ЗАКОН О ТАЈНОСТИ ПОДАТАКА

Мр *Горан* Матић

У раду су приказани најзначајнији институти Закона о тајности података уз напомену да у наредном периоду тек треба подзаконским актима детаљније уредити ову област. Неусаглашеност правног система Републике Србије у области заштите тајних података са савременим општеприхваћеним међународним стандардима и упоредно-правним искуством има за последицу неадекватну заштиту националних тајних података, и отежану сарадњу у процесу размене тајних података са другим државама и међународним организацијама. Један од циљева доношења закона био је и омогућавање транспарентности рада свих државних органа када су у питању различите области њиховог деловања, кроз значајније смањивање примене дискреционих права и арбитрарности, приликом обраде било које врсте података.

*Аутор ради као директор Канцеларије Савета за националну безбедност и заштиту тајних података

Иако су у раду приказани најзначајнији институти Закона о тајности података, у наредном периоду тек треба подзаконским актима детаљније уредити ову област, када ће бити разјашњена практична примена овог прописа. Република Србија се на почетку XXI века налази, као и Кнежевина Србија на почетку XIX века, 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 представљала би 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 јесте реформа националног система заштите тајних података. Посматрајући позитивноправна 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 из обавезе увида и давања грађанима, а проглашене су 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.

О мерама безбедности можемо, према неким ауторима[1], рећи да су оне скупови активности, радњи, и поступака које предузимају субјекти националног система безбедности (самостално или у сарадњи са другима) 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 мера безбедности јесте благовремено спречавање наступања појава које могу да угрозе националну безбедност. Осим проглашења ванредног или ратног стања, мерама безбедности сматрају се и мере приправности, мере мобилизације и мере заштите тајних података.

Систем државне безбедности представља правним прописима и политичким одлукама предвиђен и уређен делокруг надлежности, права и дужности обавештајних и безбедносних служби, војске, полиције и других институција у оквиру система националне безбедности дате државе, који систематски прикупљају, обрађују и презентују обавештајна и безбедносна сазнања и

[1] Видети: Саша Мијалковић, Национална безбедност – друго, измењено и допуњено издање, Криминалистичко-полицијска академија,Београд, 2011.

Из архива САЈ-а

Снимио: Капетан Љ. Славов,
припадник оружаних снага Р. Бугарске

спроводе друге активности по захтеву носилаца државне власти, с циљем да остваре спољну и унутрашњу безбедност земље.

Државна безбедност подразумева заштиту државног јединства, унутрашње стабилности правног и политичког система и друштвене заједнице у 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 у иностранству. Полазећи од тога, појму безбедности државе не припада само заштита државног апарата као хијерархијске организације састављене од индивидуалних и колективних носилаца државне власти (држава у ужем смислу), него и заштићеност територије и становништва обухваћених једном државном организацијом (држава у ширем смислу).

Јавну безбедност, у основи, схватамо као стање заштићености јавног поретка, односно заштите грађана и њихове имовине у држави. Под јавним поретком подразумевамо укупност јавних интереса зајамчених и заштићених правним системом, без обзира на то да ли је реч о општим (јавним ред и мир и слично) или појединачним правила (личне слободе и права, имовина и друго). Јавна безбедност се остварује откривањем, спречавањем и сузбијањем кривичних и других кажњивих дела из домена тзв. класичног криминалитета, одржавањем јавног реда и мира, осигуравањем функционисања саобраћаја на путевима, заштитом од пожара и експлозија и вршењем других стручних и административних послова. Наведене послове и задатке традиционално врше органи јавне безбедности[2].

Војна безбедност. Према истом критеријуму, понекад се и безбедност оружаних снага експлицитно издваја из општег појма безбедности, с тим што се такво схватање не може прихватити. Полазећи од специфичног објекта заштите, војна безбедност обједињује функцију (задатке) државне и јавне безбедности ради заштите оружаних снага од карактеристичних делатности којима се угрожавају стање безбедности и припреме за оружану борбу. На том плану у оружаним снагама савремених држава делују посебне службе војне безбедности у чијој се организационој структури и изван ње налазе војнообавештајне и војнобезбедносне службе. Положај, делокруг и овлашћења су им различити и зависе од многобројних фактора. Осим тога, у неким државама војна полиција и органи војне безбедности имају овлашћења и изван оружаних снага, али има и супротних примера. Имајући у виду изнето, као основни облици безбедности државе постоје једино јавна и државна (национална) безбедност.

Сама организација приступу обради тајних података била је 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. Један од проблема био је и паралелно постојање нормативе из периода СФРЈ, СРЈ, али и старих републичких прописа, који су најчешће били у правној колизији, али примењивани у пракси по инерцији.

[2] М. Милошевић, Систем државне безбедности, Београд, 2001, стр. 3-5.

Суштински, 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 међународних институција кроз успостављање процеса билатералне сарадње, али и оне везане за Евроспку унију, НАТО и слично; 5) превођење практичних позитивних и негативних искустава у одговарајућу законску и подзаконску регулативу.

Можемо закључити да је уређење система заштите тајних података процес који траје, а упоредна ускуства држава које су прошле овакве процесе говоре о периоду од 10 година или више. У државама источноевропске 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: *1) централизованог модела* (Чешка, Словачка, Бугарска, Македонија, Хрватска...), који карактерише формирање нове службе безбедности (додуше општебезбедносне или безбедносне надлежности), која представља централну националну извршну власт у области заштите тајних података, са великом бројем запослених и разноврсним надлежностима од контроле рада цивилних и војних служби безбедности до рада са тајним потписима и издавања електронског потписа и *2) децентрализованог модела* (Мађарска, Словенија, Босна и Херцеговина, Црна Гора...), који представља само једног од носиоца заштите тајних података на националном нивоу, са подељеном надлежношћу са ресорним министарствима и агенцијама, односно представља малобројну стручну агенцију која се бави координацијом свих надлежних државних органа који се баве пословима безбедности и заштитом тајних података.

Рад са подацима уређен је у више системских прописа, од којих су најзначајнији: Закон о слободном приступу информацијама од јавног значаја, Закон о заштити података о личности, као и Закон о тајности података. Поред ових, обрада података је уређена и прописима у области одбране, унутрашњих послова, здравства, службама безбедности и слично. Једна од новина у области обраде података је и увођење нових механизама контроле (који се разликују од досадашњег модела) у правни систем Републике Србије, како од институције Повереника за слободан приступ информацијама од јавног значаја и заштиту података о личности, тако и од Канцеларије Савета за националну безбедност и заштиту тајних података.

Обрада података у најширем смислу може обухватити неколико подела. Пре свега, подаци могу бити јавни – доступни најширој јавности и публиковани путем различитих јавних медија, који се у стручној јавности називају и „отвореним“ подацима. Затим, подаци могу бити са ограниченим приступом из различитих правних разлога, односно:

– *подаци од интереса за Републику Србију*, који представљају сваки податак или документ којим располаже орган 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. Дакле, у формалном смислу, то су тајни подаци који су законом, другим прописом или одлуком надлежног органа донесеном у складу са законом одређени и означени одговарајућим степеном тајности, који може бити ИНТЕРНО, ПОВЕРЉИВО, СТРОГО ПОВЕРЉИВО и ДРЖАВНА ТАЈНА;
– *подаци о личности који 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, на начин прибављања информација (слушањем, гледањем, путем увида у документ и слично) и на друга својства те информације. Податак о личности зато је сваки податак који се односи на физичко лице ако је оно одређено или одредиво;
– *пословне тајне,* које су уређене посебним прописима и не спадају у област заштите тајних података, на пример оне проистичу из прописа којима се уређује лекарска, психијатријска и психолошка делатност, адвокатура, свештенички позив и слично;
– *професионалне тајне,* које спадају у област која није на довољан начин законски уређена. Постоји само правни основ или један законски члан у прописима о привредним друштвима,

а сама обрада и критеријуми препуштени су привредним друштвима да их сами уреде. Сматрамо да би критеријуми везани за пословну тајну требало да буду уређени слично као и у закону о тајности, односно по облику и обиму штете која наступа у привредним друштвима неовлашћеним откривањем података.

Обрада података када јавност има оправдани интерес да сазна информацију. Одредбама Закона о јавном информисању[3] уређено је право на јавно информисање као право на слободу изражавања мишљења, као и права и обавезе учесника у процесу јавног информисања. Право на јавно информисање обухвата нарочито слободу изражавања мисли, слободу прикупљања, истраживања, објављивања и ширења идеја, информација и мишљења, слободу штампања и дистрибуције (растурања) новина и других јавних гласила, слободу производње и емитовања радио и телевизијског програма, слободу примања идеја, информација и мишљења, као и слободу оснивања правних лица која се баве јавним информисањем. У јавним гласилима се слободно објављују идеје, информације и мишљења о појавама, догађајима и личностима о којима јавност има оправдани интерес да сазна информацију, осим када је то другачије одређено законом, што се примењује без обзира на начин на који је прибављена информација. Носиоцима државних и политичких функција ограничена су права на заштиту приватности која имају лица на која се односи информација, ако је информација важна за јавност с обзиром на чињеницу да лице на које се односи информација обавља одређену функцију, односно права ових лица ограничена су сразмерно оправданом интересу јавности у сваком конкретном случају. Поред овог закона, интересантне су и одредбе Закона о одговорности за кршење људских права[4] (о лустрацији!) којим су уређени, односно одређени: облици и видови кршења људских права као основ за испитивање одговорности; лица према којима се спроводи поступак испитивања одговорности за кршење људских права; начела и правила поступка испитивања одговорности за кршење људских права; састав, надлежност и поступак надлежних органа и мере које се изричу лицима за која је утврђено да су кршила људска права. Интересантно је напоменути и да се поступак по овоме закону, односно обрада података о личности, спроводи без пристанка тог лица.

[3] „Службени гласник РС“ број 43/2003 и 61/2005.
[4] „Службени гласник РС“ број 58/2003 и 61/2003.

Питање односа између слободног приступа информацијама и заштите тајности података. Један од новонасталих проблема у пракси представља питање односа између слободног приступа информацијама и реализација задатка заштите тајности података. Тако, на пример, према одредбама Закона о слободном приступу информацијама, подаци се морају уступити на увид јавности, али одредбама члана 9. предвиђени су и одређени изузеци, који се односе на: 1) националну безбедност; 2) јавну безбедност; 3) комерцијалне и друге економске јавне и приватне интересе; 4) економску, монетарну и девизну политику државе; 5) спречавања, истраживања и процесуирања кривичних дела; 6) приватност и друга лична права; 7) обраду и доношење службених аката.

Поред тога, примену Закона о слободном приступу информацијама отежава околност да је овај закон први донет, да је након њега, током 2008. године, донет Закон о заштити података о личности, а да још увек не постоји Закон о заштити тајних података, који би заправо претходио овим законима и био „кровни“ или „темељни“ закон за примену закона о слободном приступу информацијама.

Закон о тајности података

Закон о тајности података усвојен је 2009. године и објављен у „Службеном гласнику РС“ број 104/2009. Овим законом уређен је јединствен систем одређивања и заштите тајних података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије, заштиту страних тајних података, приступ тајним подацима и престанак њихове тајности, надлежност органа и надзор над спровођењем овог закона, као и одговорност за неизвршавање обавеза из овог закона и друга питања значајна за заштиту тајности података.

Закон има следећу структуру: основне одредбе; одређивање тајних података; мере заштите тајних података; приступ тајним подацима; поступак за издавање сертификата односно дозволе; контрола и надзор; казнене одредбе; прелазне и завршне одредбе. У међувремену, у другој половини 2010. године, од ступања овог закона на снагу на основу њега донете су и одређене уредбе:

1) *Податак који се може одредити као тајни* јесте податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја. Тајним податком се не сматра податак који је означен као тајна ради прикривања кривичног дела, прекорачења овлашћења или злоупотребе службеног положаја или другог незаконитог акта или поступања органа јавне власти.

2) *Овлашћена лица за одређивање тајности података* су: председник Народне скупштине; председник Републике; председник Владе; руководилац органа јавне власти; изабрани, постављени или именовани функционери органа јавне власти који су за дорећивање тајних података овлашћени законом, односно прописом донетим на основу закона, или их је за то писмено овластио руководилац органа јавне власти; лице запослено у органу јавне власти које је за то писмено овластио руководилац тог органа;

3) *Поступак одређивања тајности података* почиње приликом његовог настанка, односно када орган јавне власти започне обављање посла чији је резултат настанак тајног податка. При одређивању тајности податка овлашћено лице процењује могућу штету по интересе Републике Србије.

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

5) *Посебни случајеви одређивања и означавања тајних података.* Овлашћено лице одређује као тајни онај податак који је настао обједињавањем или повезивањем података који сами по себи нису тајни, ако тако обједињени или повезани представљају податак који треба заштитити због разлога утврђених овим законом.

6) *Ознаке тајности.* 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;

7) *Степени тајности и садржина података.* Подаци од интереса за Републику Србију имају један од следећих степена тајности: ДРЖАВНА ТАЈНА – који се одређује ради спречавања настанка неотклo-

њиве тешке штете по интересе Републике Србије; СТРОГО ПОВЕРЉИВО – који се одређује ради спречавања настанка штете по интересе Републике Србије; ПОВЕРЉИВО – који се одређује ради спречавања настанка штете по интересе Републике Србије; ИНТЕРНО – који се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио. Ближе критеријуме за одређивање наведених степена тајности одређује Влада, уз претходно прибављено мишљење Савета за националну безбедност или на предлог надлежног министра, односно руководиоца органа јавне власти.

8) *Означавање страних тајних података* – документ који садржи страни тајни податак задржава ознаку степена тајности којим је означен у страној држави или међународној организацији. При означавању степена тајности докумената намењених за сарадњу са стартним државама, међународним организацијама, односно другим субјектима међународног права могу се користити и одговарајуће ознаке степена тајности на енглеском језику, и то: ДРЖАВНА ТАЈНА – TOP SECRET; СТРОГО ПОВЕРЉИВО – SECRET; ПОВЕРЉИВО – CONFIDENTAL; ИНТЕРНО – RESTRICTED.

9) *Временско ограничење тајности података* – тајност података престаје: 1) датумом утврђеним у документу у којем је садржан тајни податак – када се утврди да наступањем одређеног датума престају разлози због којих је податак проглашен за тајни; 2) наступањем одређеног догађаја утврђеног у документу који садржи тајни податак – када се утврди да наступањем одређеног догађаја престају разлози због којих је податак проглашен за тајни; 3) истеком законом одређеног рока – за степен ДРЖАВНА ТАЈНА након 30 го-

Снимио: З. Миловановић

дина, за степен СТРОГО ПОВЕРЉИВО након 15 година, за степен ПОВЕРЉИВО након 5 година, за степен ИНТЕРНО након 2 године; 4) опозивом тајности, када се утврди да постоје чињенице и околности услед којих податак престаје да буде од интереса за Републику Србију, на основу периодичне процене тајности и предлога за опозив; 5) ако је податак учињен доступним јавности.

10) *Опозив тајности* – 1) у поступку вршења контроле Канцеларија Савета за националну безбедност и заштиту тајних података може од овлашћеног лица захтевати ванредну процену тајности података и на основу те процене сама донети одлуку о опозиву тајности; 2) на основу одлуке надлежног органа овлашћено лице органа јавне власти опозива тајност податка и омогућава остваривање права тражиоцу, односно подносиоцу захтева на основу решења Повереника за информације од јавног значаја и заштиту података о личности у поступку по жалби, односно на основу одлуке надлежног суда у поступку по тужби, у складу са законом којим се уређује слободан приступ информацијама од јавног значаја и законом којим се уређује заштита података о личности; 3) у јавном интересу, када Народна скупштина, председник Републике и Влада могу са појединих докумената опозвати ознаку тајности, без обзира на степен тајности, ако је то у јавном интересу или због извршавања међународних обавеза.

11) *Периодична процена тајности.* Овлашћено лице врши периодичну процену тајности, на основу које може извршити опозив тајности, и то: 1) за степен ДРЖАВНА ТАЈНА најмање једном у 10 година; 2) за степен СТРОГО ПОВЕРЉИВО најмање једном у 5 година; 3) за степен ПОВЕРЉИВО најмање једном у 3 године; 4) за степен ИНТЕРНО најмање једном годишње.

У складу са одредбама Закона о тајности података, мере заштите тајних података обухватају следеће целине:

– *критеријуме заштите тајних података* – када орган јавне власти успоставља систем поступака и мера заштите тајних података према следећим критеријумима: 1) степену тајности; 2) природи документа у којем је садржан тајни податак; 3) процени претње за безбедност тајног податка;
– *врсте мера заштите* –опште и посебне мере заштите које се предузимају ради спречавања настанка штете, односно мере које се односе на остваривање административне, информатичко-телекомуникационе, персоналне и физичке безбедности тајних података;

Снимио: З. Миловановић

– *опште мере заштите тајних података,* које обухватају: 1) одређивање степена тајности; 2) процену претње за безбедност тајног податка; 3) одређивање начина коришћења и поступања са тајним податком; 4) одређивање одговорног лица за чување, коришћење, размену и друге радње обраде тајног податка; 5) одређивање руковаоца тајним подацима, укључујући и његову безбедносну проверу у зависности од степена тајности података; 6) одређивање посебних зона, зграда и просторија намењених заштити тајних података и страних тајних података; 7) надзор над поступањем са тајним податком; 8) мере физичко-техничке заштите података, укључујући и уградњу и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту ван безбедносне зоне; 9) мере заштите информационо-телекомуникационих система; 10) мере криптозаштите; 11) заштитни режим радних и формацијских места, у оквиру акта о унутрашњем уређењу и систематизацији радних места (принцип „ПОТРЕБНО ДА ЗНА“); 12) утврђивање посебних програма образовања и обуке за потребе обављања послова заштите тајних података и страних тајних података; 13) друге опште мере одређене законом;
– *посебне мере заштите,* које се уређују актом Владе, а неке и актом надлежног министра, односно руководиоца посебне организације;
– *обавезе руковаоца,* који предузима мере заштите тајних података и омогућава корисницима непосредан приступ тајним подацима, издаје копије докумената, води евиденције корисника и стара се о размени тајних података;
– *чување, преношење и достављање тајних података.* Они се могу преносити и достављати изван органа јавне власти само уз придржавање прописаних мера безбедности и поступака којима се обезбеђује да податке добије лице које има сертификат за приступ тајним подацима и које има право да их добије,
– *дужност обавештавања у случају губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних података и страних тајних података.* Овлашћено лице је дужно 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 ради отклањања штете и спречавања поновног губитка, крађе, оштећења, уништења или неовлашћеног откривања.

Контрола и надзор над применом Закона о тајности података

Контрола и надзор над применом Закона о тајности података може се поделити на послове који се обављају у оквиру: унутрашње контроле, Канцеларије Савета за националну безбедност и заштиту тајних података и министарства надлежног за послове правосуђа.

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.

Канцеларија Савета за националну безбедност и заштиту тајних података[5] 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 Законом о тајности података, 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. 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 другачије одређено.

Министарство надлежно за правосуђе врши надзор над спровођењем овог закона и прописа донетих на основу закона. У складу са Законом о тајности података, у вршењу надзора, ово министарство: 1) прати стање у области заштите тајних података; 2) припрема прописе неопходне за

[5] Према ратификаваним међународним споразумима и стандардима у области заштите тајних података, ова канцеларија обавља и послове NSA (National Security Authority), односно органа надлежног за спровођење одређених стандарда и политика на териотирји Србије када су у питању страни тајни подаци.

спровођење овог закона; 3) даје мишљење на предлоге прописа у области заштите тајних података; 4) 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; 5) налаже мере за унапређивање заштите тајних података; 6) контролише примену критеријума за означавање степена тајности и врши друге послове контроле у складу са одредбама овог закона; 7) подноси кривичне пријаве, захтеве за покретање прекршајног поступка и предлаже покретање другог поступка због повреде одредаба овог закона, у складу са законом; 8) сарађује са органима јавне власти у спровођењу овог закона у оквиру своје надлежности; 9) обавља и друге послове који су предвиђени 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 овог 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, руковаоца, односно корисника тајног податка.

Приступ тајним подацима

Приступ тајним подацима и коришћење података и докумената било ког степена тајности без издавања сертификата, на основу функције и ради 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, ова лица имају право на приступ тајним подацима који су означени степеном „ДРЖАВНА ТАЈНА“ и „СТРОГО ПОВЕРЉИВО“ уз претходну безбедносну проверу из члана 53. тач. 2) и 3) овог закона, 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). Лица која имају приступ тајним подацима у складу са овим законом, овлашћена су и дужна да у поступку који воде и иначе, на сваки сврсисходан начин и од свакога заштите тајност података које су сазнали и да тајним подацима приступају лично. Функционери, запослена лица, односно лица која обављају послове у органима јавне власти имају приступ тајним подацима означеним степеном тајности „ИНТЕРНО”. Наведена лица потписују изјаву, којом потврђују да ће поступати са тајним подацима у складу са законом и другим прописом.

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“.

Физичко и правно лице – корисник тајног податка, има право приступа тајним подацима који су неопходни за обављање послова из делокруга његовог рада и који су по степену тајности одређени у сертификату за приступ тајним подацима (у даљем тексту: сертификат), односно дозволи. У случају изузетне хитности у поступању, лице коме је издат сертификат, односно дозвола за приступ тајним подацима означеним нижим степеном тајности, може бити упознато са тајним податком означеним непосредно вишим степеном тајности. Ово лице је дужно да потпише изјаву, којом потврђује да ће поступати са тајним подацима, у складу са законом и другим прописом. Пре издавања сертификата, односно дозволе, лице коме се издаје сертификат дужно

је да потпише изјаву, којом потврђује да ће поступати са тајним подацима у складу са законом и другим прописом. Ако ово лице не потпише изјаву, поступак издавања сертификата, односно дозволе, обуставља се. Писана изјава чини саставни део документације на основу које је издат сертификат, односно дозвола.

*Ослобођење од дужности чувања тајности***.** Лице коме је издат сертификат, односно дозвола, те податке не може да користи у друге сврхе, осим за оне за које је сертификат, односно дозвола издата. Руководилац органа јавне власти може да на захтев надлежног органа ослободи лице дужности чувања тајности податка посебном одлуком којом ће се предвидети и мере заштите тајности података, али само за намене и у обиму који садржи захтев надлежног органа, у складу са законом. На захтев надлежног органа, руководиоца органа јавне власти дужности чувања тајности податка може ослободити орган који га је именовао, изабрао, односно поставио, о чему обавештава Канцеларију Савета.

*Достављање тајних података уз обавезу чувања тајности***.** Тајни подаци могу се доставити другом органу јавне власти на основу писменог одобрења овлашћеног лица органа јавне власти који је податке означио као тајне, ако посебним законом није одређено друкчије. Тајни податак добијен од органа јавне власти не може се без сагласности органа који је податак одредио као тајни доставити другом кориснику, ако посебним законом није одређено друкчије. Лица која обављају послове у органу јавне власти коме су достављени тајни подаци дужна су да поступају у складу са одредбама овог закона, уз обавезу поштовања ознаке тајности и предузимања мера заштите тајности података.

Достављање тајних података на основу уговорних односа. У упоредном праву и по стандардима у области заштите тајних података ове процедуре се најчешће називају „индустријском безбедношћу“, што представља један од озбиљнијих пропуста приликом доношења овог закона, који изазива највише забуне у пракси. Према закону, овлашћено лице може доставити тајне податке другим правним или физичким лицима, која по основу уговорног односа пружају услуге органу јавне власти: 1) ако правно или физичко лице испуњава организационе и техничке услове за чување тајних података у складу са овим законом и прописом донетим на основу овог закона; 2) ако су за лица која обављају уговорене послове извршене безбедносне провере и издати сертификати; 3) ако лица из тачке 2. овог става писаном изјавом потврде да су упозната са овим законом и другим прописима који уређују чување тајних података и обавежу се да ће са тајним подацима поступати у складу са тим прописима; 4) ако је приступ тајним подацима неопходно потребан ради реализације послова предвиђених уговором. Мере заштите тајних података које из наведеног проистичу морају бити садржане у уговору који у вези са реализацијом послова закључе орган јавне власти и правно или физичко лице. Руковалац тајних података код органа јавне власти успоставља и води ажурну евиденцију о тајним подацима који су достављени другим корисницима изван органа јавне власти.

Поступак издавања сертификата, односно дозволе – на који се примењују 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 његове садржине; безбедносну проверу. За вршење безбедносне провере – за степене ДРЖАВНА ТАЈНА и СТРОГО ПОВЕРЉИВО надлежна је Безбедносно-информативна агенција (за своје потребе врши и провере за ИНТЕРНО и ПОВЕРЉИВО); за степене тајности ПОВЕРЉИВО и ИНТЕРНО надлежно је министарство надлежно за унутрашње послове (за своје потребе и за степен СТРОГО ПОВЕРЉИВО); за све степене тајности у оквиру министарства надлежног за послове одбране и Војску Србије надлежна је Војнобезбедносна агенција.За сарадњу са страним државама и међународним организацијама,рок за извршење безбедносне провере је 30 дана за основну безбедносну проверу; 60 дана за потпуну безбедносну проверу; 90 дана за посебну безбедносну проверу; решење и допунску проверу. Канцеларија Савета о издавању сертификата одлучује решењем у року од 15 дана од дана достављања извештаја са препоруком. Канцеларија Савета има могућност да захтева и допунске провере ако не може утврдити да ли су испуњени законом предвиђени услови за издавање сертификата. Решење се доставља руководиоцу органа јавне власти који је тражио издавање сертификата и лицу за које је тражен сертификат. Против решења Канцеларије Савета може се поднети жалба министру надлежном за правосуђе,

а против овог решења може се покренути управни спор. Садржај, облик и достављање сертификата – уређено је посебном уредбом. Сертификат престаје да важи: 1) истеком времена за који је издат (ДРЖАВНА ТАЈНА важи 3 године, СТРОГО ПОВЕРЉИВО важи 5 година, ПОВЕРЉИВО важи 10 година и ИНТЕРНО важи 15 година); 2) престанком функције из члана 38. Закона о тајности података; 3) престанком обављања дужности и послова из делокруга рада лица из члана 40. овог закона; 4) на основу решења Канцеларије Савета у поступку провере издатог сертификата; смрћу физичког лица или престанком правног лица коме је издат сертификат; привремена забрана приступа; провера сертификата; издавање дозволе страном лицу; службене евиденције и други подаци везани за сертификат и дозволу које води Канцеларија Савета, органи надлежни за вршење безбедносних провера и органи јавне власти – на ове евиденције се примењују одредбе закона којим је уређена заштита података о личности, изузев на податке који би открили методе и поступке коришћене у прикупљању података који користе службе безбедности.

За лица којима је приступ тајним подацима потребан ради обављања функције или радних дужности у службама безбедности Републике Србије, изузетно од члана 66. овог закона, одлуку о издавању сертификата за приступ тајним подацима којима располаже служба безбедности доноси руководилац службе из члана 54. ст. 3. и 4. овог закона. Законодавац је на овај начин покушао да уреди питање приступа тајним подацима који се односе на нарочито осетљиве активности државних органа и угрожавање националне безбедности, који су традиционално били третирани као тајни подаци од највишег значаја за опстанак државе, односно настојало се да се на-

Снимио: Ј. Мамула

ће компромис између два супротстављена пола јавности и тајности, са основним задатком да се омогући успостављање контроле над активностима којима се задире у људске слободе и права, али и заштиту легитимних интереса државе. Самим тим, ове активности су изазивале највише пажње међународних организација, невладиног сектора, медија и различитих експерата из области заштите људских права.

Одбијање захтева за издавање сертификата. 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, односно дозволе из чл. 48. до 50. овог закона; 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.

Безбедносне провере физичких и правних лица

Критеријуми (безбедносни критеријуми) који се односе на заснивање радног односа у одређеним структурама, као и обављање одређених специфичних дужности у оквиру система (на пример, службе криптозаштите, ангажовање на дужностима везаним за војне службе безбедности и слично) разликују се од оних који представљају безбедносну сметњу и ризик за руковање 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. Сматрамо да их је потребно дефинисати у различитим прописима. Заједничко питање за све безбедносне провере, било да су везане за заснивање радног односа у државним органима, обављање одређених специфичних дужности у њима или су потребне ради приступа тајним подацима своде се на питање провере и процене података које обавља полиција и овлашћени органи служби безбедности. Методолошки се могу поделити на: А) проверу по месту становања и месту запослења; Б) проверу из јавних и других евиденција и оперативних евиденција којима располажу органи јавне власти, полиција и службе безбедности;

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

Када је реч о проценама, битно је указати на:

– 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 (супружника, деце, рођака и слично) и лица са којима живи у заједничком домаћинству, раније осуђиваности и слично. Ова процена обавља се на основу јавних и других података и евиденција које воде државни органи;
– процену 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.

Приликом обављања провера и процена задире се у област обраде нарочито осетљивих података о личности за потребе безбедности, одбране и слично, тако да највећи проблем у пракси може представљати, дефинисање односа нормирано стање – дискрециона процена надлежног органа.

Нарочито осетљиви подаци дефинисани су одредбама члана 16. Закона о заштити података о личности и односе се на: националну припадност; расу; пол; језик; вероисповест; припадност политичкој странци; синдикално чланство; здравствено стање; примање социјалне помоћи; жртву насиља; осуду за кривично дело; сексуални живот (или опредељење хетеро или хомосексуално). Критеријуми за безбедносне сметње и процедуре су различити за „ДРЖАВНУ ТАЈНУ“, „СТРОГО ПОВЕРЉИВО“, „ПОВЕРЉИВО“ и „ИНТЕРНО“. Провера за „ДРЖАВНУ ТАЈНУ“ обухвата податке из основног и посебног упитника за физичка и правна лица, као и

Снимио: Р. Поповић

вршење посебне безбедносне провере; провера за „СТРОГО ПОВЕРЉИВО“ обухвата податке из основног и посебног упитника за физичка и правна лица, као и вршење потпуне безбедносне провере; провера за „ИНТЕРНО“ и „ПОВЕРЉИВО“ обухвата податке из основног упитника за физичка и правна лица, као и вршење основне безбедносне провере.

У случајевима када се доноси одлука о одбијању захтева за издавање безбедносног сертификата – на основу извештаја, односно допунске безбедносне провере, одређене законом, такође су наведени одређени критеријуми за безбедносне провере и процене: 1) ако је подносилац захтева навео неистините и непотпуне податке у основном, односно посебном безбедносном упитнику. Тада могу постојати две ситуације: да је подносилац захтева или кандидат намерно поднео нетачне податке у намери да прикрије одређене чињенице које би могле имати утицаја на безбедносну процену ризика; да је подносилац захтева погрешио случајно приликом уношења података у упитник, погрешан број, слично име или презиме, превид у редоследу и слично; 2) ако подносилац не испуњава услове за издавање сертификата, односно дозволе из члана 48. до 50. овог закона – који се односе на услове за: а) *физичко лице* – држављанство Републике Србије; пунолетство; пословну способност; неосуђиваност за кривично дело за које се гони по службеној дужности, односно за прекршај предвиђен овим законом; постојање одговарајуће безбедносне провере (осим у случајевима када то није предвиђено чл. 37 и 38. став 1.); б) *правно лице* – регистровано седиште на територији Републике Србије; обављање делатности у вези са интересима из члана 8. овог закона; постојање одговарајуће безбедносне провере; ако није у поступку ликвидације или стечаја; није кажњавано мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мере безбедности забране обављања одређених регистрованих делатности или послова; уредно измирење пореских обавеза и доприноса; г) *страно лице* – поседовање одговарајућег сигурносног сертификата издатог од стране државе чији је држављанин, односно у којој правно лице има седиште или од стране међународне организације чији је члан. 3) ако подносилац захтева није обезбедио услове за предузимање прописаних мера заштите тајних података; 4) ако постоји безбедносни ризик од приступа и коришћења тајних података. Посебно питање у вези са проценама које обављају надлежне безбедносне службе представљају индикатори угрожавања националне безбедности и методлогија рада служби безбедности, који се морају по хитном поступку преиспитати и уредити на

један нови начин, који не би остављао или би остављао што мање простора за дискреционе оцене које нису утемељене на конкретним подацима који дају основа за утврђивање безбедносног ризика.

Основна и потпуна безбедносна провера. Попис критеријума за безбедносне ризике и сметње које проистичу из члана 58, 59 и 60. Закона о тајности података:

– *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 пресуде. 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 – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *кривични поступци у току* – не производе последице, осим у кривичнопроцесном смислу. Међутим, ова околност представља безбедносну сметњу и ризик за приступ тајним подацима, али и за рад на безбедносно осетљивим радним местима – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *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 – ствар процене надлежног органа (службе безбедности) – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *прекршајни поступци у току* – не производе последице, осим у прекршајнопроцесном 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 – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);

Снимио: J. Мамула

– *контакти са страним службама безбедности и обавештајним службама* – могу бити планирани кроз активности државних органа (међународна сарадња, оперативно комбиновање и слично) или самоиницијативни и за рачун ових страних служби (шпијунажа). Заснива се на дискреционој процени органа који врши проверу и на његовој оперативној документацији која као таква не може бити коришћена приликом вођења управног спора, без предузимања одговарајућих мера заштите – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *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 уређивања и вођења листе забрањених и илегалних организација је у надлежности Савета за националну безбедност – тзв. „црне листе“ – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *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. Временско важење за примену ових критеријума – када се бришу, како се евидентирају, персонална досијеа запослених, разлог за раскид радних односа – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *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* – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *служба у страним војскама и паравојним формацијама* – рок за посебну безбедносну проверу обухвата најмање десет година од дана подношења захтева (чл. 62);
– *други подаци и чињенице који физичко и правно лице чине подложним утицајима и притисцима који представљају безбедносни ризик;*
– *дугови настали услед финансијских задужења или преузетих гаранција.*

Додатни критеријуми за правна лица (чл. 59), поред оних претходно наведених, обухватали би и оне (из тач. 9) које се односе на податке о осудама за кривично дело, привредни преступ и прекршај правног лица и одговорних лица у правном лицу, као и податке поступцима за кривично дело, привредни преступ или прекршај против правног лица који су у току.

Посебна безбедносна провера. Критеријуми за потребе посебне безбедносне провере – за утврђивање безбедносног ризика приступа тајним подацима (чл. 62) 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 издавања сертификата, које би, у том случају, представљале основ за сумњу у његову поверљивост и поузданост, а нарочито ако су његове активности у супротностима са интересима Републике Србије или ако је повезан са страним лицима која могу да угрозе безбедност и међународне интересе Републике Србије.

Допунска безбедносна провера (члан 66) – ако 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 из члана 54. овог закона да изврши допунску проверу, односно допуну извештаја и израду нове препоруке, најкасније у накнадном року од 30 дана.

Казнене одредбе[6] у Закону о тајности података обухватају кривично дело и два прекршаја. *Кривично дело* из члана 98. За-

[6] У судској пракси још није забележен ниједан 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.

кона о тајности гласи: 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.

Прекршајна одговорност одговорног лица у органу јавне власти из члана 99. Закона о тајности података: 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 означе као тајни (члан 8. став 2); 2) овлашћење за одређивање тајности података пренесе на треће лице (члан 9.став 3); 3) означи тајне податке садржане у документу неодговарајућим степеном тајности (члан 11. став 2); 4) донесе одлуку о одређивању тајности податка без образложења (члан 11. став 4); 5) не опозове тајност податка после наступања датума или догађаја после којег престаје тајност податка (чл. 17. и 18); 6) не опозове тајност податка после истека законског рока за престанак тајности податка (члан 19); 7) не спроведе периодичну процену тајности податка (члан 22); 8) не опозове тајност податка на основу решења Повереника за информације од јавног значаја и заштиту података о личности или одлуке надлежног суда (члан 25); 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 (члан 28); 11) не пропише, организује и надзире опште и посебне мере заштите тајних података који одговарају степену њихове тајности (чл. 32. и 33); 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 (члан 42. став 3); 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 (члан 82. став 1); 15) решење за приступ тајним подацима не чува у посебном делу кадровског досијеа (члан 82. став 2); 16) не организује унутрашњу контролу над заштитом тајних података (члан 84. став 1); 17) не предузме мере да се образује, води и обезбеђује посебан регистар страних тајних података (члан 94. став 2). *Прекршајна одговорност руковаоца тајних података* из члана 100. Закона о тајности података:

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 (члан 34).

Обавезе које произлазе из Закона о тајности података[7]

Закон о тајности података унео је у правни систем Републике Србије један нов системски 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 наметнуо је 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, увођењем степена тајности коме лице има приступ у обављању својих послова; 6) израда аката о преносу тајних података, примени општих и посебних мера и слично; 7) одређивање руковаоца 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 службених 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.

[7] Напомена аутора: ове обавезе се примењују само на рад са страним тајним подацима, док се не уреде критеријуми за рад са подацима степена тајности ДРЖАВНА ТАЈНА, СТРОГО ПОВЕРЉИВО, ПОВЕРЉИВО и ИНТЕРНО.

Снимио: J. Мамула

Међународна сарадња у области заштите тајних података[8] обавља се на више нивоа: на првом нивоу – у оквиру међународне мултилатералне сарадње везане за евроатлантске 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 одбране, правосуђа, полиције и друге области, уз напомену да још увек не постоје посебно разрађени регионални механизми сарадње у области размене и заштите тајних података на Западном Балкану; на трећем нивоу – у оквиру билатералне сарадње држава западног Балкана, кроз потписивање појединачних билатералних споразума и њихову имплементацију у правне системе сваке државе. Значајни помак био би формирање регионалног борда директора надлежних за заштиту и размену тајних података на Западном Балкану, који би у првој фази обухватао Словенију, Хрватску, Босну и Херцеговину, Србију, Црну Гору и Македонију и који би довео до повећања степена регионалне безбедности кроз повећање конкретних активности „на терену“.

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 и реафирмацију јавне сфере.

„Пут од 1.000 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 требало да буде 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 његове практичне примене, 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, ЕУ, 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, постоје следећи садржаји: 1) физичко обезбеђење; 2) техничко обезбеђење; 3) заштитни режим формацијских или радних места и безбедносне провере; 4) заштита од пожара и експлозија; 5) заштита од елементарних непогода; 6) заштита у ванредним околностима; 7) заштита која се односи на боравак 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) контрола спровођења мера. Поред тога, морамо указати да од примене овога закона није изузет ниједан 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 и арбитрарности, приликом обраде било које врсте података.

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 требало да уреди рад само са тајним подацима који се креирају од момента његовог доношења.

Литература:

1. Милошевић, М.: *Систем државне безбедности*; Криминалистичко-полицијска академија, Београд, 2001.

2. Мијалковић, С.: *Национална безбедност* – друго, измењено и допуњено издање; Криминалистичко-полицијска академија; Београд, 2011.

[8] Република Србија је од ступања на снагу Закона о тајности података потписала међународне споразуме са НАТО, ЕУ, Словачком и Бугарском.