

- МЕТОДОЛОГИЈА ОДРЕЂИВАЊА И ПРЕСТАНКА (КЛАСИФИКАЦИЈА И ДЕКЛАСИФИКАЦИЈА) ТАЈНОСТИ ПОДАТАКА -

Режим тајности има једну основну сврху: да заштити информације чије би откривање могло нанети стварну, доказиву штету интересима националне безбедности, одбране, спољних односа или стабилном функционисању државе. Ипак, искуства земаља региона показују да пракса често одступа од ове намере. Проблем не лежи у законском оквиру, већ у слабостима његове примене, недостатку стандардизованих ризичних процена и ограниченим механизмима демократског надзора. Зато је неопходно јасно дефинисати легитимне кораке у поступку одређивања, класификације и укидања тајности – како би се разграничила оправдана заштита од институционалног скривања.

А) Одређивање тајности или класификација података и докумената

1. Када се уопште може поставити тајност? - Основни принцип је једноставан: **тајност мора бити изузетак, а не правило**. Према члану 8. Закона о тајности података, информација се може означити као тајна само ако су испуњена сва три услова:

- односи се на интерес Републике Србије,
- њено откривање би нанело штету,
- потреба заштите је претежнија од јавног интереса да се информација обелодани.

Овај троструки тест – **интерес, штета, претежност** – представља неопходан филтер који обавезно претходи свакој одлуци.

Шта по закону никада не може бити тајно (члан 3):

Закон не забрањује одређивање тајности свих података који се односе на кривична дела, злоупотребе или опасности - већ искључује могућност да се податак прогласи тајним искључиво ради прикривања кривичног дела, прекорачења овлашћења, злоупотребе службеног положаја или других незаконитих радњи органа јавне власти. Ако је тајност уведена с таквом намером, она није правно важећа, а одлука је ништавна. Ово значи да је кључна одредница намера, а не само садржај информације. Стога чак и подаци о корупцији или криминалу могу бити тајни ако њихово откривање стварно, конкретно и вероватно угрожава безбедносни интерес (на пример, идентитет извора у истрагама организованог криминала). Међутим, ако се тајност користи да би се спречило откривање неправилности, онда се ради о злоупотреби режима тајности, а не о легитимној заштити.

2. Како се одређује степен тајности? - Тајност није једна категорија – она је скала. Степен зависи од процењене висине и врсте штете.

Табела 1: Степени тајности и врста штете

Степен тајности	Опис штете која би наступила откривањем информације
Државна тајна	Неотклоњива, тешка штета по територијални интегритет, уставни поредак или међународне односе
Строго поверљиво	Тешке последице по безбедност, дипломатску позицију или рад служби безбедности
Поверљиво	Штета по функционисање органа или критичне административне процесе
Интерно	Угрожавање унутрашњег рада органа без ширих последица по јавни интерес

Кључно правило: степен тајности мора бити најнижи могући за спречавање штете, никада виши.

У пракси региона, међутим, најнижи степен („интерно“) често се третира као замена за „тајно“, док се виши степени користе масовно и некритички.

3. Процена ризика – темељ сваке одлуке

Одлука о тајности мора бити заснована на формализованој процени ризика. Та процена обухвата:

- **идентификацију типа информације** (нпр. оперативни план, уговор, анализе),
- **процену вероватноће и тежине штете**, уколико податак постане доступан неовлашћеном лицу,
- **проверу реалистичности претње** (штета мора бити стварна, озбиљна и непосредна),
- **тест претежности:** да ли би штета од откривања била већа од добити за јавни интерес?

Без ове процедуре, одлука о тајности нема правну тежину и не може бити дугорочно одржива.

4. Образложење и документација

- Одлука о тајности мора бити формално образложена, у складу са Уредбом о означавању. Образложење садржи:

- назив документа и опис садржаја који се штити,
- предложени степен тајности,
- процену могуће штете,
- позивање на члан 8. Закона,
- проверу да садржај не спада у категорије забрањене за тајност (члан 3),
- рок трајања тајности,
- предвиђени датум ревизије.

Каталози тајних података могу олакшати рад органа, али **они сами морају бити резултат ризичне процене, а не административна рутина.**

5. Престанак тајности – једнако важан као њено увођење

Озбиљан слаб простор у пракси државних органа јесте одсуство систематског декласификовања. Закон прописује да тајност престаје:

- по истеку рока (до 30 година за државну тајну),
- након наступања догађаја на који се односила (нпр. завршетак операције, уговора, пројекта),
- по решењу Повереника или суда.

Ипак, многи документи остају „тајни“ и након што више не постоји ниједан разлог за то, што подрива кредибилитет целог система.

6. Где почињу злоупотребе? - Злоупотреба настаје онда када тајност постане средство политичке или институционалне контроле информација. Најчешћи модели су:

- прекомерно означавање („све је тајно“),
- ретроактивно означавање након објављивања у медијима,
- класификација ради избегавања парламентарног или јавног надзора,
- масовно скривање уговора у одбрани, енергетици и инфраструктури,
- продужавање тајности без нове процене ризика.

Тајност тада више не штити државу, већ штити актера који жели да избегне питања.

7. Кључ је у балансу - Циљ није укинути тајност, већ је **вратити њеној изворној функцији**. У демократском поретку:

- тајност је оправдана кад штити државу,
- али је нелегитимна када штити власти од јавности.
- Зато је неопходно:
- да свака одлука о тајности буде заснована на проверљивој процени ризика,
- да образложење буде записано и доступно Поверенику,
- да декласификација буде рутинска, а не изузетак,
- да се ојачају надзорни механизми (Повереник, Канцеларија, Дирекције).

Ово није критика безбедносног система – већ предлог функционалне реформе у којој режим тајности постаје прецизан, контролисан, временски ограничен и усмерен на заштиту државе, а не политичке моћи.

Б) Престанак тајности и декласификација: легитимност система зависи од времена

Један од најчешће занемарених елемената режима тајности јесте његова **временска ограниченост**. Тајност није трајно стање, она мора имати јасно дефинисан рок трајања и услове под којима престаје. Ипак, у пракси широм региона, посебно у Србији, Босни и Херцеговини и Црној Гори, ова фаза остаје недовољно примењена. Резултат је дуготрајно задржавање докумената у статусу „тајно“ и онда када правни и безбедносни основи за класификацију више не постоје.

Када и како тајност треба да престане? - Према Закону о тајности података, тајност престаје:

- **по истеку законског рока** (до 30 година за „државну тајну“, краће за ниже степене),
- **наступањем догађаја** на који се тајност односила (завршетак пројекта, реализација оперативног плана),
- **одлуком Канцеларије Савета за националну безбедност и заштиту тајних података**
- **решењем Повереника или суда,**
- **решењем органа који је документ одредио тајним или класификовао**, након нове процене ризика.

То значи: *сваки тајни документ мора бити предмет редовног преиспитивања*, не само приликом одређивања тајности, већ и током целокупног периода њеног важења.

Где лежи проблем у пракси? - Уместо да буде системски и рутински процес, декласификација је у многим земљама региона:

- заборављена – документи остају „тајни“ и након што су постали историјски материјал,
- неформална – без нове процене ризика или валидног образложења,
- поправна – покреће се тек после жалби, медијског притиска или скандала,
- непотпуна – доставља се „редигована“ верзија са готово потпуно прекривеним садржајем.

Чак и када Повереник наложи престанак тајности или декласификацију (као у предметима ПВ-9 у Србији, БВМ у Хрватској или у случају „Беласица“ у Северној Македонији), органи често формално испуне обавезу, али суштински не омогуће приступ подацима. У таквим ситуацијама „право на приступ информацијама“ постаје само формулација, а не стварно право.

Зашто је престанак тајности или декласификација неопходна?

1. Чува веродостојност режима тајности - Тајност је снажна само када је изузетак и када је временски ограничена. Када је трајна - она се претвара у инструмент управљања информацијама, а не у инструмент заштите државе.

2. Омогућава демократски надзор - Декласификовани документи омогућавају накнадни увид у:

- политичке одлуке,
- корупцијске механизме,
- финансијске злоупотребе,
- пропусте у управљању кризама.

Без тога, институционална прошлост постаје „мртва зона“ у којој се ништа не може анализирати и из које се ништа не може научити.

3. Подржава историјско, академско и реформско истраживање - Архивска грађа је неопходна за научна истраживања, институционалну евалуацију и процесе помирења. У многим државама региона, међутим, тајност се не укида ни након неколико деценија - иако догађаји одавно припадају историјском архиву.

4. Испуњава међународне стандарде - ЕУ и НАТО имају строге механизме аутоматске декласификације по истеку рока. Док су ови механизми у Румунији и Бугарској већ део редовне администрације, у државама западног Балкана углавном су запостављени.

Шта у региону функционише добро?

- **Словенија:** Повереник редовно преиспитује одлуке и ефикасно налаже декласификацију.
- **Хрватска:** Уред Вијећа за националну сигурност има овлашћења за иницирање провера, али их користи повремено.
- **Северна Македонија:** Нове законске измене уводе аутоматску декласификацију - важан помак, мада примена још није уједначена.

Шта је неопходно урадити?

1. Увести обавезну, аутоматски престанак тајности или декласификацију – она формално у прописима постоји али се у пракси не примењује доследно. По истеку рока тајност мора престати, осим ако орган не донесе нову, образложену одлуку о продужењу.

2. Увести јавни рок ревизије - Сваки документ са ознаком тајности мора имати датум ревизије — најкасније на сваких пет година.

3. Објављивати годишње извештаје о престанку тајности или декласификацији – Повереник, Дирекције и надзорна тела треба да објављују податке о:

- броју докумената којима је престала тајност, односно декласификованих,
- разлога за декласификацију,
- степену доступности (целокупно/делимично).

4. Пооштрити контролу над „редигованим“ документима - Достављање потпуно прекривених докумената мора бити предмет правне оцене, а не техничког тумачења.

5. Едуковати службенике о природи привремености тајности - Упорно схватање да је „тајно“ исто што и „трајно“ представља структурни проблем који се решава само системским обукама.

Закључак: тајност која нестаје је јача од тајности која траје

Тајност која никада не престаје - губи смисао. Систем у коме се информације не враћају у јавну сферу осуђује сам себе на непрозирност и институционално слабљење.

Зато је престанак тајности (декласификација) једнако важна као и одређивање тајности (класификација). Она је доказ:

- да институције контролишу своје информационе токове,
- да поштују закон,
- да држава нема страх од транспарентности, чак ни онда када је непријатна.

Циљ није да све буде увек доступно. Циљ је да ништа не буде трајно сакривено. У модерној демократији, легитимитет режима тајности не мери се тиме колико смо докумената закључали - већ тиме *када, како и у којој мери их отварамо.*