународним споразумом није друкчије одређено.

Законом о тајности података предвиђено је да се тајни подаци могу размењивати са страним државама и међународним организацијама само на основу закључених међународних споразума. Једино у крајње неповољним политичким, економским или одбрамбено-безбедносним околностима за Републику Србију и ако је то неопходно ради заштите њених виталних интереса, а на захтев органа јавне власти, Канцеларија Савета размењује тајне податке са страном државом, односно међународном организацијом и без претходно закљученог међународног споразума.

Према овом Закону, страни тајни податак је „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 који је са страном државом, међународном организацијом или другим међународним субјектом закључила Република Србија“.<sup>30)</sup>

Документ који садржи страни тајни податак задржава ознаку степена тајности којим је означен у страниој држави или међународној организацији. Морала би, дакле, постојати еквивалентност одговарајућих ознака тајности. При означавању степена тајности докумената, за документа намењена за сарадњу са страним државама, међународним организацијама, односно другим субјектима међународног права, осим ознака тајности које су одређене Законом о тајности података могу се користити 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“;

30) Види: члан 2. став 1. тачка 3. истог закона.

- 4) „Restricted“ одговара ознаци степена тајности „Интерно“.<sup>31)</sup>

Страни тајни подаци могу потпадати под специфичан режим ако је тако утврђено међународним обавезама које је Република Србија преузела. Тако се рок чувања тајности података може продужити и након истека законских рокова за престанак тајности, уколико је то предвиђено међународним споразумом или другим међународним обавезама Републике Србије,<sup>32)</sup> супротно наведеној ситуацији, опозив тајности се може извршити и пре истека законских рокова ако је то у јавном интересу или због извршавања међународних обавеза. Процедуре промене степена и рока тајности, као и опозива тајности страног тајног податка, вршиће се у складу са закљученим међународним споразумом и утврђеним међународним обавезама.

Ближи режим приступа, коришћења, чувања и заштите страних тајних података одређен је међународним уговорима које је Република Србија потписала са другим државама, односно другим међународним институцијама са којима је потписала споразум.

Република Србија потписала је већи број споразума о узајамној размени и заштити тајних података са другим државама и међународним организацијама: НАТО, ЕУ, Словачком, Бугарском, Чешком, Босном и Херцеговином, Македонијом, Словенијом, Шпанијом, Руском Федерацијом и Пољском. Са одређеним државама текстови споразума су у различитим фазама усаглашавања.

Наиме, међународну сарадњу у области размене и заштите тајних података наша земља је започела закључивањем Споразума између Владе Републике Србије и Организације северноатлантског пакта (НАТО) о безбедности информација и кодекса о поступању<sup>33)</sup> и закључивањем Споразума између Републике Србије и Европске уније о безбедносним процедурама за размену и заштиту тајних података.<sup>34)</sup> На основу потписаних споразума, а у складу са Законом о тајности података, формиран је Централни регистар за стране тајне податке у Канцеларији Савета као и подрегистри у Министарству спољних послова, Мисији Републике Србије при НАТО у Бриселу и Мисији Републике Србије при Европској унији,

---

31) Види: члан 16. истог закона.

32) Види: члан 20. став 2. тачка 2. истог закона.

33) Види: *Службени гласник РС - Међународни уговори*, број 6/11.

34) Види: *Службени гласник РС - Међународни уговори*, број 1/12.

Министарству унутрашњих послова, Министарству одбране и Безбедносно-информативној агенцији.<sup>35)</sup>

Размена тајних података са НАТО и Европском унијом, без обзира на то што су споразуми потврђени, отпочела је тек када су Централни регистар и подрегистри у наведеним мисијама, министарствима и другим органима формиран и прошли сертификациону контролу експертског тима НАТО и Европске уније.

## 6. КОНТРОЛА И НАДЗОР У СПРОВОЂЕЊУ ЗАКОНА

Народна скупштина усвајањем Закона о тајности података употпунила је пакет закона о заштити података. Уређени су јединствени системи утврђивања и заштите тајних података од значаја за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије, заштиту свих иностраних тајних података, приступ тајним подацима и престанак њихове поверљивости, надлежности тела и даље спровођење, као и одговорности за неиспуњавање обавеза предвиђених овим законом и друга релевантна питања.

Надзор над спровођењем Закона о тајности података, као и прописа донетих на основу тог закона врши Министарство правде.<sup>36)</sup> У складу са тим, у вршењу надзора, 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 евиденције тајних података, као и прописе којима се уређују образац безбедносног упитника, односно образац препоруке, сертификата и дозволе; налаже мере за унапређивање заштите тајних података; контролише примену критеријума за означавање степена тајности и врши друге послове контроле у складу са одредбама овог закона; подноси кривичне пријаве, захтеве за покретање прекршајног поступка и предлаже покретање другог поступка због повреде одредаба овог закона. У складу са законом, сарађује са органима јавне власти у спровођењу овог закона, у оквиру своје надлежности обавља и друге послове

35) Службе безбедности у Србији (БИА, ВБА и ВОА) на основу Закона, утврђене државне политике, смерница Владе, као и закључака Савета за националну безбедност, остварују међународну сарадњу и размењују податке и информације са службама других земаља; више о томе види: Радојица Јлазић, *Контрола служби безбедности*, нав. дело, стр. 88–91, као и члан 36. Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији, *Службени гласник РС*, бр. 88/09, 55/12 – Одлука УС и 17/13.

36) Види: члан 97. Закона о тајности података.

предвиђене овим законом и прописима донетим на основу тог закона.

Министар правде у обавези је да одборима Народне скупштине надлежним за контролу и надзор у области одбране и безбедности (Одбор за одбрану и унутрашње послове и Одбор за контролу служби безбедности) подноси годишњи извештај о активностима у спровођењу и контроли примене Закона о тајности података.

За унутрашњу контролу над спровођењем закона и прописа донетог на основу овог закона одговоран је 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 организациона јединица у саставу министарства или агенције.<sup>37)</sup>

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

## ЛИТЕРАТУРА

- Бошковић Мило, *Криминолошки лексикон*, Матица српска, Нови Сад, 2015.
- Годишњи извештај Канцеларије Савета за националну безбедност и заштиту тајних података за 2014. годину*, Канцеларија савета за националну безбедност и заштиту тајних података, Београд, 2015.
- Ђорђевић Обрен, *Лексикон безбедности*, Партизанска књига, Београд, 1986.
- Закон о безбедносно-информативној агенцији, *Службени гласник РС*, бр. 42/02, 111/09, 65/14 – Одлука УС и 66/14.
- Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији, *Службени гласник РС*, бр. 88/09, 55/12 – Одлука УС и 17/13.
- Закон о основама уређења служби безбедности Републике Србије, *Службени гласник РС*, бр. 116/07 и 72/12.
- Закон о тајности података, *Службени гласник РС*, бр. 104/09.
- Информатор о раду БИА – ажуриран 4. јануара 2017. године*, Internet, <http://www.bia.gov.rs/download/dokumenta/Informator.pdf>, 02/03/2017.
- Лазих Радојица, *Контрола служби безбедности*, Академија за националну безбедност, ЈП „Службени гласник“, Београд, 2014.

37) Види: члан 84. и 85. Закона о тајности података, *Службени гласник РС*, број 104/09.

- Миленковић Дејан, Ракић Војин, *Слободна приступ информацијама и јавна управа*, Комитет правника за људска права, Београд, 2005.
- Перан Бранко, Горета Мирко, Вукоишић Кристина, „Појам и врсте тајни“, *Зборник радова Велеучилишта у Загребу*, бр. 3-4/2015.
- Поповић Ђорђе, „Коментар закона о тајности“, *Безбедност Западног Балкана*, октобар - децембар 2009, стр. 3–10.
- Споразум између Владе Републике Србије и Организације северноатлантског пакта о безбедности информација и кодекса о поступању, *Службени гласник РС – Међународни уговори*, бр. 6/11.
- Споразум између Републике Србије и Европске уније о безбедносним процедурама за размену и заштиту тајних података, *Службени гласник РС – Међународни уговори*, број 1/12.
- Стаменковић Бојан, „Потрага за уверењем“, *Свет безбедности*, број 3/14, Београд, 2014. стр. 75–89.
- Стојадиновић Миша, Таловић Рашковић Виолета, „Изазови развоја демократије у савременом друштву: политичко насиље и теорија (не)праведног рата“, *Српска политичка мисао*, vol. 51, бр. 1, Институт за политичке студије, Београд, 2016, стр. 49-64.
- Стојадиновић Миша, „Значај медија за развој културе мира“, *Медији и култура мира на Балкану* (приредили: Бранислав Стевановић, Александра Костић, Љубиша Митровић), Филозофски факултет – универзитет у Нишу, Центар за социолошка истраживања, Ниш, 2010, стр. 371-384.
- Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Безбедносно-информативној агенцији, *Службени гласник РС*, бр. 70/13.
- Уредба о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА“ и „СТРОГО ПОВЕРЉИВО“, *Службени гласник РС*, бр. 46/13.
- Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у органима јавне власти, *Службени гласник РС*, бр. 79/14;
- Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Министарству одбране, *Службени гласник РС*, бр. 66/14.
- Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Министарству унутрашњих послова, *Службени гласник РС*, бр. 105/13.
- Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Безбедносно-информативној агенцији, *Службени гласник РС*, бр. 70/13.
- Уредба о оснивању Канцеларије Савета за националну безбедност, *Службени гласник РС*, бр. 12/09.
- Уредба о обрасцима безбедносних упитника, *Службени гласник РС*, бр. 30/10.

- Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима, *Службени гласник РС*, бр. 54/10.
- Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима, *Службени гласник РС*“, бр. 89/10.
- Уредба о начину и поступку означавања тајности података, односно документа, *Службени гласник РС*, бр. 8/11.
- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима, *Службени гласник РС*, бр. 53/11.
- Уредба о посебним мерама надзора над поступањем са тајним подацима, *Службени гласник РС*, бр. 90/11.
- Уредба о посебним мерама физичко-техничке заштите тајних података, *Службени гласник РС*, бр. 97/11.
- Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО“ и „ИНТЕРНО“ у Канцеларији Савета за националну безбедност и заштиту тајних података, *Службени гласник РС*, бр. 86/13.
- Danezis George, Domingo-Ferrer Josep, Hansen Marit, Jaap-Henk Hoepman, Le Métayer Daniel, Tirtea Rodica, Schiffner Stefan, *Privacy and Data Protection by Design – from policy to engineering*, December 2014, European Union Agency for Network and Information Security (ENISA), 2014.
- Zakon o tajnosti podataka. Analiza Centra za evroatlantske studije*, Internet, [https://www.ceas-serbia.org/images/2015-i-pre/CEAS\\_analiza\\_-\\_Zakon\\_o\\_tajnosti\\_podataka\\_-maj\\_2015.pdf](https://www.ceas-serbia.org/images/2015-i-pre/CEAS_analiza_-_Zakon_o_tajnosti_podataka_-maj_2015.pdf), 02/03/2017.

**Radojica S. Lazic**

## **DATA SECRECY PROTECTION – FROM LEGAL BASIS TO PRACTICAL IMPLEMENTATION**

### **Resume**

In spite of defined legal norms relating to implementation of the Law on Data Secrecy, its implementation has run very slowly and has still not been finished. The said law has shown a lot of weaknesses and deficiencies in practical implementation.

However, regardless of the above said, this topic has been paid serious attention by institutions dealing with jobs of national security. Especially those whose activities imply collection, processing and storing of secret data and findings of special interest for preservation of territorial integrity and sovereignty of the state of Serbia. These, certainly, include institutions of the system of national security.

Regardless of all mechanisms applied for protection of secret data, there are several ways for their revealing. Apart from violent

burglary and theft, natural disasters caused by floods, fires, earthquakes, thunderstorms, etc., careless and improper handling, negligence by creators or users, of special significance is revealing of data to persons who are not allowed access (espionage) and interception of electronic communications.

Of all the above stated, the two latter ones are the most significant with regard to revealing of data. They present a constituent part of the methodology of activities of security services in collection of data and information, which could be of special importance for taking certain political, economic, military and other stands by top state actors.

In this respect a special methodology has been developed for getting such top secret data owned by governmental and other institutions, which could be of special importance for other parties. For these reasons many world services have perfected and continue to perfect tactics and techniques to help them get top secrets of other states.

On the other hand, all countries need to protect there secrets from disappearance and thefts. For these reasons the law has been passed based on which certain procedures are being tried to be established for the purpose of best possible protection of data.

Keywords: secret data, data protection, certification, data exchange, Council's Office, security services

---

\* Овај рад је примљен 01. августа 2017. године а прихваћен за штампу на састанку Редакције 22. августа 2017. године.