



## Заштита тајности података

### Увод

Укидањем државне заједнице Србија и Црна Гора 2006. године, Република Србија постала је самостална и независна држава, чиме су се коначно стекли институционални оквири за уређење области тајних података на начин који обезбеђује заштиту националних интереса Републике Србије и њених грађана у овој изузетно значајној области.

И поред тога, у Републици Србији још увек функционише законска и подзаконска регулатива заштите тајних података наслеђена из ранијих периода и претходних система.

Истовремено, приступање евроатланским безбедносним интеграцијама, као и потреба ефикасне и рационалне размене података са другим државама, међународним организацијама и институцијама, у складу са међународно установљеним стандардима, захтева да Република Србија у што краћем року донесе системски закон из области заштите тајних података.

Из тих разлога, намера је да се прикаже важећа регулатива у области тајних података са аспекта њене превазиђености али и да се укаже на елементе од значаја за израду новог системског закона о заштити тајних података.

### Постојеће стање

У целини посматрано, заштита тајности података, дефинисање појма државне, војне, службене, пословне и осталих тајни, одређивање података и докумената који се сматрају одговарајућим обликом тајне, као и прекршајна и кривично-правна заштита тајни, садржана је у више законских и подзаконских прописа, и то:

---

37 Државни секретар Министарства одбране Републике Србије

---

Одредбама Кривичног законика Републике Србије одређено је да се:

- државном тајном сматрају подаци или документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени државном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице по безбедност, одбрану или за политичке, војне или економске интересе Републике Србије (члан 316. став 5.);
- службеном тајном сматрају подаци или документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени службеном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за службу (члан 369. став 4.);
- војном тајном сматрају подаци који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени војном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за Војску или одбрану или безбедност земље (члан 415. став 4.);
- пословном тајном сматрају подаци и документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени пословном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за предузеће или други субјект привредног пословања (члан 240. став 4.).

Законом о одбрани (члан.126.) утврђено је да се до доношења Закона о заштити тајних података примењују одредбе раније важећег Закона о одбрани (члан 67. став 2.) по коме се тајним подацима значајним за одбрану земље сматрају документа, подаци о борбеним и другим материјалним средствима, објектима, мерама и радњама, као и други подаци чије би откривање могло нанети штету одбрани и безбедности земље.

Уредбом о критеријумима за утврђивање података значајних за одбрану земље који се морају чувати као државна или службена тајна и о утврђивању задатака и послова од посебног значаја за одбрану земље које треба штитити применом посебних мера безбедности (члан 11. ) државну тајну представљају тајни подаци чијим би откривањем могле наступити тешке последице за одбрану и безбедност земље, а који се нарочито односе на :

- војне, политичке, економске и друге процене на којима се заснива политика одбране земље;
- план опште мобилизације и план организовања припрема за одбрану државних органа, предузећа и других правних лица (План одбране земље);
- извод из Плана одбране земље и планове и програме развоја

- 
- за предузећа која су од посебног значаја за одбрану земље;
- врсте, укупне количине и размештај робних резерви у републици и капацитете и могућности ратне производње;
  - сводне анализе и оцене стања припрема за одбрану земље;
  - планове припрема и уређења државне територије за потребе одбране земље;
  - објекте од посебног значаја за одбрану земље;
  - научне и техничке проналаске од посебног значаја за одбрану земље;
  - процене, анализе и поједине мере државних органа од посебног значаја за одбрану земље, као и
  - организацију система веза, планове и средства за криптозаштиту, као и прописане норме и поступке спровођења криптозаштите.

Овом уредбом, такође је утврђено да службену тајну представљају тајни подаци чијим би откривањем могле наступити штетне последице за безбедност и одбрану земље (члан 12.).

Сваком податку који представља службену тајну, зависно од његовог значаја, уредбом је прописан један од следећих степена тајности: „строго поверљиво“, „поверљиво“ и „интерно“, и то:

1. степен тајности „строго поверљиво“ одређен је за податке чијим би откривањем могле наступити теже штетне последице за одбрану земље (члан 13.), а односе се на :

- изводе из Плана одбране земље и ратну организацију државних органа;
- извод из Плана одбране земље и мобилизацијске планове предузећа и других правних лица;
- организацију, планове, средства и систем ратних веза;
- планове организације и рада службе осматрања и обавештавања;
- врсте , количине и размештај робних резерви;
- истраживања геолошког састава земљишта, геомагнетизма, хидролошких карактеристика терена и параметара мора, а који су од посебног значаја за одбрану земље;
- научне и техничке проналаске значајне за одбрану земље;
- анализе и оцене стања припрема за одбрану јединица локалне самоуправе, појединих државних органа, предузећа и других правних лица;
- планове припрема и уређења територије за потребе одбране земље;

- 
- извештаје са инспекцијских обилазака о стању одбрамбених припрема;
  - прописе о раду државних органа, предузећа и других правних лица за време ратног или ванредног стања;
  - планирану евакуацију, рушење или онеспособљавање објекта материјално-техничких и других средстава;
  - дужности и радна места од значаја за одбрану које треба штитити применом посебних мера безбедности;
  - организацију, формацију и структуру војнотериторијалних органа и јединица, као и
  - криптозаштиту.

2. степен тајности „поверљиво“ одређен је за податке чијим би откривањем могле наступити последице за безбедност и одбрану земље (члан 14.), а одnose се на:

- картографске публикације које садрже податке од интереса за одбрану земље;
- аеро фото снимке подручја значајних за одбрану земље;
- објекте значајне за одбрану земље;
- укупну структуру кадра и њихов распоред на ратне дужности;
- дужности и радна места од значајна за одбрану земље;
- организацију и формацију јединица цивилне заштите и цивилне одбране;
- врсте и капацитете природних и вештачких склоништа за заштиту становништва и материјалних добара у рату.

3. степен тајности „интерно“ одређен је за податке од значаја за одбрану у односу на њихово коришћење и међусобну размену од стране државних органа, предузећа и других правних лица, а по свом значају не представљају податке стого поверљивог или поверљивог карактера (члан 15.).

Правилником о критеријумима за утврђивање података о Војсци који представљају војну тајну, степен војне тајне и мере за њихову заштиту (члан 12.) утврђено је да војну тајну представљају подаци о Војсци, плановима и припремама Војске, средствима наоружања и војној опреми, војним објектима и постројењима, као и сви остали подаци који се односе на делатност Војске за које се проценом утврди да би њихово откривање могло изазвати штетне последице за Војску и њене припреме за одбрану земље.

Истовремено, сваком податку који представља војну тајну наведеним правилником је прописан један од следећих степена тајности: „строго поверљиво“

во“; „поверљиво“ и „интерно“, и то:

1. строго поверљиви су они подаци за које се утврди да су нарочито значајни за Војску, чијим би откривањем могле наступити теже штетне последице за Војску и њене припреме за одбрану земље (члан 13.), а који се односе на :

- планове употребе Војске и њених здружених састава;
- организацију и формацију команди, установа и јединица Војске;
- мобилизацијска документа;
- послове оперативних центара и сталних оперативних дежурстава;
- извештаје и анализе о борбеној готовости команди, установа и јединица Војске;
- укупан распоред и бројно стање јединица и ватрену способност јединица и појединих значајних врста наоружања;
- анализе и оцене стања и попуњености јединица борбеном техником, муницијом и минско-експлозивним и погонским средствима;
- мирнодопску и ратну попуњу официрима, подофицирима и војницима, као и збирне податке о професионалном саставу;
- планове за уређење територије за потребе појединих јединица и њихову реализацију;
- војне и друге значајне објекте;
- збирне прегледе наоружања и војне опреме;
- специјална техничка средства и њихову примену, као и на наоружање и војну опрему од посебног значаја;
- набавке у земљи, увоз и извоз предмета наоружања и војне опреме од посебног значаја;
- научноистраживачке послове и научне и техничке проналаске који су од посебног значаја за наоружавање и опремање Војске;
- процене, замисли и решења у извођењу борбених дејстава у појединим варијантама одбране;
- планове и елаборате за вежбе здружених састава и обуку команди, установа и јединица Војске;
- послове криптозаштите који нису утврђени као државна тајна и стручне материјале који се користе за наставне и друге службене потребе и на организацију система веза;
- збирне статистике и евиденције за потребе Војске;
- одређене топографске послове и поједине топографске и специјалне карте;
- обавештајне и контраобавештајне послове обавештајних органа и органа безбедности, који нису утврђени као државна тајна, као и

- 
- извештаје о налазима инспекцијских органа Војске.

2. поверљиви су они подаци који се односе на делатност и задатке команди, установа и јединица Војске и одређених организација које раде за потребе Војске, средства наоружања, војну опрему и војне објекте за које су утврди да би њиховим откривањем могле наступити штетне последице за извршавање задатака команди, установа и јединица Војске (члан 14.), а који се нарочито односе на:

- формације мирнодопских команди, установа и јединица Војске;
- бројна стања команди, установа и јединица Војске;
- врсте и количине средстава наоружања јединица, техничку опрему и резерве борбених средстава којима располажу те јединице;
- тактичко-техничке карактеристике појединих врста наоружања и војне опреме;
- мирнодопску локацију јединица;
- објекте значајне за поједине команде, установе и јединице Војске, а који нису утврђени као строго поверљиви;
- поједине прописе, правила, инструкције и друго за које надлежни органи одреде;
- материјално-финансијско пословање (значајнији подаци);
- анализе и извештаје о обуци;
- одређене кадровске и персоналне послове, као и
- студије и прописе који се односе на потенцијалне противнике и разматрања могуће употребе њихових оружаних снага.

3. интерни су они подаци од значаја за Војску који су намењени за службене потребе лица на служби у Војсци, а који по свом значају не представљају податке стого поверљивог или поверљивог карактера (члан 15.).

Решењем о утврђивању података од интереса за одбрану земље који се сматрају тајним подацима из делокруга Министарства одбране и одређивању мера и поступака за њихову заштиту (члан 6), државном тајном се сматрају и:

- смернице за одбрану Републике Србије од агресије;
- одлука Владе Републике Србије о мерама приправности и упутство Министарства одбране за примену Одлуке о мерама приправности;
- појединачни планови приправности државних органа, преду-

---

зећа и других правних лица;

- планови перспективног развоја и модернизације система за одбрану земље;
- планови посебних мера безбедности којима се штите тајни подаци, послови и задаци од посебног интереса за одбрану;
- прописи и документи из области криптозаштите;
- упутство Министарства одбране о заштити и припреми планова опште мобилизације и организовања припрема за одбрану, као и
- друга документа која одреди старешина организационе јединице Министарства одбране, у складу са критеријумима које прописује Влада Републике Србије.

Овим решењем прописано је и то који се подаци сматрају службеном тајном, при чему је сваком податку који представља службену тајну, зависно од значаја, одређен један од следећих степена тајности: „строго поверљиво“; „поверљиво“ и „интерно“, и то:

1. службеном тајном „строго поверљиво“ се сматрају и подаци који се односе на:

- појединачне планове мобилизације и организовање припрема за одбрану државних органа, установа, предузећа и других правних лица;
- наредбе о изради прегледа организацијско-мобилизацијског развоја Министарства одбране и јединица и установа Министарства одбране у миру и рату, као и наредбе о организацијско-мобилизацијском развоју Министарства одбране;
- планове и елаборате за вежбе јединица Министарства одбране у сарадњи са јединицама Војске;
- извештаје и евиденције о укупном распореду и попуни јединица Министарства одбране војним обвезницима, наоружањем, војном и другом опремом;
- планове набавки у земљи, увоз и извоз предмета наоружања и војне опреме од посебног значаја за одбрану земље;
- средњорочне и годишње планове развоја, опремања и припрема за одбрану државних органа, предузећа и других правних лица и јединица које образује Министарство одбране;
- средњорочне и годишње планове материјалног опремања Војске;
- средњорочне и годишње планове изградње војних непокретности;
- средњорочне и годишње планове научно-истраживачког и

---

развојног рада за потребе Војске;

- инструкције о избору и уређењу ратних локација;
- информације, извештаје, анализе и закључке из области одбране, припремљених за потребе надлежних државних органа;
- материјале из области унутар војне проблематике који се одnose на обуку, вежбе, снабдевање и финансирање Војске;
- стручне материјале који се употребљавају за наставне и друге службене потребе у области веза и криптозаштите који нису утврђени као државна тајна;
- одлуке Владе о организовању припрема за израду Плана одбране земље;
- документацију (пројектна, урбанистичка и остала) и друге податке о комплексима и објектима од посебног значаја за одбрану земље, као и
- другу документацију коју одреди старешена организационе јединице Министарства одбране, у складу са критеријумима које је прописала Влада.

2. службеном тајном „поверљиво“ се сматрају:

- уредбе Владе о организовању веза за потребе државних органа и режиму њихове употребе за време ратног или ванредног стања;
- евиденције о врстама и капацитетима природних и вештачких склоништа за заштиту становништва и материјалних добара у рату;
- месечне и периодичне анализе и извештаји о текућем извршавању годишњих планова, задатака и финансирања Министарства одбране и Војске;
- закључени уговори са предузећима за позадинско обезбеђење мобилизације и снабдевање у рату;
- спискови дужности професионалних официра и подофицира распоређених ван Војске;
- анализе и извештаји о обучавању и оспособљавању грађана за одбрану земље;
- основе планова и програма обучавања за одбрану земље и оспособљавања на пословима одбране земље;
- подаци и евиденције из катастра непокретности за потребе одбране, као и
- друга документа која одреди старешина органа јединице Министарства одбране, у складу са критеријумима које је прописала Влада.

3. службеном тајном „интерно“ се сматрају подаци који се односе на извршавање службених потреба лица на служби у Министарству одбране, а која

---

се без одобрења надлежног старешине не могу саопштавати или објављивати

Законом о Војсци Србије (члан 38.) прописано је да је војно лице дужно да чува државну, војну, службену и пословну тајну.

Законом о државним службеницима (члан 24.) прописано је да је државни службеник дужан да чува службену или другу тајну одређену законом или другим прописом.

Законом о полицији (члан 136. став 2.) утврђено је да се службеним подацима сматрају сви подаци који су законом или прописом одређени као поверљиви, подаци и документи који су општим актом одређени као поверљиви, подаци и документи одређени од стране других органа или правних лица као поверљиви, као и мере, радње, подаци и извори информација чије би саопштавање било штетно.

Истовремено, овим законом (члан 136.) утврђено је да је полицијски службеник дужан да чува службене податке за које је сазнао у служби или поводом вршења службе.

Законом о Безбедносно - информативној агенцији (члан 23. став 1.) утврђено је да је припадник БИА дужан да чува податке БИА који представљају државну, службену, војну или пословну тајну.

Законом о привредним друштвима (члан 38.) прописано је да се пословном тајном сматра информација о пословању која је одређена оснивачким актом, актом и уговором ортака или уговором чланова друштва, односно оснивачким актом или статутом акционарског друштва, за које очигледно да би проузроковало знатну штету привредном друштву ако дође у посед трећег лица.

Пословна тајна која садржи податак од значаја за одбрану сматра се тајним податком одбране и штити сагласно одговарајућим одредбама Уредбе о критеријумима за утврђивање података значајних за одбрану земље који се морају чувати као државна или службена тајна и о утврђивању задатака и послова од посебног значаја за одбрану земље које треба штитити применом посебних мера безбедности (члан 9.).

Важећом законском регулативом уређено је питање и других врсти тајни:

Законом о патентима (члан 102.) утврђено је да је поверљиви проналазак

---

сваки проналазак који је значајан за одбрану и безбедност Републике Србије.

Законом о кривичном поступку (члан 261.) прописано је да се истражна тајна одређује на основу наређења службеног лица које предузима истражне радње због заштите интереса поступка, чувања тајни, јавног реда, разлога морала или заштите личног или породичног живота оштећеног или окривљеног лица.

Законом о јавном информисању (члан 32.) утврђено је да новинар није дужан да открије податке у вези са извором информације, осим ако се подаци односе на кривично дело, за које је забрањена казна затвора најмање 5 година (новинарска тајна).

Законом о адвокатури (члан 15. став 3.) прописано је да је адвокат дужан да чува као тајну оно што му је странка поверила (адвокатска тајна).

Законом о здравственој заштити (члан 30.) прописана је забрана да надлежни здравствени радник саопшти другим лицима личне податке о пацијенту који се односе на његово здравствено стање (лекарска тајна).

Законом о условима за обављање психолошке делатности (члан 4.) утврђено је да подаци о личности који могу да штете угледу и интегритету личности или су личне природе, а које психолог сазна у обављању делатности, представљају професионалну тајну.

Законом о црквама и верским заједницама (члан 4. став 7.) утврђено је да свештеник не може бити позван да сведочи о чињеницама и околностима које је сазнао приликом исповести (свештеничка тајна).

## **Ограничење приступа информација**

Чланом 9. Закона о приступу информацијама од јавног значаја право на приступ одговарајућим информацијама може се ограничити због: националне безбедности; јавне безбедности; комерцијалних и других економских, јавних и приватних интереса; економске, монетарне и девизне политике земље; спречавања, истраживања и процесуирања кривичних дела; приватности и других личних права; обраде и доношења службених аката, као и угрожавања живота, здравља, сигурности или имовине грађана.

---

## Кривична и дисциплинска одговорност против лица која су угрозила тајност података

Кривично - правна заштита тајних података прописана је Кривичним законом Републике Србије, и то:

*Члан 315 – шпијунажа*

*(1) Ко тајне војне, економске или службене податке или документа саопшти, преда или учини доступним страном држави или лицу које им служи, казниће се затвором од три до петнаест година.*

*(2) Ко за страну државу или организацију ствара обавештајну службу у Србији или њом руководи, казниће се затвором од пет до петнаест година.*

*(3) Ко ступи у страну обавештајну службу, прикупља за њу податке или на други начин помаже њен рад, казниће се затвором од једне до десет година.*

*(4) Ко прибавља тајне податке или документе у намери да их саопшти или преда страном држави, страном организацији или лицу које им служи, казниће се затвором од једне до осам година.*

*(5) Ако су услед дела из ст. 1. и 2. овог члана наступиле тешке последице за безбедност, економску или војну моћ земље, учинилац ће се казнити затвором најмање десет година.*

*(6) Тајном се сматрају оно војни, економски или службени подаци или документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени тајним, а чије би одавање проузроковало или би могло да проузрокује штетне последице за безбедност, одбрану или за политичке, војне или економске интересе земље.*

*Члан 316. – одавање државне тајне*

*(1) Ко неовлашћено непозваном лицу саопшти, преда или учини доступним податке или документе који су му поверени или до којих је на други начин дошао, а који представљају државну тајну, казниће се затвором од једне до десет година.*

*(2) Ко другом лицу саопшти податке или документе за које зна да су државна тајна, а до којих је противправно дошао, казниће се затвором до пет година.*

*(3) Ако је дело из става 1. овог члана извршено за време ратног стања или ванредног стања или је довело до угрожавања безбедности, економске или војне моћи Србије, учинилац ће се казнити затвором од три до петнаест година.*

*(4) Ако је дело из става 1. овог члана учињено из нехата, учинилац ће се казнити затвором од шест месеци до пет година.*

*(5) Државном тајном сматрају се подаци или документи који су законом,*

---

другим прописом или одлуком надлежног органа донесеним на основу закона проглашени државном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за безбедност, одбрану или за политичке, војне или економске интересе Србије.

(6) Државном тајном, у смислу става 5. овог члана, не сматрају се подаци или документи који су управљени на тешке повреде основних права човека, или на угрожавање уставног уређења и безбедности Србије, као и подаци или документи који за циљ имају прикривање учињеног кривичног дела за које се по закону може изрећи затвор од пет година или тежа казна.

*Члан 415. – одавање војне тајне*

(1) Ко неовлашћено другом саопштити, преда или на други начин учини доступним податке који представљају војну тајну или прибавља такве податке у намери да их преда непозваном лицу, казниће се затвором од три месеца до пет година.

(2) Ако је дело из става 1. овог члана учињено из користорубља или у погледу нарочито поверљивих података или ради објављивања или коришћења података у иностранству, учинилац ће се казнити затвором од једне до осам година.

(3) Ако је дело из става 1. овог члана учињено из нехата, учинилац ће се казнити затвором до три године.

(4) Војном тајном сматрају се подаци који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени војном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за војску Србије или одбрану или безбедност земље

(5) Војном тајном, у смислу става 4. овог члана, не сматрају се подаци или документи који су управљени на тешке повреде основних права човека, или на угрожавање уставног уређења и безбедности Србије, као и подаци или документи који за циљ имају прикривање учињеног кривичног дела за које се по закону може изрећи затвор од пет година или тежа казна.

За кривично дело из ст. 1 и 3. овог члана, ако је извршено за време ратног стања, оружаног сукоба или ванредног стања, учинилац ће се казнити казном затвора од две до десет година.

За кривично дело из става. 2 . овог члана, ако је извршено за време ратног стања, оружаног сукоба или ванредног стања, учинилац ће се казнити казном затвора од три до петнаест година.

*Члан 369. – одавање службене тајне*

(1) Службено лице које неовлашћено другом саопштити, преда или на други начин учини доступним податке који представљају службену тајну или које прибавља такве податке у намери да их преда непозваном лицу, казниће се затвором од три месеца до пет година.

(2) Ако је дело из става 1. овог члана учињено из користорубља или у погледу нарочито поверљивих података или ради објављивања или коришћења података у иностранству, учинилац ће се казнити затвором од једне до осам година.

(3) Ако је дело из става 1. овог члана учињено из нехата, учинилац ће се казнити затвором до три године.

(4) Службеном тајном сматрају се подаци или документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени службеном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за службу.

(5) Службеном тајном, у смислу става 4. овог члана, не сматрају се подаци или документи који су управљени на тешке повреде основних права човека, или на угрожавање уставног уређења и безбедности Србије, као и подаци или документи који за циљ имају прикривање учињеног кривичног дела за које се по закону може изрећи затвор од пет година или тежа казна.

(6) Одредбе ст. 1. до 4. овог члана примениће се и према лицу које је одало службену тајну пошто му је престало својство службеног лица.

#### Члан 337. – повреда тајности поступка

(1) Ко неовлашћено открије оно што је сазнао у судском, прекршајном, управном или другом законом прописаном поступку, а што се по закону не може објавити или одлуком суда или другог надлежног органа проглашеног као тајна, казниће се новчаном казном или затвором до једне године.

#### Члан 240. – одавање пословне тајне

(1) Ко неовлашћено другом саопштити, преда или на други начин учини доступним податке који представљају пословну тајну или ко прибавља такве податке у намери да их преда непозваном лицу, казниће се затвором од три месеца до пет година.

(2) Ако је дело из става 1. овог члана учињено из користорубља или у погледу нарочито поверљивих података, учинилац ће се казнити затвором од две до десет година.

(3) Ко дело из става 1. овог члана учини из нехата, казниће се затвором до три године.

(4) Пословном тајном сматрају се подаци и документи који су законом, другим прописом или одлуком надлежног органа донесеним на основу закона проглашени пословном тајном и чије би одавање проузроковало или би могло да проузрокује штетне последице за предузеће, или други субјект привредног пословања.

#### Члан 298. – оштећење рачунарских података и програма

(1) Ко неовлашћено избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм, казниће се новча-

---

ном казном или затвором до једне године.

(2) Ако је делом из става 1. овог члана проузрокована штета у износу преко 45.000 динара, учинилац ће се се казнити затвором од три месеца до три године.

(3) Ако је делом из става 1. овог члана проузрокована штета у износу преко 1.500.000 динара, учинилац ће се се казнити затвором од три месеца до пет година.

(4) Уређаји и средства којима је учињено кривично дело из ст. 1 и 2. овог члана, ако су у својини учиниоца, одузеће се.

#### Члан 299.- рачунарска саботажа

Ко унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте, казниће се затвором од шест месеци до пет година.

#### Члан 300. – прављење и уношење рачунарских вируса

(1) Ко направи рачунарски вирус у намери његовог уношења у туђ рачунар или рачунарску мрежу, казниће се новчаном казном или затвором до шест месеци.

(2) Ко унесе рачунарски вирус у туђ рачунар или рачунарску мрежу и тиме проузрокује штету, казниће се новчаном казном или затвором до две године

(3) Уређаји и средства којима је учињено кривично дело из ст. 1 и 2. овог члана одузеће се.

#### Члан 301. – рачунарска превара

(1) Ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године.

(2) Ако је делом из става 1. овог члана прибављена имовинска корист која прелази износ од 45.000 динара, учинилац ће се казнити затвором од једне до осам година.

(3) Ако је делом из става 1. овог члана прибављена имовинска корист која прелази износ од 1.000.000 динара, учинилац ће се казнити затвором од две до десет година.

(4) Ко дело из става 1. овог члана учини само у намери да другог оштети,

---

*казниће се новчаном казном или затвором до шест месеци.*

*Члан 302. – неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података*

*(1) Ко се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци.*

*(2) Ко употреби податак добијен на начин предвиђен у ставу 1. овог члана, казниће се новчаном казном или затвором до две године.*

*(3) Ако је услед дела из става 1. овог члана дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице, учинилац ће се казнити затвором до три године.*

*Члан 303. – спречавање и ограничавање приступа јавној рачунарској мрежи*

*(1) Ко неовлашћено спречава или омета приступ јавној рачунарској мрежи, казниће се новчаном казном или затвором до једне године.*

*(2) Ако дело из става 1. овог члана учини службено лице у вршењу службе, казниће се затвором до три године.*

*Члан 304. – неовлашћено коришћење рачунара или рачунарске мреже*

*(1) Ко неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист, казниће се новчаном казном или затвором до три месеца.*

*(2) Гоњење за дело из става 1. овог члана предузима се по приватној тужби.*

*Законом о архивској грађи (члан 31.) прописано је да „Ко присвоји, прикрије, у већој мери оштети, уништи или на други начин учини неупотребљивим архивску грађу или регистратурски материјал или изнесе у иностранство без претходног одобрења надлежног државног органа, односно организације или омогући другом да то учини, казниће се за кривично дело затвором три месеца до пет година“.*

На основу напред изнетог, може се констатовати следеће:

1. У Републици Србији функционишу четири аутономна сиситема заштите тајних података сагласно законом утврђеним надлежностима Министарства одбране, Министарства спољних послова, Министарства унутрашњих послова и Безбедносно-информативне агенције.

---

2. Законска, односно подзаконска регулатива из области заштите тајних података од значаја за одбрану, безбедност и других виталних интереса Републике Србије у највећем и најзначајнијем делу је наслеђена из периода функционисања бивше Савезне Републике Југославије.

3. Уочљиво је да одређена питања из области заштите тајних података нису решена на рационалан начин, с обзиром да се иста материја уређивала кроз више подзаконских аката (уредбе, решења, правилници и упутства).

4. Чињеница да су многа законска и подзаконска решења преузета из прошлих законодавних система указује на потребу реформе ове области, у складу са савременим стандардима који су установљени у области заштите и приступа тајним подацима у земљама ЕУ и другим развијеним државама.

Неодржива је ситуација у којој се још увек суочавамо са неодговарајућим класификацијама тајних података, непостојањем основних начела у вези приступа и заштите тајних података, адекватне безбедносне провере „овлашћених лица“ којима је дозвољен увид у тајне податке и др.

Из тих разлога, у Републици Србији су интензивирани активности на изради и доношењу новог системског Закона о заштити тајних података, на начин који ће у потпуности и у складу са међународно прихваћеним стандардима обезбедити остварење и заштиту интереса Републике Србије у овој области.

## **ОСНОВНИ ЕЛЕМЕНТИ ЗА ИЗРАДУ ЗАКОНА О ЗАШТИТИ ТАЈНИХ ПОДАТАКА**

### **Предмет закона**

Полазећи од суштинских питања која се односе на област заштите и коришћења тајних података, овим законом неопходно је:

1) уредити основна начела и принципе на којима се заснива закон, у складу са Уставом и међународним конвенцијама, споразумима и уговорима и уз уважавање међународно установљених стандарда заштите тајних података који су обавезујући за приступ ЕУ, односно усклађивање националног законодавства са прописима и стандардима ЕУ који регулишу област заштите тајних података. Уједно, потребно је изградити правне, организационе, структуралне и друге капацитете ради доношења подзаконских аката и

---

даље стандардизације у области заштите тајних података.

2) дефинисати појам „тајног податка“, односно податка (који може бити у облику документа, електронског записа, информације, објекта, личности, активности, послова и слично) од значаја за заштиту националне безбедности и других виталних интереса Републике Србије и њених грађана, као и њихов настанак, означавање, употребу, размену, архивирање и уништавање, у складу са међународно установљеним процедурама, правилима и стандардима.

Истовремено, дефинисати и друге појмове као на пример: „подаци значајни за одбрану“ или неку другу област; „индустријска безбедност“; „безбедносне провере и сертификарање“; „систем регистрације“; „безбедност податка“; „криптографска заштита“; „централни регистар“; „безбедност информационих система и рачунарских мрежа“; „мере заштите“, као и остале суштинске појмове који ће се користити у закону;

3) уредити питање контроле примене закона од стране законодавне, извршне и судске власти, као и јавности;

4) уредити на националном нивоу јединствен поступак за одређивање критеријума и услова за класификовање тајних података, као и за управљање и заштиту тајних података преко дистрибуције и регистарског система тајних података;

5) одредити надлежност и задатке државних органа, односно овлашћене носиоце за рад са тајним подацима;

6) утврдити листе корисника по појединим степенима тајности и приступу свим степенима тајности, са или без безбедносне провере;

7) утврдити поступак безбедносне провере и издавања безбедносног сертификата за приступ тајним подацима, као и националног тела надлежног за ове послове, имајући при томе у виду и специфичности Министарства одбране, Министарства унутрашњих послова и Безбедносно-информативне агенције;

8) одредити носиоца, односно носиоце надзора над применом овог закона и других прописа који се односе на заштиту тајних података;

9) уредити поступак уступања, размене и узајамне заштите тајних података са другим државама и међународним организацијама и институцијама;

---

10) утврдити права и обавезе државних органа, правних и физичких лица која се односе на заштиту тајних података;

11) уредити и друга питања од значаја за безбедност и заштиту тајних података.

### **Значење израза „тајни податак“**

Тајни податак је сваки податак, информација, материјал, објекат, личност, активност, посао, задатак или документ (електронски или писани запис) од значаја за заштиту националне безбедности и виталних интереса државе и њених грађана и чије би откривање, односно злоупотреба могла угрозити те интересе.

Поред већ стандардног извора, и у нашем законодавству још увек присутног става, да се тајним подацима сматрају они који се односе на националну безбедност, одбрану, спољне послове, обавештајне и контраобавештајне активности, научна истраживања, економска и финансијска питања, као и професионалну делатност, приликом предлагања одговарајућих решења неопходно је сагледати и друге области које захтевају адекватну заштиту података, као на пример криптозаштита, индустријска безбедност, заштита информатичких и комуникационих система и др.

При томе, у изради закона мора се имати у виду међународно општеприхваћена правна регулатива, али и технички стандарди (у вези информатичко-комуникационих система, преноса података и слично) у означавању тајности података према којој не постоје врсте тајности (војна, службена и пословна тајна), већ се тајни подаци разврставају по областима (национална и јавна безбедност; одбрана; спољни послови; обавештајне и безбедносне активности и сл.).

Прихватањем наведеног стандарда стекли би се услови за једнообразне, усклађене и функционалне процедуре у међународној размени и узајамној заштити тајних података.

Истовремено, законом се мора прописати да се тајним податком не може сматрати податак којим би се прикривала намера или извршење кривичног дела, прекорачење или злоупотреба службених овлашћења, односно било које друго поступање супротно Уставу и закону.

Полазећи од чињенице која се односи на имплементацију закона, односно да су неке од дефиниција или значења, већ садржани у више важећих зако-

---

на (нпр. Кривични законик, Закон о архивској грађи, Закон о привредним друштвима, Закон о информационим системима, Закон о одбрани, Закон о полицији и др.), указује се на потребу уподобљавања терминологије, израза, дефиниција, значења, као и процедура и поступака на начин који ће бити у складу са овим законом.

### **Означавање тајних података**

Законом о заштити тајних података неопходно је прописати обавезу да се тајни подаци означавају са једним од четири међународно прихваћених степена тајности, односно да називи наших степена тајности аналогно-суштински одговарају истим („TOP SECRET“ – државна тајна; „SECRET“ – строго поверљиво; „CONFIDENTIAL“ – поверљиво, као и „RESTRICTED“ – интерно), уз евентуалну могућност истовременог и паралелног коришћења нашег и међународно установљеног израза у означавању податка са неопходним степеном тајности.

На тај начин, у потпуности би се омогућила ефикасна и рационална размена података са другим државама, међународним организацијама и институцијама, сагласно потписаним међународним, односно ратификованим уговорима, споразумима и другим актима.

С тим у вези, неопходно је на националном нивоу одредити и критеријуме тајности података према степену тајности у смислу који подаци представљају државну тајну, строго поверљив, поверљив или интерно класификован материјал у односу на области које ће се законом уредити (одбрана, спољни послови и слично), а односе се на националну безбедност и заштиту виталних интереса Републике Србије и њених грађана.

Такође се може уочити да међународне безбедносне и друге организације у својим регулативима крајње уопштено одређују процедуре размене тајних података и да приликом усклађивања националног законодавства са њиховом регулативом не инсистирају на квалитету података који ће бити предмет размене, већ је то препуштено слободној процени и нивоу успостављене сарадње у области безбедности и одбране, као и у другим областима.

### **Овлашћење за означавање тајних података**

При одређивању лица овлашћених за означавање степена тајности у овом закону, морају се имати у виду и одредбе Устава Републике Србије о носиоцима законодавне, извршне и судске власти и носиоцима демократских институција; решења садржана у законима о Влади, министарствима, судо-

---

вима, државној управи, аутономној покрајини, локалној самоуправи, управним окрузима, одбрани, војсци, полицији, предузећима, јавним установама, као и решења садржана у одговарајућим другим прописима.

При одређивању податка који ће се означити степеном тајности неизоставно се поставља питање објективности, односно субјективности у одлучивању да ли конкретан податак подлеже степену тајности и ком нивоу. Поред тога, предметним законом је потребно обезбедити и одговарајуће механизме контроле рада на заштити тајности података.

Међутим, оно што је свакако битно јесте квалитативна процена података који морају бити заштићени, као на пример подаци из области националне безбедности и одбране, планови, поступци и мере које ће се предузети ради спречавања или дешавања нежељеног догађаја.

Питање које код нас, уместо стручне, често има политичку позадину јесте да ли су савремени европски стандарди и процедуре у овој области супротни националној безбедности и виталним интересима Републике Србије.

Овде је нужно рећи да се применом ових стандарда национална законодавства не условљавају нити за тим постоји било каква потреба да се у овој области прописује оно што је супротно националним интересима.

Размена тајних података као скуп административних процедура подразумева пре свега техничко-административни и методолошки аспект размене тајних података без уласка у саму садржину тајних података и њихову квалитативну материјалну процену и анализу

Из напред изнетог може се констатовати да је овде реч о усклађивању националног законодавства са међународно прихваћеном и стандардизованом процедуром размене и заштите тајних података.

### **Приступ тајним подацима**

Једно од битних питања које ће се регулисати законом јесте одређивање лица која ће без безбедносне провере, односно издавања сертификата за приступ тајним подацима, имати приступ тајним подацима свих или појединих степена тајности.

Законом је потребно утврдити да приступ свим тајним подацима, без безбедносне провере и издавања сертификата, имају државни и други функционери који су Уставом Републике Србије одређени као највиши носиоци

---

законодавне, извршне и судске власти.

С друге стране, носиоци демократско- цивилне контроле вероватно ће захтевати да приступ тајним подацима има што већи број корисника ради спречавања монопола или евентуалних злоупотреба, што може бити разумљиво, али је основна дилема да ли широк круг корисника може и у којој мери угрозити националну безбедност и виталне интересе државе.

Из тих разлога поставља се питање којим се носиоцима државних и других дужности може омогућити безуслован приступ подацима свих степена тајности, односно који је то ниво и опсег тајних података који би се омогућио сразмерно нивоу одговорности носиоца јавне функције, односно дужности а што не би било супротно националним интересима у области одбране и безбедности .

Сагледавањем упоредног искуства може се уочити да је ово питање регулисано на начин да је лицима која обављају највише државне и друге функције (председници република, скупштина, влада, судова и др.) омогућен безуслован приступ тајним подацима свих степена тајности, односно да та лица имају приступ само тајним подацима неопходним за обављање послова, сагласно Уставом и законом утврђеним надлежностима.

Слична питања поставиће се предлагачу закона приликом одређивања лица којима ће без безбедносне провере и сертификата бити одобрен приступ тајним подацима одговарајућег степена тајности.

### **Безбедносна провера и издавање сертификата за приступ тајним информацијама**

У изради одговарајућих решења по питању безбедносне провере указује се на следеће:

Безбедносна провера физичких и правних лица као обавезан поступак за лица која су или могу бити у контакту са тајним подацима не може бити спорна, као ни њен обим у односу на степен доступности тајних података.

При томе треба имати у виду специфичности делокруга рада појединих државних органа који у складу са утврђеним надлежностима имају посебну одговорност у области заштите тајних података, као на пример Министарство одбране, Министарство унутрашњих послова, Министарство спољних послова и др.

С обзиром на ширину области заштите тајних података неоспорно је да пи-

---

тање безбедносне провере лица којима је дозвољен приступ и коришћење тајних података захтева и законско уважавање селективног приступа са аспекта одређивања органа надлежног за вршење безбедносне провере.

Тако на пример, разумљиво је да безбедносну проверу за потребе Министарства одбране обавља Војнобезбедносна агенција у сарадњи са Безбедносноинформативном агенцијом и Министарством унутрашњих послова.

Исто тако, у складу са међународно установљеним стандардима и процедурама, законом је неопходно уподобити поступак и издавање безбедносних сертификата за приступ тајним подацима одговарајућег степена, као и њихов изглед и садржај у смислу општеприхваћених међународних процедура сертификације, чиме би се омогућило учешће припадника Војске Србије у бројним међународним активностима (мировне операције, школовања, учешће на међународним војним вежбама, конференцијама „затвореног“ типа и слично).

### **Орган надлежан за службене евиденције, издавање сертификата и међународну размену података**

Законом о заштити тајних података биће прописан поступак за подношење захтева за издавање безбедносног сертификата, садржина безбедносних упитника, дужина трајања безбедносне провере, доношење решења о издавању сертификата са роком важења, поступак у случају одбијања захтева и друго.

Исто тако, законом ће се утврдити поступак и начин вођења службене евиденције о донетим решењима, личним подацима подносиоца захтева, издатим сертификатима, нерешеним захтевима, праћења стања у области заштите тајних података, спровођења физичких, организационих и техничких стандарда заштите тајних података, као и других питања од значаја из ове области.

Суштинско питање јесте одређивање органа надлежног за обављање напред наведених и других послова који се односе на заштиту тајних података; ко га образује; на чији предлог и ко именује и разрешава функционера који ће руководити тим органом; ко врши надзор, као и друга питања која се односе на рад и функционисање тог органа.

При томе треба имати у виду извесност да ће се у том органу налазити и централни регистар тајних података добијених из међународне размене.

---

## Надзор

Изузетно значајно питање јесте и питање одређивања органа-носиоца вршења надзора над спровођењем закона и других прописа којим се регулише област заштите тајних података, као и законом утврђених овлашћења у вршењу надзора.

Код овог закона, питање носиоца вршења надзора зависиће од решења у вези образовања органа који ће обављати послове службене евиденције, издавања сертификата, међународне размене података и других послова од значаја из области заштите тајних података, у складу са утврђеним надлежностима.