



## ПРАВИЛНО ПРИМЕЊЕНА ТАЈНОСТ ТЕМЕЉ МОДЕРНЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И ДЕМОКРАТСКЕ ОДГОВОРНОСТИ

Демократско друштво заснива се на транспарентности као правилу и тајности као изузетку. Правилно примењена тајност није механизам затварања државе, већ инструмент заштите јавног интереса, институционалне стабилности и националне безбедности. Она се може оправдати искључиво у случајевима када би откривање информације проузроковало стварну, конкретну и вероватну штету, а не када служи као изговор за прикривање неправилности, избегавање надзора или управљање јавном перцепцијом.

Прекомерно одређивање тајности не само што подрива поверење у институције, већ и ослабљује саму безбедносну архитектуру, јер замагљује стварно осетљиве податке у мору непотребно класификоване документације.

**1. ШТА ЈЕ ЦИЉ РЕЖИМА ЗАШТИТЕ ТАЈНОСТИ ПОДАТАКА?** - није прикривање и скривање информација, већ прецизна, привремена и образложена заштита података чије би откривање могло нанети стварну, конкретну и вероватну штету интересима Републике Србије, у области националне безбедности, одбране, спољне политике, обавештајно-безбедносних послова или стабилног функционисања државе. У модерном безбедносном оквиру тајност делује као контролисани заштитни механизам, а не као средство спречавања јавности да располаже информацијама од општег значаја. Квалитетно дефинисано ограничење приступа омогућава:

- очување интегритета оперативних активности,
- спречавање стварања оперативних рањивости које би противник могао да искористи,
- заштиту међународних обавеза и односа са партнерским службама,
- чување безбедносних капацитета државе у условима динамичних хибридних претњи – при чему се ускраћивање приступа сматра неопходним искључиво када задовољава тест јавног интереса у демократском друштву.

Тајност мора бити изузетак, а не правило – управо зато што прекомерно означавање тајност слаби њену суштинску безбедносну и заштитну функцију.

**2. У ЧЕМУ ЈЕ ПРОБЛЕМ?** - У пракси, режим заштите тајности се често злоупотребљава, што доводи до прекомерног одређивања тајности података (over-classification). Ова појава није специфична само за Републику Србију, присутна је и у бројним државама региона и шире. Последице ове праксе су:

- „Замагљивање“ стварних безбедносних приоритета - када је готово сва документација „тајна“, тешко је разликовати шта је заиста критично, што умањује оперативну ефикасност и замењује стручну процену формализмом.



## ПРАВИЛНО ПРИМЕЊЕНА ТАЈНОСТ ТЕМЕЉ МОДЕРНЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И ДЕМОКРАТСКЕ ОДГОВОРНОСТИ

- **Ограничавање демократског надзора** - парламент, грађани и медији остају без података о трошењу јавних средстава, стратешким пројектима и набавкама, што подрива поверење и умањује транспарентност.
- **Прикривање неправилности** - у пракси се дешава да се уговори, извештаји о ревизији или подаци о потенцијалним спорним пословима проглашавају тајним без било какве стварне, ризиком засноване процене.
- **Смањење међуинституционалне сарадње** - прекомерна тајност онемогућава проток информација чак и између државних органа са законски утврђеним надлежностима; то води фрагментацији система и смањује капацитет реаговања у кризи.

Овакве праксе не само што компромитују националну безбедност, већ нарушавају и кључни принцип, да тајност штити државу, а не институционалне или појединачне интересе.

**3. ШТА ЗАКОН ЗАПРАВО ЗАХТЕВА?** - Према члану 8. Закона о тајности података (ЗТП), податак се може одредити као тајан искључиво ако су испуњена три услова:

1. **Односи се на законски дефинисан интерес државе** - стратешки безбедносни, одбрамбени, дипломатски или други у закону предвиђени интерес од значаја за Републику Србију.
2. **Његово откривање би нанело стварну, конкретну и вероватну штету** - процена мора бити заснована на ризику, поткрепљена аргументима, а не на општој претпоставци или субјективној процени.
3. **Заштита тог интереса претеже над јавним интересом да се до информације дође** - у демократској пракси, ово је најсложенији део примене, јер захтева активну анализу односа користи и штете.

Члан 3. ЗТП недвосмислено забрањује одређивање тајности ради **прикривања кривичних дела, злоупотребе службеног положаја или неправилности**. Ово је основни правни и етички принцип злоупотребљена тајност престаје да буде инструмент безбедности и постаје механизам злоупотребе моћи.

**4. КАКО СПРЕЧИТИ ПРЕКОМЕРНУ ТАЈНОСТ?** - Кључни кораци за исправну примену режима заштите тајности:

- **Обавезна процена ризика пре сваке одлуке о одређивање тајности**. Процена мора бити документована, структурисана и заснована на конкретним сценаријима штете (threat modeling), а не на општим формулацијама попут „могло би да нашкоди држави“.



## ПРАВИЛНО ПРИМЕЊЕНА ТАЈНОСТ ТЕМЕЉ МОДЕРНЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И ДЕМОКРАТСКЕ ОДГОВОРНОСТИ

- **Образложење одлуке – јасно, конкретно и у складу са чланом 8. ЗТП** Образложења која не садрже објашњење природе претње, типа штете и њене вероватноће, ни формално ни суштински не испуњавају захтев закона.
- **Примена принципа „најнижег неопходног степена заштите“.** Одређивање степена тајности мора бити пропорционална ризику, ако је осетљив само један мањи део документа, тајним податком се проглашава тај део, а не целина у складу са чланом 12. став 3. ЗТП
- **Редовна ревизија и опозив тајности.** Тајност није трајна, већ динамична категорија. Када ризик престане, тајност престаје. Многе злоупотребе проистичу из чињенице да се тајност никада не преиспитује.
- **Јачање надзорних механизма.** Канцеларија Савета и Министарство правде и морају имати јасне и оперативне механизме контроле, од ревизије одлука до надзора над институцијама са повећаним ризиком прекомерног одређивања тајности.

Кључну улогу у овом процесу има Канцеларија Савета за националну безбедност и заштиту тајних података, која у оквиру својих надлежности може захтевати ванредну процену тајности и сама донети одлуку о њеном опозиву (члан 24. ЗТП).

Додатне могућности за опозив тајности произилазе из појачане законске улоге Повереника за слободан приступ информацијама од јавног значаја. Повереник не само да утврђује неправилности, већ својим решењем ствара правни основ да надлежни орган опозове тајност (члан 25. ЗТП). На тај начин успоставља се директна веза између права на приступ информацијама и динамичке примене режима тајности: уколико Повереник утврди да одређивање тајности није било оправдано, орган има обавезу да опозове тајност и омогући приступ.

Најјачи институционални инструмент опозива тајности јесте јавни интерес као независни критеријум, на основу којег Народна скупштина, председник Републике и Влада могу да опозову тајност докумената било ког степена „ако је то у јавном интересу или због извршавања међународних обавеза“ (члан 26. ЗТП).

### 5. КАКО СВАКИ СЛУЖБЕНИК МОЖЕ ДА ДОПРИНЕСЕ?

- **Не одређујте тајност „по инерцији“.** Увек се запитајте: „Каква стварна и вероватна штета би наступила откривањем?“ Ако се одговор не може конкретно формулисати, вероватно не постоји основ за тајност.
- **Користите технику редакције (redaction).** Ово је стандард европске праксе, као и у складу са чланом 12. став 3. ЗТП — заштитите само осетљиве делове, а остатак документа учините доступним.



## ПРАВИЛНО ПРИМЕЊЕНА ТАЈНОСТ ТЕМЕЉ МОДЕРНЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И ДЕМОКРАТСКЕ ОДГОВОРНОСТИ

- **Запамтите: тајност престаје када информација постане јавна.** Ово је основно правило у спречавању злоупотребе поновног означавања у складу са чланом 16. став 1. тачка 5. ЗТП.
- **Следите начело: „потребно да зна (need-to-know)“, а не „потребно сакрити (need-to-hide)“.** Ограничење приступа треба да штити оперативну безбедност, али не сме да спречава институције да обављају своја законска овлашћења.

**6. ЗАШТО ОВО ШАХОВСКИМ РЕЧНИКОМ ИСКАЗАНО МАТИРА?** - Правилно управљање тајним подацима није само питање безбедности – то је показатељ демократске зрелости, институционалног интегритета и поверења грађана у државу. У доба хибридних претњи, дезинформација и сајбер ризика, тачна, динамична и одговорна примена тајности постаје предуслов за:

- **успешну европску и евроатлантску интеграцију**, где се висок ниво стандарда у одређивању степена и престанка тајности сматра показатељем поузданости државних институција;
- **ефикасну борбу против корупције**, јер исправна примена закона онемогућава злоупотребу тајности као средства прикривања неправилности;
- **оперативну компатибилност са партнерима**, посебно у одбрамбено-безбедносним структурама где се размена тајних података заснива на поверењу;
- **легитимност државних институција**, јер јавност мора знати да се заштита тајности података користи ради заштите државе, а не ради скривања одговорности.

## 7. МЕЂУНАРОДНИ ПРАВНИ ОКВИРИ – УНИВЕРЗАЛНИ СТАНДАРДИ КОЈИ ПОДРЖАВАЈУ РАВНОТЕЖУ ИЗМЕЂУ БЕЗБЕДНОСТИ И ТРАНСПАРЕНТНОСТИ

Република Србија, као чланица ОЕБС-а, Савета Европе и система УН, формално прихвата и имплементира низ међународних оквира који недвосмислено дефинишу тајност као изузетак, а не правило, у демократском друштву. Неки од најзначајнијих докумената који се директно односе на правилну примену тајности у служби националне безбедности а не као средство злоупотребе су:

**Tshwane Principles on National Security and the Right to Information (2013)** - Универзални стандард развијен у сарадњи са УН-овим специјалним известиоцем за слободу информисања, Open Society Foundations и водећим светским правним експертима. Принципи инсистирају да се тајност може увести искључиво ако постоји стварна, конкретна и вероватна штета по легитиман безбедносни интерес, а не због политичке прикладности или страха од јавне критике.



## ПРАВИЛНО ПРИМЕЊЕНА ТАЈНОСТ ТЕМЕЉ МОДЕРНЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И ДЕМОКРАТСКЕ ОДГОВОРНОСТИ

**Истанбулска декларација ОЕБС-а (1999)** - Дефинише концепт „националне безбедности“ у оквиру демократског поретка и изричито забрањује њену злоупотребу као изговор за прикривање корупције, злоупотребе власти или ненаменског трошења јавних средстава. Истиче да је транспарентност неодвојив део институционалне отпорности државе на хибридне претње.

**Тромсе конвенција Савета Европе (2009)** - Први обавезујући међународни уговор који гарантује право на приступ службеним документима као саставни део слободе изражавања. Конвенција наглашава да тајност мора бити временски ограничена, подложна независној ревизији и заснована искључиво на објективној процени ризика, а не на дискреционој процени службеника.

**Препоруке Групе држава против корупције (GRECO)** - У више циклуса евалуације истиче се да прекомерна тајност у јавним набавкама, сектору одбране и управљању јавним средствима директно ослабљује антикорупцијске механизме и подрива ефикасан институционални надзор. GRECO захтева јасна образложења, ревизију и пропорционалност у означавању степена тајности.

**УНЕСКО-ови водичи о слободи информација и националној безбедности** - Наглашавају да ограничења приступа информацијама морају бити „законита, неопходна и пропорционална у демократском друштву“, те да свака злоупотреба режима тајности представља претњу правосуђу, владавини права и демократској легитимности.

Ови документи нису „апстрактни идеали“, они представљају обавезујуће стандарде који дубоко утичу на процесе европске интеграције. Њихова доследна примена подиже кредибилитет институција, јача поверење у систем и омогућава оперативну компатибилност у међународном безбедносном и политичком окружењу.

Правилно управљање тајним подацима није питање технике, већ питање поверења. Када тајност постане изузетак заснован на доказивој штети, а не правило утемељено на непознавању прописа, страху, инерцији или административној удобности, она прераста у темељ легитимне безбедности и одговорне демократије. У том процесу, Канцеларија Савета за националну безбедност и заштиту тајних података има кључну улогу, не само кроз едукације које спроводи, већ и кроз стручну помоћ коју пружа свим органима јавне власти.