КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

Прекомерно одређивање тајности у пракси: изазови легитимне заштите и институционалне злоупотребе

Проф. др Горан Д. Матић

Београд, 2025. године

С А Д Р Ж А Ј

Executive Summary – Извршни сажетак: Управљање тајним подацима у Р. Србији 2

Уводне напомене – Баланс између заштите тајности и транспарентности у демократском друштву 4

Култура тајности и прекомерно одређивање тајности: када заштита постаје замка 10

Да ли је одређивање тајности података правно или политичко питање? 13

Међународни контекст прекомерне класификације или означавања тајности 15

Политички аспекти режима тајности у Републици Србији – између легитимне заштите и ризика злоупотребе 20

Кључни изазови у систему 21

Правни аспекти злоупотребе у одређивању и означавању тајних података 23

Институционални изазови у Републици Србији 26

Заједнички проблеми у региону: баланс између транспарентности и безбедности - изазов демократске зрелости 30

Политичка, правна и морална одговорност - регионални поглед 41

Закључна разматрања 44

Налази и препоруке 45

Препоруке у складу са стварним стањем заштите тајних података у Р. Србији 47

ПРИЛОГ 1. - Методологија одређивања и престанка (класификације и декласификације) тајности података 49

МОДЕЛ - КОНТРОЛНА ЛИСТА ЗА ПРОЦЕНУ ПОТРЕБЕ ОДРЕЂИВАЊА ТАЈНОСТИ (обавезно се прилаже уз предлог за одређивање тајности, у складу са чланом 11. став 4. Закона о тајности података) 54

ПИТАЊА ЗА ДИСКУСИЈУ: 56

Executive Summary – Извршни сажетак: Управљање тајним подацима у Републици Србији

Овај сажетак пружа преглед кључних изазова и препорука повезаних са системом заштите тајних података у Републици Србији, са посебним освртом на практичну примену Закона о тајности података, одговорност органа јавне власти и изазове у балансирању националне безбедности и транспарентности. Формални надзорни механизми у оквиру режима тајности су Канцеларија Савета за националну безбедност и заштиту тајних података (стручни надзор) и Министарство правде (инспекцијски надзор), у складу са законом.

Кључни аспекти и идентификовани изазови

1. Прекомерно одређивање степена тајности података (over-classification) - Прекомерна класификација представља системски укорењену праксу, у којој се подаци који не испуњавају критеријуме из члана 8. и члана 10. став 3. Закона — попут економских, административних или урбанистичких информација — означавају као „поверљиви“ или „строго поверљиви“ без формалне процене могуће штете. Оваква пракса производи „инфлацију тајности“ и замагљује суштинске безбедносне приоритете: систем више не прави јасну разлику између стварно осетљивих података и информација које су тек политички, финансијски или медијски непожељне. Тиме се поткопава кредибилитет читавог режима тајности.

2. Злоупотреба тајности у јавним набавкама и стратешким пројектима - Неправилно проглашавање уговора и документације тајном у области јавних набавки и стратешких инфраструктурних пројеката функционише као механизам за избегавање јавне контроле искључиво ради прикривања неправилности. Иако Закон о тајности података захтева заснивање тајности на стварној и вероватној штети, у пракси се одлуке често темеље на општим, неконкретизованим проценама ризика. Последице су двоструке: (1) ствара се простор за процедуралне пропусте и нетранспарентно доношење одлука, и (2) повећава се ризик од политички мотивисане употребе тајности као инструмента за заобилажење надзора.

3. Недостатак јединствене методологије и слаби надзорни капацитети - Улога Канцеларије Савета за националну безбедност формално обухвата координацију, методологију процене ризика и стручни надзор. Међутим, у пракси, Канцеларија често делује више као административно-техничка служба, без активног преиспитивања спорних одлука о класификацији. Инспекцијски надзор Министарства правде, иако законом предвиђен, ретко спроводи систематске контроле. Ова комбинација слабости омогућава широк дискрециони простор органима јавне власти, без ефективних корективних механизама.

4. Недовољна припрема запослених и слаби технички стандарди - Недостатак континуиране обуке и одсуство јединствених безбедносних стандарда — посебно у дигиталном окружењу — значајно повећава ризике од неовлашћеног приступа, губитка или компромитовања тајних података. Дигитализација државне управе напредује брже

од безбедносних протокола, што ствара структурни јаз између нормативних захтева и техничко-оперативних капацитета органа јавне власти.

5. Одсуство редовне ревизије и „застареле тајне“ - Иако Закон изричито обавезује на ревизију тајности у утврђеним роковима, у пракси се ова обавеза често занемарује. Тако настаје феномен „застарелих тајни“ — докумената који настављају да носе високе нивое тајности иако је процењена штета престала да буде реална или вероватна. Ово подрива основну сврху режима тајности, чија логика мора бити динамична, адаптивна и заснована на текућем безбедносном контексту.

Предлог смерница за даље поступање

1. **Успоставити обавезну, стандардизовану процену потенцијалне штете** пре одређивања било ког степена тајности, у складу са чланом 10. став 3. Закона, као основни инструмент за сузбијање over-classification-a.
2. **Интегрисати механизме редовне ревизије и опозива тајности** у оперативну праксу свих органа јавне власти, уз јасне рокове и персоналну одговорност руководилаца.
3. **Посебно регулисати употребу тајности у јавним набавкама**, уз обавезно писано образложење, праћење и накнадну контролу Канцеларије Савета за националну безбедност и заштиту тајних података и Министарства правде, како би се свеле на минимум злоупотребе.
4. **Јачати кадровске и техничке капацитете** кроз континуиране обуке, акредитацију ИКТ система и опремање заштићених простора у којима се обрађују тајни подаци.
5. **Ојачати улогу Канцеларије Саветаза националну безбедност и заштиту тајних података у стручном надзору**, укључујући систематичније преиспитивање одлука, израду јединствених методолошких упутстава и редовно извештавање о стању система. Паралелно, унапредити инспекцијске капацитете Министарства правде, уз јачање овлашћења за ефикасно санкционисање.
6. **Развијати културу безбедности у којој је тајност изузетак, а не правило**, засновану на јасној процени штете, одговорности и свести да злоупотреба тајности директно подрива поверење у институције.

Овај извршни сажетак намењен је руководиоцима и креаторима политика и има за циљ да подржи доношење стратешких и оперативних одлука које ће ојачати кредибилитет, ефикасност и законитост система заштите тајних података у Републици Србији. Уједно, ово је и предуслов за испуњавање захтева савремене безбедносне политике и међународних стандарда, посебно у оквиру преговарачког поглавља 30 (Спољна, безбедносна и одбрамбена политика), где је усклађеност режима тајности кључна за компатибилност са европским и евроатлантским партнерима.

Уводне напомене - Баланс између заштите тајности и транспарентности у демократском друштву

Државе у процесу транзиције, укључујући и Републику Србију, суочавају се са сложеним изазовима у успостављању оптималног баланса између заштите осетљивих информација и обезбеђивања неопходне транспарентности, односно између заштите интереса националне безбедности и људских права. Тај баланс није питање пуке техничке усклађености прописа, већ језгровити показатељ институционалне зрелости, одговорности и степена демократског развоја. У модерној држави, безбедност се не заснива на апсолутном скривању информација, већ на способности да се подаци прецизно, привремено и образложено штите онда када је то заиста неопходно — уз истовремено отварање јавне расправе о питањима од ширег друштвеног значаја. Стога тајност мора бити изузетак, а не правило, док њена примена мора бити подвргнута строгим, проверљивим и временски ограниченим критеријумима.

Законодавство Републике Србије пружа јасну и методолошки кохерентну основу за заштиту тајних података. Члан 8. Закона о тајности података прописује да се податак може одредити као тајан искључиво ако би његово откривање нанело стварну, конкретну и вероватну штету интересима државе, укључујући националну безбедност, одбрану, спољну или унутрашњу политику и само уколико је та заштита претежнија од јавног интереса да се до податка дође. На овај начин у закон је интегрисан принцип „претежног интереса“, који представља кључни механизам за спречавање аутоматског, административног или политички мотивисаног одређивања тајности. Ова процена није декларативна.

Важно је нагласити да Закон о тајности података регулише искључиво тајне податке који су од интереса за Републику Србију и чија заштита се заснива на процени штете по националну безбедност или друге државне интересе. Ознаке као што су „службена тајна“ у здравству, „поверљиво“ у пореској администрацији или „интерно“ у канцеларијском пословању не спадају у режим тајности из овог закона и не могу се користити за ограничавање приступа информацијама од јавног значаја без посебне правне основе.

У професионалној и правној пракси развијен је четворостепени тест јавног интереса, према којем се мора утврдити:

1. да постоји стварна и утврдива штета,
2. да је она значајна,
3. да интерес државе претеже над правом јавности да зна, и
4. да је ускраћивање приступа неопходно у демократском друштву.

Паралелно с тим, члан 3. Закона о тајности података одређује да податак који је проглашен тајним искључиво ради прикривања кривичног дела, прекорачења овлашћења, злоупотребе службеног положаја или другог незаконитог поступања органа јавне власти не може се сматрати тајним податком. Ова одредба представља јасну правну препреку против намерне злоупотребе режима тајности као средства за избегавање одговорности и прикривање неправилности. Намера се у правној пракси сматра присутном ако се одређивање тајности уводи у тренутку или у контексту у којем је чињеница о злоупотреби или кривичном делу већ јавности позната (на пример, преко медијских извештаја, парламентарног питања или кривичне пријаве). У таквим

ситуацијама, тајност се по својој природи сматра ништавном, без потребе за додатним правним поступком.

Уколико се утврди да је тајност уведена с таквом намером, одлука је ништавна, а поступање може повући и кривичноправне последице — укључујући одговорност за злоупотребу службеног положаја или фалсификовање службене исправе. У том смислу, члан 3. успоставља условну, али ефективну „црвену линију“: не према садржају информације, већ према намери њеног означавања као тајне.

Тајност настала синтезом информација - Систем мора обухватити и ситуације у којима тајност настаје синтезом, а не искључиво садржајем појединачних информација. Управо то регулише члан 12. Закона, који овлашћује да се као тајан означи податак настао обједињавањем или повезивањем иначе отворених информација, уколико тако добијена целина може да проузрокује стварну и вероватну безбедносну штету. Ово је у потпуности у складу са савременим приступом заснованим на процени штете (harm-based classification), јер се критичне претње данас најчешће идентификују анализом великих скупова података и комплексних аналитичких образаца.

Ипак, у пракси се ово овлашћење често злоупотребљава као генерализовано оправдање за масовно одређивање тајности читавих докумената, иако закон нуди јасно решење: уколико само мањи део документа садржи тајне податке, тај део се издваја као посебан прилог, док основни документ остаје јаван. Избегавање ове технике селективног издвајања (redaction) доводи до праксе у којој се комплетни извештаји, уговори или аналитички материјали проглашавају тајним без стварног добитка по безбедност, али уз значајно смањење могућности јавне и институционалне контроле.

Члан 12. прописује и да документ који садржи податке различитих степена тајности мора бити означен вишим степеном и дужим роком чувања. Иако је то логично из перспективе заштите, у одсуству прецизне и редовне ревизије ова одредба може постати механизам неоснованог проширивања тајности на читаве корпусе информација — чак и онда када осетљивост појединих елемената више није актуелна.

Тако чак и легитимне правне основе могу постати инструмент системског прекомерног одређивања тајности (over-classification) када се не примењују уз јасну методологију, стандардизоване процене ризика и функционални надзор.

Тајност престаје постојањем информације у јавности - Члан 16. Закона о тајности података прописује да тајност престаје ако је податак учињен доступним јавности. Ова одредба спречава ретроактивно одређивање тајности и онемогућава накнадно прикривање већ познатих чињеница. Чим информација постане јавна – путем медија, парламентарних расправа, јавних набавки или других канала – њена тајност аутоматски престаје, без обзира на формалну одлуку било ког органа.

У том контексту, члан 16. чини режим тајности динамичним, условљеним и временски ограниченим, а не трајним или апсолутним статусом. То је у потпуности усклађено са Tshwane Principles (2013), који инсистирају да се тајност може оправдати само уколико постоји стварна, конкретна и вероватна штета, а не апстрактна или хипотетичка претња.

Опозив тајности као правни коректив прекомерног одређивања - У пракси, ограничавање приступа информацијама често добија карактер коначног, неповратног

чина, јер се тајност погрешно схвата као трајни статус, а не као привремена мера. Међутим, Закон о тајности података изричито предвиђа механизме опозива тајности као инструмент надзора и исправке грешака у процени ризика. Ови механизми представљају функционално тежиште одговорности унутар самог режима тајности и нису секундарни „екстерни правни путеви“, већ унутрашњи корективи који се морају активирати превентивно и рефлексивно.

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). То није само административна могућност, већ стратешки потенцијал за унапређење квалитета процене ризика, посебно када дође до колизије између административне праксе и правног оквира. Ипак, у пракси Канцеларија ретко иницира ове поступке проактивно, већ углавном чека на појаву спорних случајева, чиме делује реагујуће, а не превентивно.

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. Ипак, делотворност овог механизма зависи од добровољног испуњавања обавезе од стране органа, будући да Закон не предвиђа извршне санкције за непоступање по решењу Повереника. У пракси, то често доводи до ситуација у којима се тајност формално опозива, али се суштински задржава кроз екстензивно „редиговање“.

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). Иако ова одредба пружа стратешку могућност за демистификацију система, она се у пракси примењује искључиво у изузетним и ретким случајевима, најчешће у вези са архивском грађом, а не у текућим, контроверзним процесима, попут одбрамбених набавки, енергетских уговора или пројеката финансираних средствима ЕУ.

У том контексту, опозив тајности није пуки технички поступак, већ индикатор институционалне зрелости: систем у којем се тајност лако уводи, али се ретко укида чак и када више није потребна, није само неефикасан – он је утемељен на погрешној процени ризика и слабим механизмима одговорности. Да би режим тајности био легитиман, мора бити динамичан, редовно ревидиран и спреман на исправке, не само приликом увођења, већ и приликом укидања тајности.

Међународни стандарди. Амерички систем – један од најразвијенијих у свету – прецизно дефинише појам **“over-classification”** (*прекомерно одређивање тајности*). У оквиру америчког правног и политичког оквира овај феномен се описује као коришћење режима тајности ради избегавања одговорности, контроле јавне перцепције или ограничавања непожељних јавних, политичких или медијских питања. Кључни нормативни документи, као што су **Executive Order 13526 – Classified National Security Information (Извршна уредба 13526 – Класификоване информације националне**

безбедности), систематски инсистирају на уској, конкретној и штети заснованој примени класификације.

Европска тела, попут **GRECO – Group of States against Corruption (Група држава против корупције)** при Савету Европе, у више циклуса евалуација истичу да прекомерно ослањање на тајност у јавном сектору подрива антикорупцијске механизме, умањује транспарентност и отежава институционални надзор, посебно у областима јавних набавки, безбедносних политика и управљања ресурсима.

Иако Европска унија и НАТО не користе експлицитно термин *over-classification*, њихови безбедносни оквири постављају јасне стандарде који функционално адресирају исту појаву. Тако **EU Security Rules – Rules on EU Classified Information (Правила ЕУ о руковању класификованим информацијама)** и НАТО документ **AAP-06 – NATO Glossary of Terms and Definitions (НАТО глосар термина и дефиниција)** инсистирају на томе да свака одлука о класификацији мора бити:

- **proportional (пропорционална)**,
- **justified (образложена)**,
- **based on specific and identifiable harm (заснована на конкретно утврђеној штети)**,
- **time-limited (временски ограничена)**,
- подвргнута принципима **“need-to-know” (потреба да се зна)** и – све више – **“need-to-share” (потреба да се дели)** како би се омогућила међуинституционална сарадња и смањило непотребно затварање информационих токова.

Ови стандарди, иако различито формулисани у америчком, европском и НАТО систему, конвергирају ка истој суштини: класификација мора служити заштити националне безбедности, а не институционалном интересу, избегавању контроле или прикривању неправилности.

Теоријска усаглашеност са стандардима често није праћена доследном применом у пракси. Уочљива је тенденција да се тајност третира као подразумевани поступак, нарочито у контексту јавних набавки, инфраструктурних пројеката, енергетике и уговора који укључују значајан страни капитал или европске фондове. Документи понекад добијају висок степен тајности без адекватне процене ризика, без детаљног образложења или без јасно дефинисаног безбедносног интереса.

Највећи проблем произилази из формалног спровођења техничких стандарда без суштинског повезивања са критеријумима из члана 8. и апсолутним забранама из члана 3. То нарушава поверење у институције и отежава испуњавање европских стандарда транспарентности.

Иако су режим тајности и право на приступ информацијама регулисани одвојеним законима, у пракси често долази до колизије. Члан 9. став 5. Закона о слободном приступу информацијама прописује да се приступ може ограничити ако би тиме постала доступна информација која је одређена као тајна. Иако делује технички неутрално, ова одредба у пракси доводи до ситуације у којој формално одређивање тајности, чак и када је неосновано, постаје готово апсолутан разлог за ускраћивање приступа.

Ипак, исти члан 9. предвиђа да ограничење мора испунити три кумулативна услова: тест неопходности, тест претежног интереса и тест специфичности (конкретна вероватна штета). Терет доказивања лежи на органу, што представља кључни механизам демократске контроле. Проблем је што се у пракси ова три теста често примењују декларативно или се уопште не примењују.

Две системске последице прекомерног одређивања тајности огледају се у:

1. **Обесмишљавање система заштите.** Пречеста, неселективна употреба тајности смањује кредибилитет саме ознаке и доводи до ситуације у којој се стварно осетљиви подаци не издвајају довољно јасно у односу на небитне или рутинске информације.
2. **Ограничавање демократског надзора.** Парламент, надзорна тела и медији најчешће остају без кључних података потребних за контролу трошења јавних средстава, стратешких одлука или истраживање могућих неправилности.

ENISA пракса. Пракса **ENISA – European Union Agency for Cybersecurity (Агенција Европске уније за сајбер безбедност)** у домену сајбер безбедности јасно показује да повећана **транспарентност у управљању сајбер инцидентима** значајно подиже отпорност система. Насупрот томе, прекомерна тајност смањује степен међусекторске сарадње, како између државних институција, тако и између јавног и приватног сектора. Оваква затвореност је у директној супротности са принципом **"need-to-share" (потреба да се дели)**, који је, према европским сајбер безбедносним стандардима, кључан за ефикасну размену техничких информација, индикатора компромитовања (IoCs) и других оперативно значајних података.

У земљама региона забележени су бројни примери прекомерног одређивања тајности: случај **Рогашка Слатина (2021)**, затим пројекат **модернизације БВМ – „Borbeno vozilo M-80" (Борбено возило М-80)** из 2022. године, затим пројекат **Термоелектрана Бања Лука (2020)**, као и уговор са **KMW –** *Krauss-Maffei Wegmann GmbH & Co. KG* **(Краус-Мафеј Вегман ГмбХ и Ко. КГ)** из 2019. године. У појединим државама региона пример је и набавка кинеских транспортера **ПВ-9 –** *Type PV-9 Armored Personnel Carrier* **(оклопни транспортер ПВ-9)** из 2022. године. Напомена: Ознака ПВ-9 у јавним изворима региона није униформно стандардизована; најчешће се односи на комерцијалну извозну варијанту кинеског оклопног транспортера која се у стручним анализама означава као „PV-9" или „Type PV-9". Остављено је у двојезичној форми ради терминолошке доследности.

Ови случајеви указују на заједничке обрасце: масовно означавање докумената као тајних, ретроактивно увођење тајности, непрестано продужавање рокова трајања тајности и систематско ограничавање приступа извештајима о неправилностима, чак и у деловима који по природи не могу бити класификовани. Проблем није у законском оквиру, већ у његовој примени, институционалној култури и недостатку професионалне одговорности.

Постојећи надзорни механизми по Закону о тајности података – унутрашња контрола у органима јавне власти (члан 84), стручни надзор Канцеларије Савета за националну безбедност и заштиту тајних података (чланови 85–96) и инспекцијски надзор Министарства правде (члан 97) – формално су добро разрађени, али у пракси често делују недовољно делотворно. За постизање стварне одговорности неопходно је да сви

ови механизми функционишу проактивно и узајамно повезано: унутрашња контрола мора да преиспитује сваку одлуку о одређивању тајности пре њеног ступања на снагу; Канцеларија Савета треба да преузме стратешку улогу у утврђивању стандарда, преиспитивању праксе и издавању оперативних упутстава; а Министарство правде мора да спроводи систематске инспекцијске провере, а не да реагује искључиво на пријаве.

У том смислу, „надзор изнутра“ није питање индивидуалне професионалне етике, већ доследне примене правно обавезних процедура које осигуравају да одлука о тајности буде заснована на реалној процени могуће штете, а не на политичкој или административној прикладности, уз ефикасан парламентарни надзор над секторима у којима постоји повишен ризик од злоупотребе тајности.

GRECO, пуним називом **Group of States against Corruption (Група држава против корупције)** при Савету Европе, у својим редовним евалуационим процесима — пре свега у оквиру **Evaluation Reports / Compliance Reports (Евалуациони извештаји / Извештаји о усклађености)** у *III и IV кругу евалуација* - систематски указује да прекомерна тајност у поступцима јавних набавки представља индикатор слабости у управљању јавним пословима, посебно у погледу транспарентности, интегритета и контролних механизама. У тим документима GRECO наглашава да непропорционална или нејасно образложена примена тајности у јавним набавкама умањује могућност јавног надзора, повећава простор за неправилности и отежава спречавање сукоба интереса и коруптивних ризика.

Транспарентност није слабост - она је знак институционалне снаге. Држава је најјача онда када је отворена тамо где то не угрожава безбедност, а чврсто заштићена тамо где је то заиста неопходно. Решења укључују:

- стандардизовану процену ризика пре сваке одлуке,
- обавезно образложење одлука,
- јасно разграничење категорија „интерно“ и „поверљиво“,
- аутоматски престанак тајности по истеку рока,
- јачање овлашћења надзорних органа,
- систематску обуку службеника,
- ефикаснији парламентарни надзор.

Истинска безбедност није само у заштити информација, већ и у способности да се о питањима од јавног значаја води аргументована и информисана јавна расправа.

Да ли се комплексна проблематика прекомерног одређивања тајности може решити једном административном процедуром, упутством или подзаконским актом - или је она дубље укорењена у институционалну културу, правне тековине и ниво демократске зрелости друштва? Другим речима: **Да ли нам је потребна боља форма надзора - или дубља, професионална одговорност службеника који одлучују о тајности?**

Одговор на ово питање одредиће да ли ће тајност у Републици Србији бити изузетак у служби националне безбедности – или правило у функцији управљања информацијама.

Култура тајности и прекомерно одређивање тајности: када заштита постаје замка

У савременој држави, режим тајности није само технички механизам заштите осетљивих информација, он представља огледало институционалне културе и начина на који систем схвата однос између безбедности, транспарентности и демократске одговорности. Када та култура почива на претпоставци да је „боље сакрити него ризиковати“, формира се системска динамика прекомерног одређивања тајности (over-classification), процес у којем информације добијају статус тајних иако реални, спољашњи безбедносни ризици то не оправдавају. Ова појава није пуки правни изузетак који се претвара у правило; она постаје стратегија управљања информацијама, често у служби политичке, административне или институционалне удобности.

1. Прекомерно одређивање тајности (Over-classification) - Over-classification означава праксу додељивања тајности информацијама које не испуњавају основне критеријуме за заштиту: да би њихово откривање нанело стварну, конкретну и вероватну штету легитимном државном интересу. Уместо да тајност буде прецизан, рестриктиван инструмент, она постаје „подразумевана вредност“ – административни рефлекс, техничка формалност или чак свесни механизам прикривања.

Последице су дубинске и системске:

- **Ерозија ефикасности заштите**: стварно осетљиви подаци изгубљени су у маси непотребно класификованих докумената.
- **Сужавање демократског надзора**: јавност, парламент и контролни органи губе увид у информације неопходне за процену законитости, транспарентности и рационалног коришћења јавних ресурса.

Овакво структурно ширење тајности подрива основни принцип: тајност мора штитити државу од ризика, а не државне органе од јавности.

2. Одређивање тајности засновано на штети (Harm-based classification) - Идеални оквир за утврђивање тајности је harm-based classification – модел у којем свака одлука о класификацији мора бити заснована на јасно идентификованој, мерљивој и вероватној штети која би наступила откривањем информације. То значи да критеријуми морају бити операционализовани кроз стандардизоване процене ризика, а не ослоњени на хипотетичке, опште или административно погодне претпоставке.

У Србији је овај принцип формално уграђен у члан 8. Закона о тајности података, али без обавезне методологије процене ризика често остаје декларативан. „Штета“ тако постаје еластична категорија – прилагођава се контексту, интересима или чак тренутној политичкој осетљивости, што подрива кредибилитет читавог режима заштите.

3. Принцип потребно да се зна (Need-to-know principle) - Need-to-know principle је темељни безбедносни стандард НАТО-а, ЕУ и шире међународне праксе: приступ тајним информацијама има само онај коме је тај податак заиста потребан за обављање службених дужности. Ово минимизира ризик од унутрашњег цурења, повећава индивидуалну одговорност и спречава ширење тајности изван оправданих оквира.

У системима у којима култура тајности деградира у културу контроле, овај принцип се изопачује: документи се закључавају не ради реалне потребе, већ ради „опште сигурности“ у којој је пожељно да мање људи зна. Парадоксално, ова пракса умањује безбедност: ствара паралелне канале комуникације, неформалне пречице и подстиче институционалну недоверљивост.

4. Административни прекомерни одговор (Administrative overreach) - настаје када органи јавне власти прекорачују своја овлашћења не због намере да злоупотребе моћ, већ због удобности, инертности или незнања. У домену тајности, ово значи да се цео документ проглашава „тајним“ зато што је брже и једноставније него применити технику делимичног прекривања (redaction) и заштитити само заиста осетљиве делове.

Иако често незлонамерно, овакво поступање има системску последицу: тајност постепено постаје синоним за неприступачност, а не за стварну заштиту ризичних информација. То подрива поверење у институције и слаби принцип пропорционалности на којем правни режим тајности мора да почива.

5. Политичка тајност (Political secrecy) - означава коришћење тајности у сврхе које немају реалне везе са националном безбедношћу: управљање јавном перцепцијом, избегавање демократског надзора или заштиту политичке стабилности. Ово је посебно видљиво у сферама као што су јавне набавке, спољнополитички договори или енергетски и инфраструктурни пројекти.

У таквим ситуацијама, „национални интерес“ шири се тако да обухвати и аспекте који су у суштини комерцијални или административни. Таква пракса је директно супротстављена Tshwane Principles и Истанбулској повељи ОЕБС-а, који недвосмислено забрањују употребу националне безбедности као изговора за прикривање корупције, неефикасности или злоуправе јавним ресурсима.

6. Успон тајности (Classification creep) - представља постепено ширење простора тајности на информације које у почетку нису биле сматране осетљивим. Овај процес може бити последица:

- **технолошке трансформације** - дигитални документи се често класификују по „инерцији“
- **политичке динамике** - у кризама долази до механичког повишавања степена тајности
- **неадаптираних спољних стандарда** - механичко преузимање НАТО или ЕУ методологије без локалне контекстуализације

Успон тајности није само питање квантитета — он мења природу државе. Институција која треба да делује у јавном интересу постепено неконтролисано прелази у стање деловања под окриљем „тајног интереса“, који није подложан јавном преиспитивању.

7. Непрозирност система (Opacity / Invisibility of the system) - Крајњи резултат свих описаних феномена је системска непрозирност. У таквом окружењу јавност, надзорни органи, независна тела, али и сами државни службеници често не знају:

- колико се тајних докумената производи,
- на основу којих образложења,

- како се та одређивања ревидирају,
- када и како документи престају да буду тајни.

Без јавних извештаја, статистике и независних ревизија, режим тајности постаје невидљив – не подлеже спољашњој контроли, нити унутрашњем учењу. Та „црна кутија“ блокира могућност реформе, јер нема података за процену ефикасности, законитости и пропорционалности система.

8. Од „need-to-know“ ка „need-to-share“: баланс безбедности и сарадње у доба хибридних претњи - Конвенционални приступ безбедносној заштити традиционално се темељи на принципу *need-to-know* — приступ тајним информацијама омогућава се искључиво оним лицима чија професионална улога захтева познавање тих података. Овај модел значајно смањује ризик од неовлашћеног приступа, али у доба хибридних претњи, сајбер напада и комплексних, вишедимензионалних безбедносних изазова, показује своја ограничења. Уколико се ослања искључиво на рестрикцију, држава ризикује да фрагментира информациони ток између институција, ослаби координацију и онемогући благовремено, превентивно деловање.

Због тога се у међународној пракси – нарочито у ЕУ и НАТО-у – све више афирмише принцип *need-to-share*. Овај концепт не потире *need-to-know*, већ га функционално надограђује: полази од претпоставке да информације морају бити доступне актерима који их могу оперативно искористити за безбедносне, аналитичке, кризне или превентивне сврхе, чак и ако нису непосредни учесници у стварању тих података. *Need-to-share* омогућава адаптивност, убрзава заједничко реаговање и ствара предуслове за колективну отпорност на нетрадиционалне претње – од дезинформација и сајбер инцидената, до организованог криминала и природних катастрофа.

У системима у којима доминира култура „тајности ради тајности“, овај принцип је често потиснут или практично занемарен. Последице су вишеструке и структурно штетне:

- **институционална слепоћа -** кључни актери не виде ширу оперативну слику, јер подаци остају изоловани у силосима, без механизама за међусобну размену или укрштање;
- **неспособност колективног одговора -** виталне информације остају заробљене у појединачним подсистемима, док се претња шири хоризонтално, преко домена надлежности и институционалних граница.

У том смислу, прекомерно одређивање тајности не ограничава само демократски надзор; оно директно подрива функционисање и ефикасност безбедносног система. Без *need-to-share* логике, држава губи способност интеграције информација, слабљење предиктивних капацитета постаје неминовно, а читав спектар јавних, приватних и цивилних актера остаје неангажован, иако имају легитимну и неопходну улогу у националној отпорности.

Култура тајности као институционална матрица - Ова констелација појмова - прекомерно одређивање тајности, административни прекомерни одговор, политичка тајност, успон тајности и непрозирност система - не представља збир појединачних грешака. Она твори кохерентну институционалну културу, која обликује начин доношења одлука, структурира расподелу одговорности и дефинише однос државе према јавности.

Кључна иновација модерних безбедносних система није у повећању количине тајних информација, већ у *паметном управљању информацијама* - када делити, са ким, под којим условима и на основу какве процене ризика. У том контексту, *need-to-know* и *need-to-share* нису сукобљени концепти: они су два стуба исте безбедносне архитектуре. Први штити од злоупотребе; други обезбеђује функционалну ефикасност.

Тајност као изузетак није само правни принцип - она је културни показатељ демократске зрелости. Режим који није у стању да јасно дефинише шта треба сакрити, зашто и до када, није само институционално неефикасан - он постаје легитимно оспорив, јер функционише као механизам контроле, а не заштите.

У наредним поглављима овај аналитички оквир биће примењен на праксу Републике Србије и региона Југоисточне Европе, упоређен са међународним стандардима и повезан са конкретним правним, институционалним и политичким изазовима - са јасном премисом да безбедност 21. века не почива на тајности као забрани, већ на поверењу као предуслову сарадње.

Да ли је одређивање тајности података правно или политичко питање?

Одређивање тајности података у Републици Србији формално је правно питање, утемељено на прецизно дефинисаним критеријумима и процедуралним гаранцијама. Према члану 8. Закона о тајности података, податак се може одредити као тајан искључиво ако су испуњена три кумулативна услова:

1. **Постојање легитимног државног интереса** – податак се мора односити на области дефинисане у члану 8. став 2. Закона: национална и јавна безбедност, одбрана, спољна политика, безбедносно-обавештајни послови или стабилно функционисање државних институција. Легитимност интереса овде није апстрактна, већ захтева конкретну и правно утемељену повезаност са суштинским функцијама државе.
2. **Стварна, конкретна и вероватна штета** – откривање податка мора проузроковати процењиву, предвидиву и озбиљну штету по заштићени интерес; није довољно да штета буде хипотетичка, апстрактна или „политички удобна“. Овај критеријум уводи објективни филтер који ограничава произвољност у одређивању тајности.
3. **Претежност државног интереса над јавним интересом** – заштита државних интереса мора објективно надјачавати право јавности на приступ информацијама од јавног значаја. Ово осигурава да тајност не постане средство за прикривање управних или политичких недоследности, већ да остане инструмент строго ограниченог и пропорционалног значаја.

Овај троструки тест, инспирисан **Tshwane Principles on National Security and the Right to Information (2013)** – Тшване принципи о националној безбедности и праву на информације (2013) – представља не само формалну процедуру, већ и суштински правни филтер против произвољности и злоупотребе. Свака одлука мора бити праћена документованом проценом ризика, објашњењем пропорционалности и применом принципа најнижег неопходног степена заштите, у складу са концептом „демократске нужности“ (**necessary in a democratic society**).

Такво законско уређење усклађено је са највишим међународним стандардима. **Tshwane Principles (2013)** наглашавају да тајност може бити оправдана само ако постоји јасно идентификована, конкретна и вероватна штета по легитиман безбедносни интерес. **OSCE Istanbul Document (1999)** – Истанбулска повеља ОЕБС-а (1999) – забрањује злоупотребу националне безбедности као изговора за прикривање корупције, злоупотреба и неправилног трошења јавних ресурса. **Council of Europe Convention on Access to Official Documents (CETS No. 205, 2009)** – Конвенција Савета Европе о приступу службеним документима (Тромсе конвенција, 2009) – наглашава да тајност мора представљати изузетак, а не подразумевано правило; мора бити временски ограничена, подложна независној ревизији и заснована на објективној, а не политички мотивисаној процени ризика.

Изазови праксе и системска одступања - У пракси, међутим, често долази до дубоког и системског одступања од ових принципа. Тајност се, уместо да буде строго ограничена, све чешће јавља као подразумевани режим у областима као што су јавне набавке, енергетика, инфраструктурни и одбрамбени пројекти или програми финансирани из фондова Европске уније. Често ова проглашења нису праћена реалном проценом ризика, нити садрже детаљно и правно утемељено образложење. Често се дешава и да се подаци проглашавају тајним иако су већ доступни јавности – путем саопштења страних актера, докумената међународних организација или медијских извештаја. Ова пракса производи двоструку последицу:

1. **Ослабљивање ефикасности режима заштите** – када се ознака „тајности“ примењује широко, масовно и без диференцијације, критични подаци (идентитет извора, одбрамбене структуре, информације о сајбер претњама) губе специфичан статус и постају рањиви на пропусте у заштити.
2. **Ограничење демократског надзора** – парламент, медији, надзорна тела и грађани остају без могућности да контролишу трошење јавних средстава, провере стратешке одлуке или оцењују оправданост великих пројеката. Тако се нарушава кључна функција демократског система – контрола власти и одговорност извршних органа.

Важно је нагласити да злоупотреба тајности није последица недовољно уређеног законодавства. Закон о тајности података је методолошки кохерентан и усклађен са европским нормама. Проблем лежи у недоследној примени, непостојању јединствене методологије процене штете, институционалној инерцији и слабим механизмима надзора. У таквом амбијенту, тајност постаје политички инструмент контроле информација, а не професионални инструмент заштите стварних безбедносних интереса. Најчешћи облици укључују:

- **Масовно одређивање тајности** – цела документа или групе докумената проглашавају се тајним ради административне једноставности, уместо примене технике изузимања осетљивих сегмената (члан 12. Закона).
- **Непотребно продужавање тајности** – ознаке остају на снази и када реалан ризик више не постоји, супротно стандардима европских механизама аутоматске декласификације.
- **Проглашавање тајним података ван штићених области** – финансијски подаци, цене, техничке спецификације или уговори који не могу нанети штету држави.

- **Целокупно проглашење докумената за тајне** – извештаји или анализе се класификују у целини, чак и када је само мали део садржаја осетљив.
- **Политичка инструментализација** – тајност се користи за избегавање јавне расправе, ограничење медијског интересовања или заобилажење парламентарног надзора, нарочито у контексту великих финансијских и геополитички значајних пројеката.

Последице злоупотребе - Таква пракса доводи до:

- ерозије кредибилитета режима тајности – када је све „тајно“, ознака губи смисао;
- слабљења демократског надзора над јавним средствима, укључујући и фондове Европске уније;
- пада поверења грађана у институције безбедности и државну управу;
- повећања оперативних трошкова и компликација у руковању тајним подацима;
- отежавања међуинституционалне сарадње, јер прекомерна тајност смањује ефикасну размену информација.

Република Србија није изузетак у региону. Земље Балкана показују сличне обрасце: концепт „националног интереса“ често се неосновано проширује не ради заштите безбедности, већ ради избегавања јавне контроле. Тај тренд указује на дубљи институционални проблем – недовољно развијену културу транспарентности, одговорности и правне предвидивости. У одсуству прецизних и операционализованих критеријума за процену штете, као и ригорозних механизама ревизије и декласификације, „национална безбедност“ постаје категорија чија се садржина прилагођава политичким потребама, а не објективној процени ризика.

Циљ ове анализе није да умањи значај режима тајности – она је нужан инструмент сваке модерне државе. Међутим, тајност не сме постати супституит за транспарентност нити формални штит од одговорности. У демократском друштву, безбедност се не гради на апсолутном скривању, већ на способности да се о кључним питањима води рационална, информисана и јавна расправа. Тајност је легитимна само када је прецизна, стручна, временски ограничена и подложна независном надзору – а не када служи као механизам прикривања или политичке контроле информација.

Међународни контекст прекомерне класификације или означавања тајности

Прекомерна класификација – односно означавање информација као тајних без постојања реалне, конкретне и вероватне штете по легитиман безбедносни интерес – не представља безбедносну меру, већ системску злоупотребу која подрива демократску одговорност, ослабљује заштиту заиста осетљивих података и онемогућава ефикасан надзор. У савременом контексту хибридних претњи, сајбер ратовања и информационих операција, прецизно и ограничено коришћење тајности – а не њена инфлација – представља једини пут ка стабилном и веродостојном систему националне безбедности.

У доба када се информација претвара у стратешко оружје, а дезинформације и кампање утицаја постају свакодневица, питање како разликовати „стварну и реалну тајност“ од „инструменталне тајности“ постаје кључни индикатор институционалне зрелости. Прекомерна класификација – често примењивана ради прикривања неефикасности, корупције или политички непожељних података – не само да крши право на

информације, већ и активно ослабљује саму безбедносну архитектуру. Међународна пракса – од Уједињених нација до НАТО-а – уједначава се око једног основног принципа: тајност мора бити пропорционална, временски ограничена, методолошки заснована и подвргнута независном надзору.

Дефиниције и универзални (УН) модел - Иако Уједињене нације (UN – **United Nations / Уједињене нације**) као такве немају уједначен систем класификације, њихови специјализовани органи и повезане организације развили су принципе који граде универзални оквир за равнотежу између безбедности и транспарентности. Кључни међу њима су **UNESCO** – *United Nations Educational, Scientific and Cultural Organization / Организација Уједињених нација за образовање, науку и културу* – водичи о слободи информација и националној безбедности, који наглашавају да ограничења морају бити „законита, неопходна и пропорционална у демократском друштву". Слично томе, **ОЕБС (OSCE – Organization for Security and Co-operation in Europe / Организација за безбедност и сарадњу у Европи)** је више пута издавао препоруке о транспарентности у безбедносним питањима, посебно кроз Истанбулску декларацију, која истиче да „тајност не сме бити коришћена као изговор за избегавање одговорности".

На европском континенту, Савет Европе је начинио историјски корак усвајањем Конвенције о приступу службеним документима (Тромсе конвенција, 2009) – првог обавезујућег међународног уговора који гарантује право на информације као део слободе изражавања. Конвенција не забрањује класификацију, али инсистира да она мора бити заснована на „стварној штети по националну безбедност или друге легитимне интересе", а не на политичкој прикладности. Овај став додатно је оснажен Резолуцијама Парламентарне скупштине Савета Европе, које упозоравају да „прекомерна тајност угрожава демократску легитимност и антикорупцијски надзор".

Најсвеобухватнији оквир представљају **Tshwane Principles on National Security and the Right to Information (2013)**, развијени у сарадњи светских стручњака, Open Society Foundations, УН-овог специјалног известиоца за слободу изражавања и академских институција. Tshwane Principles утврђују да се тајност може оправдати само ако постоји стварна, конкретна и вероватна штета по легитиман безбедносни интерес, а не потенцијална, апстрактна или хипотетичка претња. Додатно, принципи инсистирају да класификација мора бити временски ограничена, подвргнута независном надзору и праћена заштитом информатора који откривају злоупотребе у јавном интересу. Ови принципи постали су референтна тачка за бројне реформе широм света, укључујући и европске.

Амерички модел - Појам „over-classification" најпрецизније је дефинисан у правној и институционалној пракси Сједињених Америчких Држава. Кључни нормативни оквир представља **Executive Order 13526 „Classified National Security Information"** (29. децембар 2009), који прописује да се информације могу класификовати искључиво ако њихово откривање може нанети „идентификовану или вероватну штету националној безбедности". Наредба експлицитно забрањује класификацију из „политичких разлога, ради избегавања срамоте или нелагодности, или ради спречавања јавног надзора", чиме директно адресира злоупотребу тајности као инструмента управљања перцепцијама.

Executive Order 13526 предвиђа аутоматску декласификацију након 25 година, осим ако се не докаже континуирана потреба за тајношћу, као и редовну ревизију класификованих

докумената на сваких 10 година. Наредба је допуњена одредбама о заштити узбуњивача и механизмима усклађеним са **Freedom of Information Act (FOIA)**, који омогућава приступ информацијама уз изузетке ограничене на стварну безбедносну штету.

Кључну улогу у надзору игра **Public Interest Declassification Board (PIDB)** – независно тело које саветује председника. У извештају *Reducing Overclassification* (2012) и препорукама *Modernizing the Classification System* (2020), PIDB упозорава да систематска прекомерна класификација ослабљује управљање безбедношћу, подстиче институционалну апатију и доводи до „засићења“ система непотребно класификованим документима, што нарушава заштиту заиста осетљивих информација. **Reducing Overclassification Act (2010)** формално је признао проблем и увео обавезе федералним агенцијама за његово смањење – кроз обуку, стандардизацију и развој индикатора оптерећења система.

Овај приступ у потпуности је усклађен са Tshwane Principles, који наглашавају да се тајност може оправдати само постојањем стварне, конкретне и вероватне штете, уз временско ограничење, независни надзор и заштиту информатора.

Европски приступи - Иако Европска унија и НАТО не користе формални термин „over-classification“, њихови нормативни оквири систематски одбацују праксе које тај појам описује: неоправдану, произвољну или рутинску класификацију информација које не представљају стварну безбедносну претњу. Овај приступ је у складу са Tshwane Principles (2013), који утврђују да се ограничења приступу могу увести само у случају конкретне, вероватне и идентификоване штете, а не на основу апстрактних ризика. Tshwane Principles такође инсистирају на заштити узбуњивача, што је Европски парламент додатно учврстио Резолуцијом о заштити информатора из 2020.

У оквиру ЕУ, правни темељ за управљање тајним информацијама представља **Council Decision 2013/488/EU**, конкретизована кроз **EU Security Rules for Protecting EU Classified Information (C(2019) 6110)**. Систем обухвата четири нивоа класификације – од EU TOP SECRET до EU RESTRICTED – уз обавезу да се свако одређење заснива на „конкретној и вероватној штети“. Правила предвиђају аутоматску декласификацију након 10 или 15 година, обавезну обуку службеника и увођење унутрашњих безбедносних ревизора у институцијама.

Посебна пажња посвећена је дигиталној заштити тајних информација – стандардима за електронску обраду, шифровање, контролу приступа и заштиту од сајбер-претњи – што је пресудно у ери хибридних ризика. Додатно, тела као што су **INTCEN (Европски центар за обавештајне и ситуационе анализе)** и **SIAC (Јединствена способност обавештајне анализе)** примењују јединствене протоколе за заједничко руковање осетљивим информацијама.

Националне праксе значајно варирају: шведски **Offentlighetsprincipen** подразумева претпоставку јавности свих докумената, док Немачка балансира између **BDSG** и закона о слободи информација. Податци **RAND-a** и **CSIS-a** показују да прекомерна класификација генерише милионске трошкове, а **Global RTI Rating** указује да земље са високим нивоом тајности имају слабије антикорупцијске показатеље.

НАТО систем - има један од најстроже уређених система управљања тајношћу, дефинисан у **Allied Administrative Publication AAP-06 „Security Policy“ (2023)** и

допуњен **NATO Information Management and Security Policy**. Систем НАТО предвиђа четири нивоа класификације – **COSMIC TOP SECRET, SECRET, CONFIDENTIAL и RESTRICTED** – док се **NATO UNCLASSIFIED** не сматра делом режима тајности.

Класификација је директно повезана са техничким безбедносним захтевима: изолованим мрежама, мултифакторском аутентификацијом, шифровањем у транзиту и миру, системима за детекцију интрузија и сајбер-инциденте. Пратећи документи, укључујући **NATO Cyber Defence Policy** и **NATO Classification Guide for Cyber Defence**, прецизирају третман информација у домену сајбер-операција и критичне инфраструктуре.

Принцип **need-to-know** је централни – приступ информацијама је ограничен само на лица чија је улога непосредно повезана са садржајем информације, што значајно смањује унутрашње ризике од злоупотребе или случајног откривања. Надзор врше **NATO Security Committee** и **Information Assurance Board**, уз редовне аудите у државама чланицама.

Посебно значајан механизам је **EU–NATO Structured Dialogue on Cyber Defence** (од 2016, интензивиран 2023), који усклађује приступе заштити информација и хибридним претњама. Заједничке вежбе, размена пракси и стандардизација дигиталне заштите осигуравају оперативну компатибилност и међусавезничко поверење.

Критички поглед на Уједињено Краљевство као неадекватан модел за земље Балкана - Иако формално поседује развијен систем правне регулације, Уједињено Краљевство не представља погодан модел за земље Балкана, нарочито не за Републику Србију у процесу европских интеграција. Његов дуални систем – који комбинује **Official Secrets Acts** (строге санкције за „процурење“ тајних информација) и **Freedom of Information Act 2000** (право на приступ информацијама) – у пракси функционише у дубокој тензији, често у корист режима тајности.

Кључни проблем британског модела је институционално ослобођење извршне власти од ефикасног надзора. Министарства рутински одбијају захтеве за приступ информацијама под општим изговором „националне безбедности“ или „заједничког интереса Краљевства“, често без конкретне процене штете или образложења. Иако постоји **Information Commissioner's Office (ICO)**, његове одлуке су ретко извршне, а министарства имају широка дискрециона овлашћења да супротставе своје процене надзорним телима. Последица је да се правно гарантовано „право на информације“ у многим областима – од јавних набавки до спољне политике – претвара у формалност.

Недавни примери, попут одбијања објаве детаља уговора са компанијом **AstraZeneca** током пандемије под изговором „конфиденцијалности пословне тајне“, иако су уговори били финансирани државним новцем, илуструју како се безбедносни и комерцијални изговори користе као алтернатива транспарентности, а не као изузетак заснован на стварном ризику. Таква пракса, која је у складу са британском традицијом егзекутивног првенства над парламентарном контролом, јасно супротставља европској логици: у ЕУ је транспарентност правило, а тајност изузетак, док је у УК обрнуто.

Земљама попут Републике Србије, које формално теже европским стандардима, али стварно морају да превазиђу инерцију културе тајности као инструмента контроле, британски модел не нуди решења – већ упозорење. Механичко преузимање елемената

попут „поверљивости у јавним набавкама“ или „широке тумачења националног интереса“ може само продубити постојеће злоупотребе. Уместо УК, референтни модел треба бити Скандинавија, где је „јавност као правило“ уткана у институционалну и културну ДНК, или ЕУ систем, где је свака одлука о тајности подвргнута ревизији, временском року и начелу пропорционалности.

Остали модели и компаративни оквири - Ван трансатлантског простора, више земаља развило је моделе који нуде значајне компаративне увиде. Канада, за разлику од УК, јасно раздваја **Access to Information Act** и **Security of Information Act**, уз снажан надзор информационог комесара – модел који омогућава јасну дистинкцију између безбедносне заштите и управљања информацијама.

У транзиционим земљама, искуства су варијабилна. Балтичке државе (Естонија, Летонија, Литванија) примењују минималну неопходну тајност и дигиталну транспарентност, док Украјина и земље западног Балкана често задржавају културу тајности као политички инструмент, посебно у одбрани, безбедности и јавним набавкама. OECD препоруке истичу нужност промене организационе културе – од „тајност као норма“ ка „тајност као изузетак“.

Технолошки изазови додатно компликују ситуацију: аутоматизовани системи и AI алгоритми често погрешно класификују документе због недостатка контекста, док дигитално архивирање омогућава бржу декласификацију, али захтева техничку инфраструктуру која у многим земљама још увек није доступна.

Појава дигиталних платформи као што су **WikiLeaks** и **DDoSecrets** доводи у питање државну монополизацију информација. Иако контроверзне, ове платформе показују да у доба глобалне комуникације тајност више није гаранција безбедности, већ изазов за управљање поверењем и институционалном веродостојношћу.

Проблем, дакле, не лежи у самом постојању режима тајности – који је суштински и неопходан за функционисање савремених безбедносних и одбрамбених система – већ у начину његове примене. Злоупотреба настаје онда када недостају конзистентна процена ризика, јасна методологија, временско ограничење и функционалан, независан надзор – услови који се у међународној пракси, од Вашингтона до Брисела, сматрају минималним стандардима доброг управљања тајним информацијама у дигиталном добу.

Стога, кључно није питање да ли тајност треба да постоји, већ да ли је сваки појединачни случај тајности оправдан, документован, временски ограничен и подвргнут надзору. Оног тренутка када тајност престане да служи државном интересу и почне да функционише као средство управљања перцепцијама, она губи легитимност – а са њом и веродостојност целокупног система безбедносне заштите. У том смислу, стандарди **ЕУ, НАТО-а и САД** нису само оквири за заштиту информација, већ и механизми за осигурање демократске одговорности, институционалног интегритета и отпорности на хибридне претње – нарочито у земљама у транзицији, где је баланс између безбедности и транспарентности посебно осетљив и политички значајан.

Политички аспекти режима тајности у Републици Србији – између легитимне заштите и ризика злоупотребе

Режим тајности података представља кључни инструмент за заштиту националних интереса, али у Србији често прераста у механизам ограничавања транспарентности и демократског надзора. Наслеђе југословенског система, комбиновано са фрагментираном државном управом и недовољном институционалном контролом, ствара простор за прекомерну класификацију информација – феномен познат као „over-classification“. Ова анализа истражује историјске, институционалне и политичке изазове у примени Закона о тајности података, упоређујући их са међународним стандардима (Tshwane Principles, ОЕБС препоруке, европска пракса) и предлагањем мера за успостављање баланса између безбедности и одговорности.

Структурна наслеђеност и фрагментација система заштите тајних података - Проблеми у примени режима тајности у Србији нису само резултат тренутних политичких или административних пракси, већ дубоко укорењених институционалних и историјских трајекторија. Наслеђе система заштите тајних података, изведено из концепта „Општенародне одбране и друштвене самозаштите“ СФРЈ, није адекватно трансформисано током 1990-их. Напротив, дошло је до деструкције уређених капацитета: формално задржан систем рада са тајним подацима није праћен адекватном инфраструктуром, кадровском обуком или јединственом методологијом. Истовремено, целовита државна управа није један систем, већ скуп аутономних субсистема – одбране, полиције, дипломатије, служби безбедности, судства, канцеларијског пословања, па чак и локалне самоуправе – од којих сваки има сопствене прописе, нормативе и културе рада са тајним подацима, често засноване на архаичним актима из периода СФРЈ или СРЈ.

Посебно проблематично је стање у „осталој“ државној управи (попут министарстава здравства, правде или пољопривреде), где се категорија „службене тајне“, која ни по природи ни по обиму не испуњава услове Закона о тајности података, користи као паралелни режим ограничења приступа информацијама. То доводи до ситуације да се подаци о здравственом стању пацијената, пореским обвезницима или пољопривредним сортама третирају као „тајни“, иако немају никакве везе с легитимним интересима националне безбедности.

Таква фрагментација ствара правну неизвесност, произвољност у одређивању тајности и простор за злоупотребу, јер сваки сектор може да примењује своју интерпретацију „националног интереса“ без координације са централним надзорним телима, а неретко и у супротности са принципима члана 8. Закона. Без јединствене методологије процене ризика, јединствене културе професионалне одговорности и технички опремљене Управе за заједничке послове, тајност постаје не функција заштите, већ функција административне инерције, страха или политичких потреба.

Режим заштите тајности у Републици Србији, као и у већини држава, има двоструку и у суштини комплементарну сврху:

- Заштитити стварне интересе јавних политика – националну безбедност, одбрану, унутрашње и спољне послове – укључујући оперативне податке и изворе информација обавештајно-безбедносних структура и полиције, планове одбране,

опремање и употребу војске, кибернетичке ризике, процене претњи по националну безбедност и осетљиве дипломатске преговоре.
- Обезбедити транспарентност и одговорност у свим другим областима јавног интереса, где не постоји реална опасност по државу, институције или грађане.

Међутим, у пракси се често дешава да се правно предвиђени изузетак – тајност – третира као правило. Овај тренд одговара глобално дефинисаном феномену „over-classification“, али у српском контексту добија посебну димензију услед сложене структуре државне управе и институционалне асиметрије између њених делова. Србија поседује двокомпонентну управну архитектуру: с једне стране, институционални оквир (министарства, специјализоване службе, органи, окрузи и други органи јавне власти) организован је по централно-егзекутивном (француском) моделу, што чини тајност лако доступном као алатом егзекутиве; с друге стране, јавни службеници су, у складу са Законом о јавним службеницима и европском праксом, формално устројени по немачком правном моделу – као професионалци који треба да делују независно од политичких промена, у складу са начелима законитости, пропорционалности и неутралности. У теорији, овај дуализам треба да обезбеди равнотежу између политичког вођства и професионалне, правно ограничене примене режима тајности. У пракси, међутим, та равнотежа се често не остварује, што ствара простор за произвољну класификацију под политичким или административним притиском, уз слабу унутрашњу контролу професионалних стандарда.

Ово производи ризик двоструког поремећаја у систему: • Прво, ослабљује се ефикасност стварне заштите: када се све означава као „тајно“, категорија губи веродостојност, а критични подаци не добијају пажњу коју заслужују. • Друго, неоправдано се ограничава могућност демократског надзора у областима где он не сме бити угрожен – финансије одбрамбених набавки, енергетски пројекти од јавног значаја, управљање јавним ресурсима и спровођење политика у областима безбедности, здравства или инфраструктуре – што је посебно истакнуто у препорукама Групе држава против корупције (GRECO) и ОЕБС-а, који упозоравају да таква пракса слаби антикорупцијске механизме и подрива принцип одговорности.

Ово није питање „анти-државне агенде“, већ питање функционалног држављанства и здраве демократске праксе. У том смислу, *Tshwane Principles on National Security and the Right to Information* (2013), као и ОЕБС-ове препоруке о националној безбедности и транспарентности, нуде универзални тест: тајност мора проћи строгу проверу јавног интереса, која подразумева да (1) постоји стварна, конкретна и вероватна штета од откривања; (2) заштита тог интереса претеже над правом јавности да зна; и (3) ограничавање приступа је неопходно у демократском друштву — што значи да не постоји блажи начин да се постигне исти циљ. Овај приступ је део међународних обавеза Србије као чланице ОЕБС-а и Уједињених нација, а не само „западни идеал“.

Кључни изазови у систему

Институционална асиметрија – органи који одређују степен тајности често нису подвргнути ефикасној унутрашњој контроли која би систематски преиспитивала оправданост класификације. Недостатак хоризонталне и вертикалне контроле — од унутрашњих ревизија, преко инспекцијског надзора, до парламентарних одбора — омогућава простор за произвољност и злоупотребу без последица. За разлику од система у државама чланицама Европске уније, где постоје унутрашњи безбедносни ревизори и

независни надзорни органи, српски систем нема формализован механизам за независну ревизију одлука о тајности. Без таквог механизма, одлука о тајности постаје питање административне удобности, а не стварне безбедносне потребе.

Неуједначена пракса - у пракси се дешава да се степен тајности додељује без свеобухватне и адекватне процене ризика предвиђене чланом 8. Закона о тајности података. Тако се чак и економски, административни или технички подаци означавају као „тајни“, иако њихово објављивање не би проузроковало никакву штету држави. Овакво проширење обима тајности поткопава поверење јавности и функционалност система, јер се тајност претвара у општу категорију уместо да остане прецизно ограничена мера у складу с природом ризика. Ово директно крши принципе Конвенције Савета Европе о приступу службеним документима (Тромсе конвенција), коју Србија, као чланица Савета Европе, има обавезу да имплементира.

Колизија закона: слобода приступу информацијама од јавног значаја на удару - кључни проблем у пракси представља недовољно усклађен однос између Закона о слободном приступу информацијама од јавног значаја и Закона о тајности података. Иако Закон о слободи информација предвиђа широк приступ, одлуке о тајности често се доносе ретроактивно или без образложења, чиме се фактички онемогућава примену права на информације. Ово је у супротности с препорукама УНЕСКО-а (UNESCO) и резолуцијама Парламентарне скупштине Савета Европе, које истичу да тајност не сме бити коришћена као апсолутан изузетак од правила транспарентности.

Међународна сарадња и неадекватна транспозиција стандарда - иако Србија није чланица НАТО-а, већ учесник програма Партнерство за мир (Partnership for Peace – PfP), у пракси се често дешава да се стандарди попут AAP-06 или НАТО класификационог система примене механички, без адаптације на домаћи правни поредак. Посебно је проблематично када се домаћи документи класификују искључиво зато што садрже референцу на НАТО или документ Европске уније, а не због стварне осетљивости. У таквим случајевима домаћа процена ризика не постоји, а примена страног стандарда постаје изговор за затварање информација. Иако НАТО директно не надзире српски систем, као кандидат за чланство у Европској унији Србија има обавезу да усвоји европске стандарде управљања тајним информацијама - укључујући принцип пропорционалности и временско ограничење - у оквиру Поглавља 23 (Правосуђе и основна права) и Поглавља 30 (Спољна, безбедносна и одбрамбена политика).

Дигитализација и нови изазови - у ери дигитализације државне управе, када се све више докумената креира, чува и размењује електронским путем, проблем прекомерне класификације добија нову димензију. Србија је у фази имплементације е-архива, е-управе и националног система за кибер безбедност, али без јасних протокола за дигиталну класификацију, шифровање и контролу приступа, ризик од цурења или, супротно, произвољног закључавања информација расте. У том контексту, сајбер безбедност не треба замењивати „тајношћу“, већ развијати техничке мере заштите (мултифакторска аутентификација, изоловани – air-gapped – системи за најосетљивије податке) које обезбеђују и безбедност и, где је могуће, транспарентност. Ово је у складу с европским оквиром за кибер безбедност и стратегијом дигиталне трансформације коју Србија активно усваја као део европских интеграција.

Кризне ситуације и информациони рат - у временима појачаних хибридних претњи, миграционих таласа или политичких турбуленција, јавља се тенденција да се режим

тајности користи као механизам управљања информационим токовима. У таквим околностима граница између легитимне оперативне потребе и политичке контроле јавности постаје нејасна — што може произвести дугорочну штету институционалном интегритету. *Tshwane Principles* и препоруке ОЕБС-а истичу да управо у „изузетним околностима“ мора постојати јачи, а не слабији надзор, јер је ризик од злоупотребе тада највећи.

Ово није оптужба против система националне безбедности или институција, већ позив на њихово унапређење кроз доследнију, строжију и аналитички засновану примену постојећих критеријума. Постоје области у којима је тајност не само оправдана већ и неопходна: • заштита извора и метода у борби против организованог криминала и тероризма; • очување интегритета критичних инфраструктура; • ситуације у којима би објављивање информација онемогућило супротстављање противнику или угрозило позицију државе у међународним преговорима.

Проблем, дакле, није у постојању режима тајности као таквог, већ у недовољно строгом придржавању законских принципа „стварне штете“ и „претежног државног интереса“, који би требало да буду основни филтери за одређивање тајности или класификацију. Режим тајности мора бити:

- **тачан** - заснован на методолошки уређеној, прецизној и професионалној процени ризика, у складу с *Tshwane Principles*, препорукама ОЕБС-а и европском праксом;
- **временски ограничен** - уз редовно преиспитивање оправданости, јер тајност која не зна када да престане угрожава саму себе - што је основни принцип аутоматске декласификације у Европској унији (10–15 година);
- **пропорционалан** - ни више ни мање него што је неопходно.

Премало тајности угрожава безбедност; превише тајности подрива демократски надзор. Успешан систем није онај који крије све, већ онај који зна шта заиста мора да заштити - и зашто. Овакво уређење режима тајности не подрива државу, већ јој даје алате да буде јача, легитимнија и одговорнија, без компромитовања сопствених безбедносних интереса - јер се у демократском друштву легитимност тајности не мери тиме колико се крије, већ тиме колико је прецизно, привремено и оправдано образложена.

У том смислу, усвајање међународних стандарда није спољни притисак, већ стратешка потреба у процесу изградње демократског друштва у складу с европским вредностима - процес у који је Србија, као званични кандидат за чланство у Европској унији, дубоко укључена. Успостављање институционалне равнотеже између централно-егзекутивне структуре и професионалног, правно ограниченог понашања службеника представља кључни предуслов за исправну примену тајности - не као алат управљања информацијама, већ као прецизно, временски ограничено и проверљиво средство заштите стварних државних интереса.

Правни аспекти злоупотребе у одређивању и означавању тајних података

Примена режима тајности у Републици Србији мора бити у складу са принципима законитости, пропорционалности и неопходности, који су утврђени Законом о тајности података. Ипак, у пракси се често јављају значајна одступања од ових принципа, што доводи до правног нереда, институционалне недоследности и ослабљења легитимитета

читавог система заштите података. Иако сам закон предвиђа да се као тајни податак може одредити 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 (чл. 8. ст. 1 ЗТП), ова одредба није реторичка формулација, већ обавезан правни филтер. Како истиче теорија, испуњење услова из члана 8. захтева документовану процену стварне, конкретне и вероватне штете, као и тест претежности у складу са стандардима демократског друштва — што значи да ограничавање приступа мора бити неопходно, а не само погодно. Најчешћи облици правне злоупотребе укључују:

- **Непоштовање принципа пропорционалности и нужности** – Степен тајности се понекад додељује без стварне процене да ли би објављивање информације могло нанети штету интересима националне безбедности. Уместо утемељене анализе ризика, класификација се примењује рутински, често ради административне удобности или прикривања недовољне транспарентности. У таквим случајевима, одлука о тајности није само неовлашћена – она је правно ништавна, јер не испуњава услове из члана 8. Закона.
- **Одређивање тајности ван законом предвиђених критеријума и рокова** – Ознаке тајности се понекад додељују подацима који очигледно не спадају у заштићене категорије (чл. 8. ст. 2 ЗТП), или се рокови трајања тајности произвољно продужавају без одговарајућег образложења. Такве праксе нарушавају основни принцип контролисане и временски ограничене класификације. Посебно је озбиљно када се тајност додели информацијама које су јасно забрањене за класификацију чланом 3. Закона, јер тада одлука није само неправна, већ може чинити елемент кривичног дела, попут злоупотребе положаја.
- **Неадекватна употреба ознаке „Интерно“** – Ознака „Интерно“, иако је део формалног режима тајности, често се користи као општа категорија за све осетљиве информације. Ова пракса потиче из правног наслеђа претходног система и данас служи као механизам избегавања обавезе достављања информација у поступку слободног приступа. Таква употреба ознаке ствара паралелни, нелегитимни режим ограничења приступа, који заобилази и Закон о тајности података и Закон о слободном приступу информацијама, али се ретко санкционише.
- **Недовољна примена механизама престанка тајности** – Ознака тајности се често задржава и након истека законског рока, наступања догађаја на који се односила, или чак након одлуке Канцеларије Савета за националну безбедност и заштиту тајних података, решења Повереника или одлуке надлежног суда, у складу са одредбама из чл. 17–25. Закона о тајности података. Задржавање тајности без правног основа нарушава принцип периодичног преиспитивања оправданости одређивања тајности. Како проф. Матић наглашава, тајност која не зна када да престане, угрожава саму себе, јер тиме губи сваку везу са привременом и исцрпном природом режима тајности.

Један од кључних проблема јесте одсуство ефикасних санкција за службена лица која неосновано одреде, означе или задрже тајност. Иако Закон о тајности података прецизно регулише услове за одређивање тајности или класификацију, он не предвиђа кривичну одговорност за прекомерно означавање. Члан 98. санкционише искључиво незаконито откривање или прибављање тајних података, али не и њихову неоправдану или злоупотребљену заштиту. Ипак, у одређеним ситуацијама могу се применити друга

кривична дела, када злоупотреба тајности представља сегмент ширег незаконитог деловања:

• **Злоупотреба службеног положаја (чл. 359. КЗ)** – ако се овлашћење за одређивање тајности или класификацију користи ради прикривања штетних радњи, незаконите користи или неправилности.

• **Несавестан рад у служби (чл. 361. КЗ)** – када надлежно лице поступа изван дозвољених законских оквира, било кршењем закона или других општих прописа или аката, односно ако очигледно несавесно поступа у служби.

• **Фалсификовање службене исправе (чл. 357. КЗ)** – ако се лажно уносе подаци о степену тајности ради прикривања садржаја документа.

Ова дела добијају јасну коруптивну димензију када се тајност користи као алат за:

- прикривање финансијских токова у јавним набавкама,
- ограничавање контроле над фаворизованим добављачима,
- скривање договора у вези са примањем мита (чл. 367–368. КЗ),
- утицај на исход јавних набавки или кадровска решења путем трговине утицајем (чл. 366. КЗ).

Упркос постојању норми које омогућавају санкционисање прекомерног означавања, њихова примена је ретка. Додатно, недовољно функционише прекршајни систем одговорности. Члан 99. Закона о тајности података прописује 17 прекршаја повезаних са неправилном применом режима тајности, укључујући:

- неоправдано означавање тајности (чл. 8. ст. 2),
- погрешан или неодговарајући степен тајности података (чл. 11. ст. 2),
- доношење одлуке о одређивању тајности без образложења (чл. 11. ст. 4),
- непредузимање периодичне процене ризика (чл. 22),
- неопозивање тајности по решењу Повереника или одлуци суда (чл. 25),
- непримењивање општих и посебних мера заштите (чл. 32–33),
- непоштовање режима страних тајних података (чл. 94).

За ове прекршаје прописане су новчане казне од 5.000 до 50.000 динара за одговорно лице у органу јавне власти, као и за руковаоца тајним подацима који не предузме потребне мере заштите (чл. 100). Иако формално предвиђене, ове санкције у пракси имају ограничен превентивни ефекат, управо због ретке примене. Додатни проблем представља и ограничена судска заштита. У пракси је изузетно тешко преиспитати оправданост одређивања тајности или класификације, јер су судовима често недоступни релевантни материјали, поступци трају дуго, а процесне баријере одвраћају странке од покретања спорова. Последица је да се одлуке о одређивању тајности или класификацији ретко стављају под ефективан правни надзор, чиме се угрожава право на слободан приступ информацијама од јавног значаја.

Постоји и проблем колизије закона. Закон о слободном приступу информацијама од јавног значаја може бити практично обеснажен ако се ознака тајности користи као инструмент за избегавање обавезе достављања информација. Иако су предвиђене санкције за непоступање по решењу Повереника, оне се ретко примењују.

Сличне слабости постоје и у Закону о одбрани, који прописује прекршаје у вези са руковањем тајним подацима у систему одбране – од неправилног складиштења до недозвољеног располагања документима и приступа без сертификата. Међутим, и ту је примена правила ограничена, а санкције често имају више формалан него превентиван ефекат.

Институционални изазови у Републици Србији

Примена режима тајности у Републици Србији суочава се са бројним структурним и функционалним ограничењима која омогућавају не само неадекватну примену, већ и злоупотребу законских одредби. Ови проблеми не произилазе из недостатка правног оквира, већ из слабе институционалне културе, неуједначене праксе, ограничених капацитета и недовољно ефикасног надзора. Када се ови изазови посматрају у дубљем аналитичком контексту, посебно кроз призму јавне политике као организованог, стручног и институционализованог одговора државе на конкретна друштвена питања, они указују на системски недостатак интегрисаног механизма који би спојио правни, оперативни и контролни аспект управљања тајним подацима, чиме се ствара простор за произвољне интерпретације и неједнак третман докумената различитих органа.

У том смислу, тајност мора бити део безбедносне политике као облика јавне политике, а не алат административне или политичке контроле. Јавна политика се, за разлику од опште политике, бави управљањем и решавањем стварних проблема кроз институционално утемељене, транспарентне и одговорне механизме. Када тајност постане одступање од ове логике, она више не служи држави, већ државним органима.

Један од основних изазова јесте недовољна обука јавних службеника и функционера надлежних за одређивање степена тајности. Без систематске и стандардизоване едукације, лица која доносе одлуке о одређивању тајности често немају довољно знања о критеријумима из Закона о тајности података, посебно о процени могуће штете, принципу пропорционалности и потреби документованог образложења. Такве околности доводе до тога да се тајност третира као административна формалност, а не као инструмент заштите конкретних безбедносних интереса. Аналитички гледано, ово значи да се институционални капацитети не само да не развијају у правцу стратешког управљања информацијама, већ и стварају структурне слабости које директно утичу на кредибилитет и легитимност целог система.

Овај приступ је у изразитој супротности са европском праксом, где су обука и сертификација службеника који раде са тајним подацима обавезни елементи, као што је предвиђено у „EU Security Rules for Protecting EU Classified Information“ (C(2019) 6110). Слично томе, ОЕБС и Савет Европе истичу да „ефикасна заштита тајних информација претпоставља професионалну, а не произвољну, класификацију“. Овде се појављује важна аналитичка порука: формална усаглашеност са прописима није довољна ако не постоји дубински имплементиран професионални стандард који интегрише правну строгоћу са практичном применом у различитим институционалним контекстима.

Постоји значајна варијабилност у пракси различитих органа – полиције, Министарства одбране, БИА, Министарства спољних послова и других министарстава, који често дају различите интерпретације истог закона. То резултира непредвидивошћу: исти тип документа може бити одређен и означен као тајни у једном органу, док је у другом доступан без ограничења. Оваква неуједначеност ослабљује кредибилитет система и

отвара простор за произвољност. Са аналитичког аспекта, непостојање јединственог методолошког оквира значи да нема механизама који би објективно елиминисали ризик селективне или политички мотивисане класификације, што директно утиче на перцепцију јавности и међународних партнера о функционалности система.

Посебно проблематичан фактор представљају неформални утицаји на одлуке о одређивању тајности. Ове одлуке у бројним случајевима не заснивају се на безбедносној процени, већ на политичким, администрацијским или институционалним разлозима, било ради управљања информационим токовима, контроле јавне перцепције или заштите појединих лица од политичке или службене одговорности. Ово је у директној супротности са Tshwane Principles и Истанбулском хартијом за безбедност ОЕБС-а (1999), која изричито упозорава да „национална безбедност не сме бити коришћена као оправдање за прикривање корупције, злоупотребе власти или других пропуста у јавној управи“. Аналитички, ово указује на дубљи структурни проблем: одлуке о тајности уместо да штите државне интересе, могу постати инструмент политичке управљачке моћи. Кључна институционална слабост огледа се и у недовољној улози надзорних актера:

- **Министарство правде**, као инспекцијски орган, изузетно ретко спроводи активну проверу оправданости одређивања тајности, за разлику од ЕУ праксе, где су инспекције редован и систематски део надзора. Ово указује на потребу за институционалним механизам који осигура континуитет и доследност контроле.
- **Канцеларија Савета за националну безбедност и заштиту тајних података**, иако стручна служба Владе Републике Србије и формално надлежна за координацију, углавном делује административно, без снажнијег стратешког ангажмана у преиспитивању донетих одлука. Аналитички, ово открива празнину између формалне надлежности и стварног стратешког утицаја на управљање тајним информацијама.
- **Безбедносно-информациона агенција (БИА)** има ограничену улогу у непосредном надзору процеса одређивања тајности, упркос централној улози у заштити свих осетљивих података. Недостатак интегрисаног механизма сарадње између БИА и других надзорних актера повећава ризик да кључни безбедносни подаци буду погрешно или произвољно категорисани.

Додатно, у систему недостаје јединствен методолошки стандард процене ризика (risk assessment framework). Иако закон прописује да се тајност може одредити само ако је потреба за заштитом интереса државе претежнија од интереса јавности да зна (чл. 8. ст. 1 ЗТП), у пракси процена ризика често није документована, нити се спроводи по јасним критеријумима. Ово указује на фундаментални институционални недостатак: одлуке се доносе без објективне потврде оправданости, што ствара простор за неједнак третман и поткопава легитимитет система у очима јавности и међународних партнера. Европска унија је развила стандардизоване калибрисане матрице ризика за све нивое класификације, што значајно смањује могућност субјективних одлука и омогућава конзистентну примену правила – пример који указује на потребу систематског трансфера знања и стандарда.

Типични модели злоупотребе у пракси - Системска природа проблема може се илустровати кроз понављајуће моделе злоупотребе:

- Одређивање тајности великих инфраструктурних пројеката (енергетика, логистика), иако садржај нема стварне везе са националном безбедношћу, чиме се избегава јавна расправа о финансијским и техничким аспектима.
- Означавање пословних уговора са страним партнерима као „тајних“, често мотивисано комерцијалним, а не безбедносним разлозима.
- Скривање интерних извештаја о корупцији под ознаком тајности, супротно препорукама GRECO-а, што онемогућава антикорупцијски надзор.
- Продужавање „привремене тајности“ током година без ревизије, у супротности са ЕУ системом аутоматске декласификације.
- Ретроактивна класификација докумената након што су већ постали јавни, као реакција на медијски интерес.
- Масовно означавање докумената након политичких смена, ради контроле информација о претходним руководствима.

Последице злоупотребе - Системска злоупотреба режима тајности производи трајне негативне ефекте:

- Смањује поверење јавности у институције, нарочито у безбедносни сектор и правосуђе.
- Успорава борбу против корупције јер кључни извештаји остају недоступни.
- Ограничава транспарентност у управљању јавним средствима, онемогућавајући ефективну парламентарну и грађанску контролу, нарочито у пројектима финансираним из ЕУ фонда.
- Нарушава међународну сарадњу јер партнери наилазе на непредвидљивост у приступу документима, што представља препреку европским интеграцијама.
- Производи феномен „ерозије тајности“: када се ознака злоупотребљава, слаби њена вредност и веродостојност, што угрожава заштиту стварно осетљивих података.

Мере за спречавање злоупотребе - Да би режим тајности био легитиман, функционалан и конзистентан, неопходно је:

- Увођење стандардизованог модела процене ризика, обавезног за све органе у поступку класификације – у складу са европским примерима и Tshwane Principles.
- Јачање надзорних механизама, укључујући независне инспекције, парламентарни надзор и унутрашње контролне линије у органима јавне власти.
- Строга примена принципа „јавно је правило, тајно је изузетак“, у складу са чланом 8. ст. 1. Закона о тајности података и Тромсе конвенцијом Савета Европе.
- Објављивање јавних образложења за одлуке о класификацији, без откривања садржаја, али са јасним навођењем природе ризика и основа за процену.
- Аутоматска ревизија и декласификација по истеку рока, без потребе за додатном одлуком - кључни елемент EU Security Rules.
- Обавезна едукација и обука свих службеника и функционера који раде са тајним подацима, уз сертификацију за лица са приступом врхунски осетљивим информацијама.
- Јачање улоге Канцеларије Савета за националну безбедност и заштиту тајних података, укључујући проширење овлашћења за преиспитивање одлука о одређивању тајности и санкционисање поступања супротних закону — у складу са улогом унутрашњих безбедносних ревизора у ЕУ институцијама.

Пример из праксе: Одређивање тајности уговора о набавци кинеских ПВ-9 бронетранспортера као „Строго поверљиво“ - У октобру 2021. године Министарство одбране Републике Србије закључило је уговор о набавци 16 оклопних возила ПВ-9 (кинески *Type 08*) у вредности од око 50 милиона долара, финансиран кредитом Кине. Ова набавка је привукла значајну пажњу јавности због свог стратешког значаја, геополитичког контекста и недостатка транспарентних информација о процени потреба Војске Србије. Након појављивања фотографија возила у медијима, организација KRIK поднела је захтев за приступ кључним подацима: тексту уговора, ценама, условима испоруке и гаранције, техничким спецификацијама, као и образложењу оперативне потребе. У фебруару 2022. Министарство одбране одбило је захтев, образлажући да су сви документи одређени степеном тајности или класификовани као „Строго поверљиво“ због „интереса безбедности и одбране“. Међутим, процена ризика и детаљно образложење одређивања тајности или класификације, обавезни елементи по Закону о тајности података, нису достављени, што указује на непотпуно придржавање законских процедура.

Повереник за слободан приступ информацијама, у решењу бр. 437/22 из марта 2022. године, утврдио је да одређивање тајности или класификација није била оправдана у делу који се односи на финансијске и уговорне параметре, који ни по једном критеријуму не представљају оперативно осетљиве податке. Повереник је наложио делимичну декласификацију или престанак тајности. Иако је Министарство формално поступило по решењу, достављени материјал је био обимно редигован, са великим „црним блоковима“, чиме је онемогућена суштинска употреба информација. На овај начин правно испуњавање обавезе није довело до реалне транспарентности. Додатни проблем, који има и аналитичку тежину, јесте чињеница да су техничке карактеристике возила и општи услови набавке већ били јавно доступни, јер су их објавили кинески произвођачи и бројни међународни медији. Упркос томе, домаћа јавност, као и парламентарни Одбор за одбрану, и даље немају увид у кључне елементе уговора: трошкове одржавања, структуру кредитних услова, реалну укупну вредност и параметре испоруке. Према оценама независних аналитичара, наведене цене су видљиво више у односу на сличне уговоре у региону, што додатно повећава потребу за транспарентним увидом и јавним надзором.

Овај случај јасно илуструје системски лош приступ режиму тајности, односно погрешну примену прописа: не ради заштите безбедности или оперативних капацитета, већ ради ограничења јавног увида у значајне финансијске трошкове и политичке одлуке. Функционално, ово доводи до слабљења демократског надзора, док на симболичком нивоу производи „инфлацију тајности“, ситуацију у којој ознаке тајности губе тежину, а стварно осетљиви подаци постају мање заштићени због прекомерне употребе одређивања тајности или класификације у областима где она није оправдана.

Извори

- Решење Повереника за слободан приступ информацијама, бр. 437/22, 28.03.2022.
- KRIK: *„Zašto su ugovori o nabavci kineskih tenkova 'strogo poverljivi'?“*, 15. фебруар 2022.

- Balkan Insight: *„Serbia's Chinese-Made Armoured Vehicles Arrive Amid Secrecy"*, 18. новембар 2021.
- BETA Ekonomika: *„Nabavka oklopnih vozila: Koliko košta PV-9?"*, 2022.

Заједнички проблеми у региону: баланс између транспарентности и безбедности - изазов демократске зрелости

Питање режима тајности у југоисточној Европи превазилази формалну и техничку примену законских одредби и директно се уплиће у ткиво демократског развоја, као и у степен прилагођавања евроатлантским стандардима. У контексту чланства или кандидатура за ЕУ и НАТО, пракса класификације информација више није искључиво питање националне безбедности — већ постаје мерљив индикатор институционалне отворености, ефективности надзора и спремности власти да преузму одговорност према јавности. Формално усвајање закона није довољно: стварни тест лежи у доследној примени принципа владавине права, прозрачности и равнотеже између извршне, законодавне и надзорне власти. Начин, интензитет и мотивација којима се користи категорија тајности одсликавају доминантну политичку културу, да ли је она заснована на међусобном поверењу, провери и дијалогу са грађанима или на затвореној логици информационе контроле и избегавања јавне одговорности.

Прекомерна класификација, ретроактивно проглашавање података за тајне, као и масовно означавање јавних уговора, нису административни пропусти, већ системски феномени који активно ометају реформе безбедносног сектора, функционисање отвореног тржишта, ефикасну борбу против корупције и развој квалитетне јавне политике. Злоупотреба тајности директно подрива суштинске европске вредности: прозрачност, веродостојност институција и равнотежу између грана власти. Стога, способност државе да примењује тајност строго ограничено, временски условљено и на основу објективне, доказиве процене ризика, а не као општи алат управљања информацијама, постаје један од најзначајнијих показатеља институционалне зрелости и демократске легитимности.

Успешна интеграција у евроатлантске структуре захтева не само хармонизацију законодавства, већ и дубоку културну трансформацију: ка схватању да јавност није претња, већ активни партнер у одржавању стабилности, одговорности и дугорочне безбедности државе. Заштита легитимних државних интереса и право јавности да зна нису антагонистички принципи, већ комплементарни и међузависни стубови сваке зреле демократије. Њихов баланс није опционални компромис, већ предуслов за трајну сигурност, институционалну поузданост и поверење грађана у 21. веку.

Овај изазов није специфичан само за Западни Балкан. Шире регионално искуство — укључујући Румунију, Бугарску, Албанију, Грчку и Турску — указује на заједничке обрасце, са варијацијама у интензитету и степену институционалне консолидације:

- **Румунија и Бугарска**, иако дугогодишње чланице ЕУ и НАТО-а, и даље се суочавају са случајевима прекомерне класификације, посебно у доменима одбрамбених набавки, безбедносно-обавештајних процена и унутрашњих стратегија, често уз слабу улогу парламентарног надзора.

- **Албанија**, као чланица НАТО-а од 2009. године и кандидат за ЕУ, активно напредује у законодавној хармонизацији, али јој недостаје конзистентност у примени и развој независних надзорних институција које би обезбедиле спровођење промена у пракси.
- **Грчка** формално прати међународне норме, али независни извори и стручни извештаји указују на селективну употребу тајности у политички осетљивим контекстима, као што су миграциона криза, безбедносна сарадња и одлуке о унутрашњој безбедности.
- **Турска**, као стратешки партнер у региону, има формално строг систем заштите тајних података, али га у пракси често користи као инструмент безбедносне реторике у антитерористичким операцијама, уз систематско ограничење улоге парламента, медија и независних регулатора.

Слично томе, у државама насталим распадом Југославије - Словенији, Хрватској, Босни и Херцеговини, Црној Гори и Северној Македонији - правни оквири су у највећој мери усклађени са европским и евроатлантским стандардима. Ипак, у пракси се јављају структурни изазови у спровођењу кључних принципа: пропорционалности, нужности и временског ограничења тајности. Најзначајнији проблеми укључују:

- прекомерно означавање тајности или класификација информација које по својој природи не представљају безбедносни ризик - попут економских, административних, урбанистичких или еколошких података - често без формиране процене стварне штете коју би њихово објављивање могло изазвати;
- одсуство стандардизованог модела процене ризика, што доводи до фрагментиране и неусклађене праксе између различитих министарстава, безбедносних служби и нивоа власти, омогућавајући произвољност и дуплирање категорија;
- инструменталну употребу тајности у политички осетљивим ситуацијама, не због стварне безбедносне угрожености, већ као механизам за управљање јавном агендом, смањење медијске изложености или одлагање одговорности - на пример у случајевима скандала у јавним набавкама или преговора са страним партнерима;
- ограничену ефикасност надзорних тела, укључујући повереника за слободан приступ информацијама, надлежне парламентарне комисије и координационе органе за режим тајности, који често немају адекватна овлашћења, ресурсе или политичку подршку да своје препоруке спроведу у пракси;
- недовољну примењеност механизама декласификације, услед чега значајан број докумената остаје под ознаком тајности дуго након што су изгубили осетљивост, чиме се не само наноси штета транспарентности већ се и релативизује поузданост категоризације података који заиста захтевају заштиту.

Ови феномени не одражавају недостатак воље за усклађивање са европским стандардима, већ пре тешкоће у њиховој доследној, дубински усвојеној и културно укорењеној примени. Управо је процес превођења формалних норми у стабилну, одговорну и рефлексивну административну праксу највише изложен политичким и институционалним инерцијама. У томе лежи срж регионалног изазова: како нормативни минимум не претворити у пуку декларацију, већ у истинску културу одговорности - у којој тајност није алтернатива транспарентности, већ њен условљени и привремени изузетак, увек отворен за проверу, ревизију и одговорност.

Словенија: Развијен оквир и изоловане злоупотребе

Словенија поседује један од најразвијенијих и најформализованијих система заштите тајних података у региону Западног Балкана, у складу са својим статусом пуноправне чланице Европске уније и НАТО-а од 2004. године. Њен правни оквир - заснован на *Zakon o varstvu tajnih podatkov* (Закону о заштити тајних података) и усаглашен са EU Security Rules (C(2019) 6110) и НАТО-овим класификационим стандардима - предвиђа строге процедуре за процену ризика, временско ограничење тајности, обавезну обуку службеника и постојање централизованог надзора. У теорији, систем испуњава све услове које *Tshwane Principles* и ОЕБС сматрају минималним за демократску управу тајним информацијама: пропорционалност, конкретну штету, независан надзор и заштиту информатора.

Ипак, и у овом зрелом систему јављају се изоловане, али значајне злоупотребе, што указује на то да квалитет режима тајности не зависи само од формалних закона, већ и од институционалне културе и политичке воље. Најчешће се прекомерна класификација јавља у секторима са високим степеном политичке осетљивости, пре свега у Министарству одбране, Министарству за спољне послове и безбедносним службама, где се понекад класификују стратешки документи, дипломатска преписка или интерне анализе које не садрже стварно осетљиве информације (као што су извори, методе, технички детаљи кибер одбране или оперативни планови), већ се више односе на политичке процене, трошкове или административне процесе.

У таквим случајевима, тајност функционише мање као безбедносна мера, а више као инструмент управљања информационим протоком, посебно током периода политичке напетости — избора, владиних криза или јавних скандала. Оваква пракса, мада није системска, и даље ограничава делотворност парламентарног и медијског надзора, чиме се подрива један од темеља парламентарне демократије. Системски посматрано, ово је индикатор да чак и најразвијенији правни оквири остају рањиви на културолошке и политичке факторе који утичу на примену закона.

Кључну улогу у систему игра *Kancelarija za varnost tajnih podatkov* (Канцеларија за заштиту тајних података), која је задужена за координацију, развој методологије процене ризика, вођење централне евиденције класификованих докумената и обуку службеника. На папиру, ова институција има потенцијал да буде активни гарант конзистентности и пропорционалности у примени режима тајности. У пракси, међутим, њена функција често остаје административна и реагујућа, а не проактивна и надзорна. Канцеларија ретко иницира самосталне провере или претходне процене оправданости класификације, нити има снажна санкциона овлашћења према органима који не поштују принципе закона.

Као последица, простор за административну дискрецију остаје отворен, а тајност се повремено третира као формални покривач за избегавање јавне расправе, а не као мера заснована на конкретном, вероватном и документованом ризику. Ово илуструје суштинску аналитичку поуку: формална институционална структура не гарантује делотворност система ако култура примене не интегрише принципе транспарентности, одговорности и професионализма.

Овај напет однос између развијеног оквира и слабе примене добро илуструје случај термалног центра у Рогашкој Слатини (2021). Пројекат вредности 30 милиона евра,

финансиран из државног буџета, био је искључиво економске и административне природе - укључивао је уговоре, трошковне процене, техничку документацију и услове испоруке. Упркос очигледној недостатку безбедносне осетљивости, Министарство финансија је означило целокупну документацију као „Тајно“.

Када је поднет захтев за приступом информацијама, Повереник за слободан приступ информацијама, као независан надзорни орган, утврдио је да није дата ниједна конкретна процена могуће штете, да одлука крши принцип пропорционалности и да је у директној супротности са Законом о заштити тајних података. Повереник је наредио декласификацију небезбедносних делова документације, чиме је повратио равнотежу између државног интереса и права јавности на информисање.

Овај случај је нарочито релевантан јер демонстрира две кључне тачке:

1. Чак и у земљама са развијеним институционалним оквирима, прекомерна класификација остаје могућа - не због недостатка закона, већ због непостојања културе отворености у одређеним сегментима власти.
2. Ефикасност система зависи од делотворности надзорних институција - у овом случају, Повереник је испунио своју уставну улогу, али његова моћ је ретроактивна, што значи да се злоупотреба спречава тек након што се догоди.

Кључно питање које овај случај поставља и које је централно за целу дебату о тајности – гласи: када је тајност оправдана, а када је она само механизам за избегавање одговорности? Одговор не лежи у дужини закона или броју институција, већ у доследној примени три основна принципа:

- да тајност буде изузетак, а не правило;
- да буде заснована на конкретној, вероватној и предвидивој штети, а не на апстрактним „потенцијалним ризицима“;
- да буде временски ограничена, уз обавезу редовне ревизије и аутоматске декласификације.

Словенија, као чланица ЕУ и НАТО-а, има све неопходне правне, техничке и институционалне алате за испуњавање ових услова. Изазов који јој остаје и који је заједнички за велики број демократија - јесте превођење формалног оквира у стварну праксу, где се тајност не користи као инструмент власти, већ као одговорна и временски ограничена мера у служби одржавања безбедности у отвореном друштву.

Извор: Извештај Повереника за слободан приступ информацијама Републике Словеније за 2021, стр. 45–47.

Хрватска: између формалне усклађености и праксе злоупотребе

Хрватска поседује законски оквир за заштиту тајних података који је формално усклађен са стандардима Европске уније и НАТО-а, што је резултат вишегодишњег процеса европских и евроатлантских интеграција - Хрватска је чланица ЕУ од 2013. и НАТО-а од 2009. године. Закон о заштити тајних података предвиђа четири нивоа класификације, обавезу процене стварне и вероватне штете, принцип пропорционалности и обавезу временског ограничења. На папиру, систем испуњава кључне услове које *Tshwane Principles on National Security and the Right to Information* (2013) и ОЕБС-ова

Истанбулска хартија за безбедност (1999) сматрају минималним за демократску примену тајности: да она буде изузетак, а не правило, да буде заснована на конкретној штети и да буде подвргнута независном надзору.

Ипак, у пракси се стално јављају системски изазови у одржавању баланса између легитимне безбедносне заштите и права јавности на информисање. Проблем није у одсуству закона, већ у недовољној институционалној култури одговорности и недовољној ефикасности надзорних механизама. Најчешћи облици злоупотребе упућују на то да се тајност често користи не као безбедносна мера, већ као инструмент управљања информационим протоком у политички осетљивим тренуцима, што указује на дубоку везу између правних прописа и доминантне политичке културе унутар државних институција.

Кључни проблеми у пракси:

- **Масовна класификација уговора у одбрамбеној и енергетској сфери**, често због финансијских, комерцијалних или политичких разлога, а не стварних безбедносних ризика. У таквим случајевима, тајност се користи да би се избегла јавна расправа о трошковима, испорученостима или условима уговора, чиме се омогућава мањак антикорупцијског надзора - управо онај ризик који GRECO и ОЕБС истичу као последицу прекомерне тајности.
- **Ретроактивна класификација** - проглашавање докумената „тајним“ након што су информације већ биле доступне јавности, нпр. кроз поступке јавних набавки, медије или парламентарне расправе. Таква пракса супротставља се основи правне сигурности и европској пракси, где је класификација претходна мера, а не реакција на јавни притисак.
- **Нејасно разграничавање између „интерно“, „поверљиво“ и „тајно“**, што доводи до превентивног коришћења највиших степена тајности као „сигурније“ административне опције - феномен познат у теорији као „инфлација тајности“. Ово је у директној супротности са принципом најмање неопходне заштите, који је кључан у ЕУ и НАТО системима.
- **Ограничена ефикасност надзора**: Повереник за слободан приступ информацијама често утврђује злоупотребе у својим одлукама, али нема довољна овлашћења за спровођење решења у праксу - његова улога остаје ретроактивна и препоручљива, што слаби делотворност целог система.

Кључни институционални актер у овом систему је *Уред Вијећа за националну сигурност (UVNS)*, који теоријски има двојаку надлежност: координацију политике националне безбедности и стручни надзор режима тајности. Таква двострука улога би требало да осигура равнотежу између безбедносне ефикасности и демократске одговорности. У пракси, међутим, UVNS делује пре свега као административна тачка координације, а не као независан надзорни орган. Институција ретко иницира самосталне провере, преиспитује спорне одлуке или издаје мишљења која би могла да ограниче произвољност. Његова недовољна видљивост и ниска активност омогућавају да се тајност и даље третира као инструмент управљања информационим током, а не као заштита легитимних државних интереса.

Ове тенденције драматично илуструје случај **ретроактивне класификације уговора о модернизацији борбених возила БВМ (2022)**. Након што су детаљи уговора - укључујући трошкове, спецификације и услове испоруке - постали јавно доступни као

део конкурсне документације у јавној набавци и након објаве на порталу Index.hr, Министарство одбране је ретроактивно прогласило цео уговор „тајним“. У одлуци није достављено конкретно образложење како би те информације могле угрозити интересе одбране - што представља очигледно кршење члана 8. Закона о заштити тајних података, који захтева процену стварне штете. Хелсиншки комитет за људска права оценио је овај случај као озбиљно кршење правне сигурности и непоштовање европских стандарда, истичући да „ретроактивна тајност није безбедносна мера, већ покушај цензуре под изговором државне безбедности“.

Овај пример показује да, иако Хрватска има формално савршен систем, његова функционална легитимност зависи од доследности примене и политичке воље за транспарентност. У ери хибридних претњи и дезинформација, где је поверење у институције кључно, прекомерна класификација не штити државу - она је угрожава, јер поткопава један од темеља демократског поретка: право грађана да знају како се троше њихови порези и како се доносе стратешке одлуке.

Кључни изазов за Хрватску, као и за друге чланице ЕУ, није у стварању нових закона, већ у успостављању институционалне културе у којој је тајност последње средство, а не први рефлекс - културе у којој се свака одлука о класификацији документује, образложи и подвргне независном преиспитивању, не зато што је то формална обавеза, већ зато што је то услов за легитимност власти у отвореном друштву.

Извор: *Index.hr*, „Ugovor o modernizaciji oklopnih vozila proglašen tajnim nakon objave“, 18. мај 2022; Извештај Хелсиншког комитета за људска права, 2022.

Босна и Херцеговина: фрагментација система и злоупотреба тајности

Режим тајности у Босни и Херцеговини функционише унутар једног од најсложенијих институционалних окружења у Европи - са три нивоа власти: државним, ентитетским (Федерација БиХ и Република Српска) и Брчко Дистриктом. Ова конституционална фрагментација не само да отежава усаглашавање закона, већ и системски омогућава произвољну и политички мотивисану примену режима тајности. Иако постоје одвојени закони о тајности података на свим нивоима власти, они се често разликују у дефиницијама, поступцима и степену надзора, што води до правне неизвесности, конфликтних одлука и двоструких стандарда - чак и унутар истог сектора, као што су одбрана, дипломатија или управљање европским фондовима. Ова фрагментација ствара институционалну празнину у којој се закон примењује селективно, што отвара простор за злоупотребу тајности као алата политичке контроле, уместо заштите стварних безбедносних интереса.

Као последица, тајност у БиХ често постаје инструмент политичке контроле, а не механизам заштите стварних безбедносних интереса. Ово је посебно изражено у областима где се интерсикују финансијски, политички и геостратегијски интереси: одбрамбени пројекти, двострани споразуми са страним државама, велике инфраструктурне инвестиције и пројекти финансирани из средстава Европске уније. У тим контекстима, информације се класификују не због „стварне и вероватне штете“ по државни интерес, већ да би се спречило медијско праћење, избегла јавна расправа или прикриле неправилности у трошењу јавних средстава. Практично, ово значи да се европски стандарди транспарентности поштују у фази финансирања, али се системски

игноришу у домаћој имплементацији - што ствара паралексни однос између формалне обавезе и стварне праксе.

Један од најозбиљнијих облика злоупотребе је **системско скривање извештаја о корупцији**, често ретроактивно, тек након што информације доспеју у јавност. Уместо да се тајност користи проактивно - као заштита осетљивих метода или извора - она се реактивно уводи као средство цензуре, чиме се онемогућава независан надзор и подрива сама идеја одговорности власти. Оваква пракса је у директној супротности не само са чланом 8. закона о тајности (који захтева процену конкретне штете), већ и са *Тромсе конвенцијом* Савета Европе, ОЕБС-овим принципима и ЕУ условима за приступ фондским средствима, који инсистирају на транспарентности у управљању јавним средствима.

На државном нивоу, **Сектор за тајне податке у Министарству сигурности БиХ** формално развија стандарде, води централну евиденцију и врши стручни надзор над применом закона. Међутим, због дубоке политичке фрагментације, одсуства политичке воље за надзор над ентитетима и слабог ангажмана у спорним случајевима, његова улога у пракси се своди на административну координацију, а не на функционалан надзор. Институција ретко преиспитује одлуке ентитетских органа, не издаје мишљења о неусаглашеним праксама и нема овлашћења да санкционише злоупотребе — што омогућава да се злоупотреба тајности нормализује као део свакодневног политичког инжењеринга.

Овај проблем је драматично илустрован случајем **Термоелектране „Бања Лука“ (2020)**. Унутрашњи извештај Агенције за предузетништво и Инвестиционог фонда Републике Српске открио је озбиљне неправилности у пројекту вредном 29 милиона евра, који је био финансиран из средстава Европске уније. Након што су детаљи извештаја стигли у јавност преко медија, целокупна документација је ретроактивно проглашена „тајном“ - без конкретног образложења о томе како би објава могла да угрози националну безбедност, одбрану или дипломатске односе. Центар за истраживачко новинарство (CIN) и Transparency International BiH истакли су да је класификација искоришћена не ради заштите безбедности, већ ради прикривања могућих злоупотреба и избегавања одговорности. Овај случај, парадоксалан у свом окрету, показује како европски стандарди транспарентности могу бити формално прихваћени, али стварно поткопани унутар фрагментисаног система који нема центрифугалну силу ка отворености.

Кључна дилема коју овај случај поставља - и која је централна за читав регионални контекст - гласи: **тајност треба да штити државу, а не актере од отвореног рачуна**. У БиХ, где политичка лојалност често превазилази институционалну одговорност, ова разлика постаје све мутнија. У том смислу, проблем није у одсуству закона, већ у одсуству заједничког простора за јавни интерес - простора у којем би тајност била изузетак, а не политичка стратегија.

Без решавања ових структурних питања - укључујући усклађивање законских оквира, јачање независног надзора и стварање јединствене методологије процене ризика - режим тајности у БиХ ће и даље служити **фрагментацији власти, а не заштити заједничких безбедносних интереса**. У ери када транспарентност постаје услов не само за европске интеграције, већ и за опстанак демократије, тајност као политичка тактика постаје не само неефикасна - већ и деструктивна.

Извор: CIN BiH, „Izvještaj o korupciji u TE Banja Luka klasifikovan kao tajni“, 12. октобар 2020.

Црна Гора: Формална усклађеност и неуједначена пракса

Као чланица НАТО-а од 2017. године и кандидат за чланство у Европској унији, Црна Гора је формално усагласила свој законски оквир за заштиту класификованих података са међународним стандардима. Закон о заштити тајних података предвиђа четири нивоа класификације, обавезу процене стварне и вероватне штете, принцип пропорционалности, као и временско ограничење тајности - елементи који су у складу са *Tshwane Principles on National Security and the Right to Information* (2013), НАТО-овом *Security Policy* (AAP-06) и ЕУ *Security Rules* (C(2019) 6110). У теорији, овај оквир обезбеђује оно што ОЕБС дефинише као „баланс између легитимне безбедности и демократске одговорности“.

Ипак, у пракси постоји значајан раскорак између формалне усклађености и стварне примене. Одлуке о класификацији често одступају од основних правних и етичких принципа: нужности, пропорционалности и временског ограничења. Уместо да се тајност примењује као прецизна и ограничена мера, она се често користи као административни рефлекс или политички инструмент, што поткопава и ефикасност система заштите и легитимност власти.

Најизраженији проблеми у пракси:

- **Прекомерно означавање тајности**, посебно у одбрамбеним набавкама, међународним војним уговорима и аналитичким извештајима безбедносних служби. Уместо да се примени техника црвених линија (*redaction*) - која омогућава заштиту само стварно осетљивих делова (као што су методе, извори, технички детаљи сигурносних система) - често се целокупни документи класификују, иако већина њиховог садржаја (трошкови, рокови, општи услови) нема везе са националном безбедношћу. Ово је у директној супротности са НАТО-овим принципом „најмање неопходне заштите“ и европском праксом, где је селективна класификација обавезна.
- **Политичка инструментализација**: статистички и квалитативно, број одлука о класификацији расте у периодима политичке нестабилности - избора, владиних криза или јавних скандала. Ово указује на то да се тајност не користи искључиво због безбедности, већ као средство управљања јавним информационим протоком, чиме се ограничава могућност парламентарног и медијског надзора - управо онај ризик који ОЕБС-ова *Истанбулска хартија за безбедност* (1999) изричито забрањује.
- **Неадекватан надзор**: формално делегиран двема кључним телима - Поверенику за слободан приступ информацијама и Дирекцији за тајне податке у Министарству одбране. Међутим, оба актера располажу ограниченим овлашћењима и делују пре свега као административни, а не надзорни органи. Повереник може да утврди злоупотребу и да изда препоруку за декласификацију, али нема везану правну моћ да принуди органе на поступање. Дирекција углавном води централизовану евиденцију и обезбеђује обуку, али редовно избегава преиспитивање спорних одлука или издавање мишљења са санкционим ефектом. Као резултат, контрола остаје формална, а злоупотребе се ретко коригују, што ствара перманентни простор за произвољ.

Овај проблем је јасно илустрован случајем **уговора са немачком компанијом KMW (2019)** за набавку војних возила. Уговор је одмах проглашен „Врло тајно“, уз опште образложење „заштите међународне сарадње“. Међутим, основни детаљи - типови возила, намена, општи оквир сарадње - већ су били јавно доступни кроз саопштења Министарства одбране и сајт партнера. Оно што је задржано као тајно - финансијски подаци: цена, рокови испоруке, гаранције и услови плаћања - управо су они који су од кључног значаја за антикорупцијски и фискални надзор. Повереник за слободан приступ информацијама је захтевао делимичну декласификацију небезбедносних делова, али је захтев одбијен без конкретне процене ризика, што представља очигледно кршење члана 8. Закона.

Овај случај наглашава кључну истину која се појављује широм региона: **формална усаглашеност са међународним стандардима није довољна без политичке воље за доследну и одговорну праксу**. У Црној Гори, као и у другим земљама Западног Балкана, тајност често постаје алтернатива транспарентности, а не њен комплемент. У ери када ЕУ инсистира на „транспарентности као услову за финансирање“ и када НАТО захтева „оперативну компатибилност кроз отвореност“, таква пракса не само да угрожава демократску одговорност, већ и отежава интеграцију и међународну сарадњу.

Кључни изазов за Црну Гору није у доношењу нових закона, већ у развоју **институционалне културе** у којој се тајност користи само када је заиста неопходна — а не као средство избегавања јавног надзора. Легитимност власти у демократском друштву не мери се колико се крије, већ колико се прецизно, привремено и оправдано образложи свака одлука о класификацији.

Извор: Radio Televizija Crne Gore (RTCG), „Ugovor sa KMW proglašen 'vrlo tajno'“, 20. новембар 2019.

Северна Македонија: Међународна транспарентност, домаћа тајновитост

Северна Македонија, као чланица НАТО-а од 2020. године и званични кандидат за чланство у Европској унији, формално испуњава евроатлантске стандарде заштите тајних података. Закон о заштити тајних података предвиђа јасне критеријуме за класификацију, укључујући стварну и вероватну штету по легитиман државни интерес, принцип пропорционалности и обавезу временског ограничења. На папиру, систем је у складу са *Tshwane Principles*, НАТО-овом *Security Policy* (AAP-06) и ЕУ оквиром за управљање класификованим информацијама, а самим тим и са основним демократским стандардима које ОЕБС и Савет Европе сматрају минималним за отворено друштво.

Ипак, у пракси постоји јасан и системски размак између формалног оквира и стварне примене. Овај раскорак омогућава селективну примену правила, административну дискрецију без надзора и политички мотивисану класификацију, што поткопава и ефикасност система заштите и легитимност институција у очима грађана.

Најчешћи проблеми у пракси:

- **Класификација енергетских уговора** (нпр. гасоводи, електране) под општим изговором „националног интереса“, иако су пројекти финансирани од стране међународних финансијских институција - попут Европске банке за обнову и развој (EBRD), које експлицитно захтевају транспарентност као услов

финансирања. У тим случајевима, тајност се не користи за заштиту безбедности, већ за спречавање јавне расправе о трошковима, исплатама или уговорним одредбама, што је у директној супротности са Тромсе конвенцијом Савета Европе, која налаже да „транспарентност је правило, а тајност изузетак“.

- **Ограничен приступ стратешким плановима полиције и војске** током реформи, што онемогућава парламентарни и јавни надзор над процесима кључним за демократизацију и европске интеграције. Иако су такви документи често општи по садржају (мисије, приоритети, организациона шема), они се системски означавају као „тајни“, чиме се демократски надзор своди на формалност.
- **Нејасна употреба ознаке „интерно“** као замена за „тајно“, без обавезне процене ризика или образложења. Ова пракса, позната у теорији као „превентивна класификација“, води томе да се осетљивост података претпоставља, а не процењује, што је у супротности са НАТО-овим захтевом да свака класификација мора бити „јасно образложена“.
- **Ограничена ефикасност Повереника за слободан приступ информацијама**, који иако редовно утврђује злоупотребе и доноси одлуке у складу са законом, нема извршна овлашћења да принуди органе на поступање. Његова улога остаје ретроактивна и препоручљива, што слаби делотворност целог система заштите права на информације.

Централну улогу у систему има **Дирекција за класификоване информације**, која је формално задужена за координацију режима тајности, вођење централне евиденције, обавезну обуку службеника и спровођење провера. Међутим, у пракси Дирекција делује више као административни регистар него као активни надзорни орган. Ретко иницира независне провере, не објављује годишње извештаје о стању класификације, нити јавно образлаже контроверзне одлуке, што оставља простор за непрозирне и неодговорне праксе. Да би систем био легитиман, Дирекција мора преузети јачу иницијативу: проактивно преиспитивати одлуке о класификацији, објављивати агрегиране податке о броју и разлозима класификације и јавно мотивисати одступања од стандарда.

Овај системски недостатак је драматично илустрован **случајем уговора о гасоводу „Беласица“ (2020)**. Пројекат, финансиран од стране EBRD, проглашен је „Тајним“ због „угрожавања националног интереса“. Међутим, документ није садржао војне, обавештајне или оперативне безбедносне елементе, уместо тога, радило се о комерцијалном уговору о изградњи инфраструктуре, чији су кључни финансијски и технички подаци већ били јавни у извештајима EBRD. Повереник је утврдио да је класификација несразмерна, недокументована и у супротности са законом, те је наложио декласификацију небезбедносних делова.

Овај пример показује кључну напетост у савременој држави у транзицији: када се транспарентност према међународним партнерима (као услов за финансирање) сусреће са тајновитошћу према властитим грађанима, граница између легитимне заштите и политичког скривања постаје мутна. Формална усаглашеност са европским стандардима није довољна, она мора бити праћена доследном применом, институционалном одговорношћу и културом отворености.

Конзистентна и прецизна примена режима тајности није питање техничке исправности, већ темељ поверења у демократске институције. У Северној Македонији, као и у

читавом региону, тајност која се користи као оправдање за затварање система подрива сам циљ европских интеграција: изградњу отворене, одговорне и легитимне државе.

Извор: Изјава Повереника за слободан приступ информацијама Северне Македоније, 15. април 2021.

Текстуално појашњење табеле — ниво присутности проблема по државама

Проблем / Држава	Словенија	Хрватска	Босна и Херцеговина	Црна Гора	Северна Македонија	Србија
Прекомерно означавање	✓	✓✓	✓✓✓	✓✓	✓✓	✓✓✓
Политичка инструментализација	✓	✓✓	✓✓✓	✓✓	✓✓	✓✓✓
Недостатак процене ризика	✓	✓✓	✓✓✓	✓✓	✓✓	✓✓✓
Ретроактивна класификација	△	✓✓	✓✓	✓	✓	✓✓
Слаб надзор Повереника	△	✓	✓✓✓	✓✓	✓✓	✓✓
Масовно означавање уговора	△	✓✓	✓✓	✓✓	✓✓	✓✓✓

Напомене:

- ✓ = присутно
- ✓✓ = умерено распрострањено
- ✓✓✓ = системски, дубоко укорењен проблем
- △ = повремено

Контекстуална анализа - Разлике у присутности проблема у региону најбоље се разумеју кроз институционалну зрелост, координацију надзорних тела и стабилност правне праксе, а не као показатељ „бољих“ или „лошијих“ политичких система.

- **Словенија** има најразвијенији надзорни оквир: Канцеларија за варност тајних података и Повереник за приступ информацијама делују ефикасно, па су проблеми ретки и углавном изоловани (✓ или △).
- **Хрватска** испуњава формалне стандарде, али у пракси постоји извесна резервисаност у реаговању на спорне класификације, нарочито у одбрани (✓✓).
- **Босна и Херцеговина** се суочава са структурним изазовима услед сложеног уређења; ризик од политички мотивисане класификације остаје висок, посебно код пројеката са страним финансирањем (✓✓✓).
- **Црна Гора** има формално усклађен систем, али надзор је углавном административан; током политички осетљивих периода јављају се примери шире класификације, без нарушавања институционалног оквира (✓✓).
- **Северна Македонија** је ојачала институционални систем, али пракса је још у развоју; поједини примери „тајности“ енергетских уговора показују потребу за прецизнијом проценом ризика (✓✓).
- **Србија** има развијен нормативни оквир, али се у пракси јављају изазови у координацији и примену стандарда; у одбрамбеним набавкама и стратешким

документима доминира превентивна или ретроактивна класификација, чак и када садржај није заиста осетљив (✓✓✓).

Ова анализа није осуда, већ професионална процена усклађености закона и праксе, са циљем подстицања размене добрих пракси и унапређења система, у оквиру којег тајност остаје легитиман, али изузетан и добро образложен инструмент, у складу са принципом: *„јавно као правило, тајно као изузетак“*.

Политичка, правна и морална одговорност - регионални поглед

У свих шест земаља региона - Словенији, Хрватској, Босни и Херцеговини, Црној Гори, Србији и Северној Македонији постоји ризик да се режим тајности користи не само ради заштите легитимних националних интереса, већ и као инструмент избегавања политичке, правне или институционалне одговорности. Иако су законски оквири у великој мери усклађени са евроатлантским стандардима, у пракси се често нарушава равнотежа између права јавности да зна и обавезе државе да штити стварно осетљиве информације. Та равнотежа, утврђена троструким тестом из члана 8. Закона о тајности података Републике Србије (постојање легитимног интереса, стварна и вероватна штета, претежност државног над јавним интересом), није апстрактан теоријски оквир, већ практични механизам намењен спречавању да тајност постане замена за транспарентност. Када тај механизам није функционалан, злоупотреба настаје не због недостатка закона, већ због слабости политичке воље, професионалне културе и институционалног надзора. Ове злоупотребе најбоље се разумеју кроз три међусобно повезане димензије.

Политичка димензија: национални интерес као политички штит - Када се ознака „национални интерес“ употребљава као општи, недефинисан алиби за скривање спорних или проблематичних одлука, без конкретне, документоване и вероватне штете, тајност престаје да буде инструмент безбедности и постаје средство политичке економије моћи. У секторима где су стратешки, финансијски и дипломатски интереси најконцентричнији, попут одбрамбених набавки, спољнополитичких договора или кадровских решења, тајност често није реакција на реалну претњу, већ механизам управљања информацијама.

Пример из Србије то јасно показује: означавање финансијских детаља уговора о набавци војне опреме као „строго поверљиво“ онемогућава парламентарни надзор и јавну расправу о трошковима, моделима финансирања и техничким карактеристикама. Ти подаци, сами по себи, не садрже оперативне планове, не откривају изворе, нити омогућавају супротстављање Војске Србије. Они не угрожавају оперативне способности нити представљају стратешку тајну. Уместо тога, тајност постаје заштитни зид између извршне власти и демократске контроле - у супротности са основним принципом да надзор није препрека безбедности, већ њен предуслов.

Правна димензија: формална процедура као замена за правну одговорност - Закони у региону јасно прописују да свака одлука о одређивању тајности или класификацији мора бити заснована на стварној, конкретној и вероватној штети; да мора бити образложена, заснована на процени ризика и временски ограничена. То значи да се

тајност не може увести „на општу опасност“ или „у име државе“. Међутим, у пракси ове процедуре често остају формалне, посебно када одлуке доносе високи државни функционери који су ретко изложени ефикасном независном надзору.

Један од најпроблематичнијих облика правне неодговорности јесте ретроактивна класификација, честа у Хрватској, Црној Гори и Србији када се документи проглашавају тајним тек након што су постали предмет медијске пажње или јавне расправе. Такав поступак није превентивна мера заштите; он је реактивна интервенција. Он не спречава штету, он управља последицама јавног интересовања. У том тренутку, Закон о тајности података више није инструмент безбедности, већ техничко средство за избегавање негативних политичких ефеката. То подрива кредибилитет правног поретка и сигурност система тајних података.

Морална димензија: замена индивидуалне одговорности колективним алибима - Када се индивидуална одговорност за одлучивање о тајности разводњава кроз формуле попут „нисам био обавештен“, „нисам имао избор“ или „то је државни интерес“, тајност се од професионалне категорије претвара у морално компромитован инструмент. То је у директној супротности са два основна принципа:

1. **Тајност је изузетак, а не правило.**
2. **Тајност не сме прикривати злоупотребе, кривична дела или повреде људских права**, што је недвосмислено прописано чланом 3. Закона о тајности података.

Илустративан је пример из Босне и Херцеговине: извештај о корупцији у термоелектрани „Бања Лука“, финансираној средствима Европске уније, проглашен је тајним неколико месеци након што су медији већ објавили његов садржај. То није заштита државе, то је институционални акт самозаштите. Оваква реакција не само да крши закон, већ директно онемогућава антикорупцијски, парламентарни или регулаторни надзор. У том тренутку тајност не служи држави, већ појединачним актерима унутар система.

Регионалне разлике: не у природи проблема, већ у капацитету отпора - Злоупотребе режима тајности нису специфичност једне земље, већ системски израз политичке, институционалне и професионалне културе. Због тога се земље региона не разликују по самој природи проблема, већ по интензитету злоупотреба и степену институционалне отпорности.

Словенија, иако није имуна на ове појаве, има развијеније механизме контроле: ефикасну институцију Повереника, функционалну Канцеларију за варност тајних податков и утемељену културу преиспитивања извршне власти. Због тога су одлуке о класификацији обавезно образложене, временски ограничене и подложне редовном надзору.

У осталим земљама региона, посебно у областима одбране, безбедности и енергетике, тајност често функционише као средство искључивања јавности из процеса одлучивања. Тај тренд дугорочно угрожава демократију, слабећи парламентарни и медијски надзор, али и саму безбедност: кредибилитет ознаке тајности се урушава када се примењује на

податке који немају стварни, конкретан и вероватан безбедносни ризик. Када „све постане тајно“, губи се поверење у оно што је заиста потребно штитити.

Регионалне препоруке: од формалног ка функционалном усаглашавању - Реформа режима тајности не може се свести на доношење нових подзаконских аката или техничке измене административних упутстава. Она мора бити институционална, политичка и културна, јер проблем није у формалној структури одлука, већ у намери, пракси и контексту њиховог доношења. Кључне мере обухватају:

- **обавезну и документовану процену ризика** пре сваког одређивања тајности или класификације, уз доследну примену четворостепеног теста јавног интереса (стварна штета, тежина штете, претежност државног над јавним интересом, неопходност ограничења);
- **јачање инспекцијских, надзорних и стручних тела** (Канцеларије Савета за националну безбедност и заштиту тајн их података, Дирекције за тајне податке, Уреда Вијећа за националну сигурност), уз проширена овлашћења за преиспитивање одлука, санкционисање злоупотреба и превентивно деловање;
- **аутоматски престанак тајности и обавезну декласификацију по истеку рока**, уз захтев за новом, образложеном проценом уколико се тајност продужава — како би се избегло стање „застарелих тајни“ које изгубе сваку безбедносну сврху, али настављају да ограничавају приступ;
- **системску и ситуационо оријентисану обуку службеника**, са посебним нагласком на схватање тајности као привременог и изузетног инструмента, а не као подразумеваног статуса или заштитног механизма;
- **јасно разграничење између административних података „за службену или ограничену употребу“ од тајних података са ознакама тајности „интерно/поверљиво/строго поверљиво/државна тајна“**, како би се спречила злоупотреба паралелних, нерегулисаних режима ограничења приступа и избегло скривање информација у административним категоријама које формално нису део система тајности;
- **годишње јавне извештаје** о броју, трајању, тематици и основима одређивања тајности или класификације без откривања садржаја, али са јасним приказом логике одлучивања и трендова у пракси;
- **јачање парламентарног надзора у безбедносном и одбрамбеном сектору**, уз обезбеђивање адекватних безбедносних сертификата за чланове надлежних одбора, како би надзор био ефикасан, а не искључиво формалан.

Тајност је легитимна све док служи држави тако што штити стварне интересе од стварних, конкретних и вероватних претњи. Међутим, она губи своју правну, политичку и моралну основу оног тренутка када се користи да би се избегла питања, прикрили трошкови или ограничила демократска контрола. Због тога ревизија праксе одређивања тајности не представља анти-безбедносну меру – напротив, она је предуслов за одрживу, кредибилну и демократски засновану безбедност.

Систем у коме се тајност не процењује по броју скривених докумената, већ по прецизности, оправданости и привремености сваке појединачне одлуке, јесте систем у ком тајност не функционише као алтернатива транспарентности, већ као њена комплементарна мера у служби јавног интереса.

Закључна разматрања

Режим тајности у Републици Србији, као и шире у земљама Балкана, има јасно дефинисану сврху: заштитити информације чије би откривање могло нанети стварну, конкретну и вероватну штету интересима националне безбедности, одбране, спољне политике или стабилности државних институција. Како истиче теорија, та штета мора бити представљена у јасним и конкретним параметрима, а не у апстрактним или хипотетичким претпоставкама. Закони о тајности података у региону у великој мери прате евроатлантске стандарде и формално обезбеђују неопходне институционалне механизме. Ипак, значајни изазови јављају се управо у примени троструког теста из члана 8. Закона о тајности података: *интерес – стварна штета – претежност над јавним интересом*. Уместо да буде изузетак, како је законски предвиђено, тајност се често претвара у рутинску праксу, укључујући и документе који садрже искључиво економске, административне или техничке податке, а чије би објављивање имало занемарљив или никакав безбедносни утицај.

Овакав приступ производи двоструку системску штету. С једне стране, нарушава се ефикасност стварне заштите, јер ознака "тајности" губи на тежини када се примењује масовно и без јасног критеријума; у таквом амбијенту заиста осетљиви подаци, као што су извори обавештајних служби, планови одбране или подаци о кибернетским претњама - губе неопходан степен посебне заштите. С друге стране, прекомерна тајност ограничава демократску контролу управо у областима где она мора бити несметана: у надзору трошења јавних средстава, у енергетским аранжманима, у одбрамбеним набавкама или у вођењу стратешких инфраструктурних пројеката.

Разлике међу државама региона нису у типологији проблема, већ у нивоу институционалне отпорности према произвољној примени. У Словенији и Хрватској надзорна тела, попут Повереника за слободан приступ информацијама од јавног значаја, Уреда Вијећа за националну сигурност или Канцеларије за тајне податке - имају превентивну и корективну функцију и успевају да ублаже последице појединачних злоупотреба. У другим државама, као што су Србија, Црна Гора, БиХ или Северна Македонија, надзорни механизми су фрагментирани, формални или недовољно ефикасни, што омогућава распрострањене праксе ретроактивног одређивања тајности, прекомерног означавања уговора, прикривања финансијских услова или изостављања процене ризика као обавезног корака.

Посебно је карактеристично за државе настале распадом бивше Југославије да проблем није у нормативном оквиру. који је у великој мери усаглашен са европским стандардима, већ у доследности примене. Уместо да буде мерена, пропорционална и добро образложена мера, тајност постаје аутоматизована, продужавана и често ретроактивна, па чак и у случајевима у којима су подаци већ јавни преко међународних партнера или медија. Такав приступ крши не само члан 8, већ и експлицитну забрану из члана 3. Закона, који искључује могућност одређивања тајности за податке који се односе на злоупотребе, неправилности или кршење закона и људских права.

Ипак, ова анализа није усмерена на критику институција, већ на потребу њиховог функционалног унапређења, у складу са *Tshwane Principles*, праксом НАТО-а и стандардима ЕУ. Циљ није укидање тајности, већ њено враћање изворној сврси, да буде изузетак заснован на стварној, документованој процени ризика, а не административни ритуал или инструмент политичке контроле. То се може постићи кроз следеће кораке:

- свака одлука о одређивању тајности или класификацији мора бити праћена документованом проценом ризика у складу са чланом 8. ст. 1 ЗТП;
- образложење одлуке мора бити доступно јавности у неповерљивом облику, како би се омогућио ефикасан надзор;
- аутоматски престанак тајности и декласификација по истеку рока морају постати правило, а не изузетак који се игнорише;
- Министарство правде и Канцеларија Савета за националну безбедност и заштиту тајних података морају добити одговарајућа законска овлашћења и техничке ресурсе за вршење стварног надзора, укључујући санкционисање.

На крају, нужно је истакнути следеће: **Оправдани интерес јавности да зна није апсолутна и неограничена категорија. Тајност је оправдана онда када штити државу од стварних, конкретних и вероватних претњи. Али тајност губи сваку правну, политичку и моралну легитимност када служи за прикривање трошења јавних средстава, неправилности или ограничења демократског надзора.**

У том смислу, ревизија праксе одређивања тајности није анти-безбедносна мера, већ предуслов за одржив и легитиман систем националне безбедности у модерној демократији. У таквој држави, тајност не сме бити правило, а истина не сме бити изузетак. Промена, да би била успешна, мора бити институционална, политичка и културна - и мора започети од спознаје да право јавности да зна није претња држави, већ основ њене снаге.

Налази и препоруке

Кључни налази и препоруке из материјала о прекомерној класификацији поверљивих информација могу се формулисати на следећи начин:

Кључни налази

1. **Прекомерно одређивање тајности или класификација информација представља системски изазов** који доводи до слабљења транспарентности, смањења јавног поверења и нарушавања легитимности безбедносних и државних институција. Уместо да штити безбедност, она често производи супротне ефекте.
2. **Постојећа пракса одређивања тајности нли класификације често је преопширна, неуједначена и нормативно неадекватно примењена**, што резултира непотребном бирократизацијом процеса, успорава административне процедуре и отежава оперативно деловање.
3. **Међународни стандарди и препоруке (GRECO, Tshwane Principles, ENISA)** јасно налажу потребу за прецизним критеријумима, пропорционалношћу и минималним обимом одређивања тајности или класификације. У поређењу с њима, регионалне праксе показују значајне одступања, нарочито у контексту јавних набавки и међународних уговора.
4. **Ефикасан систем одређивања тајности или класификације мора одржавати равнотежу између националне безбедности и права јавности да зна**, где је тајност изузетак, а транспарентност подразумевано правило.

5. **Редован преглед, ревизија и временска ограниченост класификације** представљају кључни услов за спречавање прекомерне и ретроактивне тајности. Ови механизми су у великој мери минимално коришћени или недовољно институционализовани.
6. **Проблем није у закону, већ у институционалној култури и политичкој вољи.** Иако нормативни оквир у већини држава региона формално испуњава европске и НАТО стандарде, примена зависи од институционалне зрелости, професионалних навика и спремности политичких актера да ограниче сопствену дискрецију. Управо је то тачка највећег одступања у пракси.
7. **Прекомерно одређивање тајности или класификација често се користи као алат за избегавање одговорности**, нарочито у јавним набавкама, међународним уговорима и стратешким инфраструктурним пројектима. У тим случајевима тајност не служи заштити безбедносних интереса, већ одлагању јавне контроле и управљању политичком перцепцијом, што представља облик злоупотребе и супротставља се основним принципима *апсолутне забране одређивања тајности* или класификације (забрана одређивања тајности или класификације података о прикривања кривичних дела, злоупотребе службеног положаја или других незаконитих радњи) из члана 3. и *троструког теста јавног интереса* (интерес – стварна штета – претежност над правом јавности да зна) из члана 8. Закона о тајности података.
8. **Статус кво у примени режима тајности носи мерљив стратешки, политички и институционални ризик.** Непоступање у унапређењу система тајности — чак и уз постојећи законски оквир — не представља „безбедан избор“, већ активно излагање државе вишеструким и узајамно повезаним ризицима.
    - **У ЕУ преговарачким поглављима (23 и 30)**, одсуство функционалног, транспарентног и надзорно одговорног режима тајности може довести до блокаде или успоравања процеса интеграција, нарочито у областима везаним за владавину права, правосуђе, безбедносни сектор и спољну политику. ЕУ не посматра тајност као техничко питање, већ као део шире инфраструктуре интегритета институција, а непредвидивост у одређивању тајности или класификацији података сигнализира слабост система контроле.
    - **У домену борбе против корупције**, прекомерна тајност у јавним набавкама, одбрамбеним уговорима и инфраструктурним пројектима емпиријски повећава простор за неправилности, што доследно потврђују извештаји GRECO-а и европских антикорупцијских тела. Када се кључни елементи уговора, техничких спецификација или одлука о финансирању проглашавају тајним без јасне процене ризика, надзорни механизми постају нефункционални, а одговорност се замењује административним формализмом.
    - **У дипломатским и безбедносним односима са ЕУ, НАТО-ом и партнерима**, неусаглашеност режима одређивања тајнсоти или класификације са међународним стандардима отежава размену поверљивих информација, заједничке вежбе, оперативну планирање и техничку сарадњу. Поверење се у овим односима не гради на формалним декларацијама, већ на предвидивости, конзистентности и институционалној зрелости система руковања тајним подацима.
    - **Унутар државе**, одлагање реформи продубљује деградацију институционалне културе. Тајност се све више третира као инструмент управљања и контроле, а не као мера заштите, што подрива кредибилитет

система националне безбедности. Истовремено, демотивише професионалне службенике и подстиче праксе које фаворизују краткорочну политичку удобност науштрб правних стандарда и дугорочне институционалне стабилности.

- **Трошкови прекомерне тајности су реални, кумулативни и често невидљиви док не произведу системску штету.** Они обухватају материјалне трошкове (инфраструктура безбедности, посебни системи обраде, архивирање, логистика), али и нематеријалне: губитак поверења, слабљење парламентарног и јавног надзора, раст корупцијских ризика и смањење квалитета јавних политика. Студије RAND-а и CSIS-а показују да системи са високим степеном прекомерне одређивања тајности или класификације имају нижи ниво оперативне ефикасности, слабије механизме одговорности и виши ниво корупцијских инцидената, што их чини структурно мање отпорним на кризе и хибридне претње.

Препоруке у складу са стварним стањем заштите тајних података у Републици Србији

1. Ојачати примену постојећих критеријума за одређивање тајности, уместо доношења нових. Закон о тајности података, Уредбе о критеријумима за одређивање степена тајности и Одлуке о детаљним условима за процену штете већ садрже јасне, уједначене и методолошки засноване стандарде. Проблем није у нормативном оквиру, већ у неконзистентној примени. Неопходно је да свака одлука о одређивању степена тајности буде документована, заснована на процени стварног и вероватног ризика и у складу са важећим актима, а не на апстрактно дефинисаним „националним интересима“.
2. Увести обавезну, стандардизовану и периодичну обуку за све јавне службенике који доносе одлуке о тајности, са акцентом на разликовање стварне безбедносне штете од политичке или административне непријатности. Обука мора бити практична, а не формална, и треба да укључи симулације процена ризика, анализу типичних грешака и последица произвољности. Циљ је да се административна обавеза трансформише у професионалну одговорност.
3. Оснажити надзорне механизме у оквиру система тајности - пре свега Канцеларију Савета за националну безбедност и заштиту тајних података (стручни надзор) и Министарство правде (инспекцијски надзор). Ово подразумева:

    - да Канцеларија Савета проактивно преиспитује одлуке о одређивању степена тајности, уместо да се своди на вођење статистичких евиденција;
    - да Министарство правде спроводи редовне и целовите инспекцијске провере, а не само да реагује на пријаве;
    - да оба тела јавно извештавају о стању праксе (без откривања садржаја тајних података), укључујући број неправилно осређених тајних података и препоруке за исправке.

4. Хармонизовати домаћу праксу са међународним стандардима који су већ уграђени у закон – начелом пропорционалности, принципом најмање неопходне заштите и временске ограничености. Посебно је важно увести праксу аутоматске ревизије (ако не и аутоматског престанка тајности или декласификације) по

истеку предвиђеног рока, у складу са стандардима ЕУ и НАТО. Ово не захтева измену закона, већ доследну примену постојећих одредби о редовној ревизији.

5. Повећати унутрашњу одговорност у органима јавне власти јачањем улоге унутрашње контроле и старешине органа, који су по закону одговорни за исправност поступања са тајним подацима. Неопходно је раздвојити функцију одређивања тајности, функцију руковања тајним подацима и функцију унутрашњег надзора, као и обезбедити да свака одлука буде предмет унутрашњег преиспитивања пре њеног ступања на снагу - чиме се спречавају ретроактивне и реактивне класификације.

Напомена: Питање јавног надзора и улоге цивилног друштва односи се на домен права на слободан приступ информацијама, а не на правни и безбедносни режим тајности података. У овом контексту, тајност представља изузетак од правила транспарентности, а не њен саставни део. Зато је кључно да се јавна расправа, која се води у другим оквирима, не меша са процедуралном и безбедносно-техничком логиком система тајности, чији је главни циљ заштита стварно осетљивих информација, а не отвореност ради отворености.

ПРИЛОГ 1. - Методологија одређивања и престанка (класификације и декласификације) 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 фомално 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,
- разлозима за декласификацију,
- степену доступности (целокупно/делимично).

4. Појачати 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*.

МОДЕЛ - КОНТРОЛНА ЛИСТА ЗА ПРОЦЕНУ ПОТРЕБЕ ОДРЕЂИВАЊА ТАЈНОСТИ (обавезно се прилаже уз предлог за одређивање тајности, у складу са чланом 11. став 4. Закона о тајности података)

1. Повезаност са законом дефинисаним интересима државе - Документ садржи информације које се односе на интересе Републике Србије у смислу члана 8. став 2. Закона о тајности података:

☐ национална и јавна безбедност

☐ одбрамбени послови

☐ спољнополитички послови

☐ безбедносни и обавештајни послови

2. Процена врсте и нивоа штете *(у складу са чланом 14. Закона о тајности података и Уредбом о начину одређивања степена тајности)* - Откривање информације би проузроковало штету интересима Републике Србије:

☐ **неотклоњиву, тешку штету** по територијални интегритет, уставни поредак, одбрану или међународне односе → **Државна тајна**

☐ **тешку штету** по безбедност, дипломатску позицију или рад служби безбедности → **Строго поверљиво**

☐ **штету** по функционисање органа, критичне процесе или обављање службених послова → **Поверљиво**

☐ **штету** која се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио. → **Интерно**

3. Алтернативе одређивању тајности *(члан 12. Закона о тајности података)* - Да ли постоји могућност да се заштита оствари без одређивања тајности целокупног документа (нпр. редиговањем, заштитом само осетљивих делова)?

☐ Да

☐ Не

4. Статус информације у јавности - Да ли је информација или њен суштински садржај већ доступан јавности (нпр. преко других докумената, отворених извора, објава страних партнера или међународних институција)?

☐ Да

☐ Не

5. Забрањено одређивање тајности *(члан 3. Закона о тајности података)* - Да ли је информација означена као тајна искључиво ради прикривања:

☐ кривичног дела

☐ повреде људских права

☐ злоупотребе службеног положаја

☐ незаконитог деловања органа власти

☐ опасности по живот, здравље или животну средину

→ Ако је одговор „Да“ на било које од наведеног, **одређивање тајности је забрањено** чланом 3. Закона о тајности података.

6. Предложени степен тајности *(члан 14. Закона о тајности података и Уредба)*

☐ Државна тајна
☐ Строго поверљиво
☐ Поверљиво
☐ Интерно

7. Образложење степена тајности (најнижи неопходан степен за спречавање штете, у складу са чланом 11. став 3. Закона о тајности података)

На основу процене, подаци се разврставају или категоришу у један од следећих степена тајности узимајући у обзир озбиљност потенцијалне штете по нарушавање интереса Републике Србије настало као последицу неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последицу друге радње обраде тајних података у складу са уредбама о ближим критеријумима за одређивање степена тајности „државна тајна“, „строго поверљиво“, „поверљиво“ и „интерно“ („Службени гласник Републике Србије“ број 46/2013, 70/2013, 86/2013, 105/2013, 66/2014 и 79/2014):

8. Предвиђени рок трајања тајности - (члан 18. Закона: до 30 година за „Државну тајну”, краће за ниже степене, или до наступања одређеног догађаја)

☐ до _____ (датум)
☐ до наступања догађаја: _____

9. Датум следеће ревизије (обавезно унапред одредити; не може бити дуже од пет година од дана одређивања тајности – члан 22. Закона)

Датум: _____

Описни део – правна основа за одређивање степена тајности - Одређивање степена тајности заснива се на члану 14. Закона о тајности података, који дефинише врсту и тежину штете која би наступила откривањем информације, као и на Уредби о начину и поступку одређивања тајности података, односно докумената („Службени гласник РС“, бр. 8/2011), која прописује:

- да се **„Државна тајна“** одређује када би откривање проузроковало неотклоњиву, тешку штету по националну безбедност, територијални интегритет, одбрану или уставни поредак;
- да се **„Строго поверљиво“** одређује када би откривање проузроковало тешку штету по спољну политику, дипломатске односе или рад безбедносно-обавештајних служби;
- да се **„Поверљиво“** одређује када би откривање проузроковало штету по функционисање органа, критичне административне процесе или безбедност информационих система;
- да ознака **„Интерно“** као део режима тајности у смислу Закона, користи се за податке чије откривање може проузроковати штету, односно утицати на

унутрашњи рад органа, због чега задире у јавни интерес и оправдава ограничење права на приступ информацијама.

Степен тајности утврђује се пропорционално и у складу са принципом најнижег могућег степена неопходног за спречавање штете (члан 11. став 3 ЗТП). Одлука се доноси од стране органа јавне власти, уз обавезно образложење и документовану процену ризика, у складу са члановима 11. и 22. Закона о тајности података.

Ова контролна листа може се користити као стандардизовани образац у свим органима јавне власти у Републици Србији и представља оперативну примену троструког теста из члана 8. Закона: **интерес – штета – претежност**.

ПИТАЊА ЗА ДИСКУСИЈУ:

„Када тајност више није средство заштите државе, већ алат за управљање информацијама - шта се заправо штити?“

Ова питања отварају простор за размену искустава, анализу изазова и дефинисање добрих пракси у области заштите тајних података. Циљ је истражити границу између легитимне безбедносне заштите и прекомерног ограничавања приступа информацијама и како ту равнотежу обезбедити кроз правни оквир, институционалне механизме и политичку вољу.

Словенија има један од најразвијенијих система у региону, а Канцеларија за варност тајних податков има стручну надлежност. Ипак, пример термалног центра у Рогашкој Слатини показује да чак и у тако уређеном систему долази до прекомерне класификације. Како видите могућност трансформације Канцеларије из административног органа у активни надзорни механизам? И како дефинисати границу између оправдане тајности и непотребног ограничења приступа информацијама јавног интереса?

Хрватска је формално усклађена са стандардима ЕУ и НАТО-а, а Уред Вијећа за националну сигурност има улогу координације политике и стручног надзора. Међутим, пример ретроактивне класификације уговора о модернизацији БВМ возила показује да се тајност понекад користи након медијске пажње, а не као превентивна мера. Постоје ли услови да се такве одлуке преиспитују пре него што постану фактом? И како обезбедити да Уред има довољне надлежности и моћи да ефикасно исправи таква одступања?

Босна и Херцеговина Услед политичке фрагментације надлежност за тајне податке је распоређена на више нивоа власти. Пример накнадног класификације извештаја о неправилностима у Термоелектрани „Бања Лука“ након медијског интересовања доводи у питање да ли се тајност користи ради заштите државе или избегавања одговорности. Како успоставити јединствени систем процене ризика и надзора који би функционисао независно од политичких притисака и осигурао транспарентност пројеката финансираних из европских средстава?

Црна Гора Као чланица НАТО-а, Црна Гора има формално усклађен законски оквир, али пример уговора са KMW показује да се често уводи највиши степен тајности без конкретне процене ризика. Како објаснити дисбаланс између међународне транспарентности и домаће тајновитости? И како јачати улогу Дирекције за тајне податке да може деловати када се тајност користи не за безбедност, већ за избегавање демократског надзора?

Северна Македонија Дирекција за класификоване информације је формално ојачана, али пример гасовода „Беласица“ показује да се ознака тајности користи и за пројекте транспарентне на међународном нивоу иако нема безбедносно осетљивих података. Како разјаснити критеријуме за примену ознаке „национални интерес“ у односу на „безбедносни интерес“? И како обезбедити да ознака „интерно“ не постане средство за избегавање јавног надзора?