

- METODOLOGIJA ODREĐIVANJA I PRESTANKA (KLASIFIKACIJA I DEKLASIFIKACIJA) TAJNOSTI PODATAKA -

Režim tajnosti ima jednu osnovnu svrhu: da zaštiti informacije čije bi otkrivanje moglo naneti stvarnu, dokazivu štetu interesima nacionalne bezbednosti, odbrane, spoljnih odnosa ili stabilnom funkcionisanju države. Ipak, iskustva zemalja regiona pokazuju da praksa često odstupa od ove namere. Problem ne leži u zakonskom okviru, već u slabostima njegove primene, nedostatku standardizovanih rizičnih procena i ograničenim mehanizmima demokratskog nadzora. Zato je neophodno jasno definisati legitimne korake u postupku određivanja, klasifikacije i ukidanja tajnosti – kako bi se razgraničila opravdana zaštita od institucionalnog skrivanja.

A) Određivanje tajnosti ili klasifikacija podataka i dokumenata

1. Kada se uopšte može postaviti tajnost? - Osnovni princip je jednostavan: **tajnost mora biti izuzetak, a ne pravilo**. Prema članu 8. Zakona o tajnosti podataka, informacija se može označiti kao tajna samo ako su ispunjena sva tri uslova:

- odnosi se na interes Republike Srbije,
- njeno otkrivanje bi nanelo štetu,
- potreba zaštite je pretežnija od javnog interesa da se informacija obelodani.

Ovaj trostruki test – **interes, šteta, pretežnost** – predstavlja neophodan filter koji obavezno prethodi svakoj odluci.

Šta po zakonu nikada ne može biti tajno (član 3):

Zakon ne zabranjuje određivanje tajnosti svih podataka koji se odnose na krivična dela, zloupotrebe ili opasnosti - već isključuje mogućnost da se podatak proglasi tajnim isključivo radi prikrivanja krivičnog dela, prekoračenja ovlašćenja, zloupotrebe službenog položaja ili drugih nezakonitih radnji organa javne vlasti. Ako je tajnost uvedena s takvom namerom, ona nije pravno važeća, a odluka je ništavna. Ovo znači da je ključna odrednica namera, a ne samo sadržaj informacije. Stoga čak i podaci o korupciji ili kriminalu mogu biti tajni ako njihovo otkrivanje stvarno, konkretno i verovatno ugrožava bezbednosni interes (na primer, identitet izvora u istragama organizovanog kriminala). Međutim, ako se tajnost koristi da bi se sprečilo otkrivanje nepravilnosti, onda se radi o zloupotrebi režima tajnosti, a ne o legitimnoj zaštiti.

2. Kako se određuje stepen tajnosti? - Tajnost nije jedna kategorija – ona je skala. Stepen zavisi od procenjene visine i vrste štete.

Tabela 1: Stepni tajnosti i vrsta štete

Stepen tajnosti	Opis štete koja bi nastupila otkrivanjem informacije
Državna tajna	Neotklonjiva, teška šteta po teritorijalni integritet, ustavni poredak ili međunarodne odnose
Strogo poverljivo	Teške posledice po bezbednost, diplomatsku poziciju ili rad službi bezbednosti
Poverljivo	Šteta po funkcionisanje organa ili kritične administrativne procese
Interno	Ugrožavanje unutrašnjeg rada organa bez širih posledica po javni interes

Ključno pravilo: stepen tajnosti mora biti najniži mogući za sprečavanje štete, nikada viši.

U praksi regiona, međutim, najniži stepen („interno“) često se tretira kao zamena za „tajno“, dok se viši stepeni koriste masovno i nekritički.

3. Procena rizika – temelj svake odluke

Odluka o tajnosti mora biti zasnovana na formalizovanoj proceni rizika. Ta procena obuhvata:

- **identifikaciju tipa informacije** (npr. operativni plan, ugovor, analize),
- **procenu verovatnoće i težine štete**, ukoliko podatak postane dostupan neovlašćenom licu,
- **proveru realističnosti pretnje** (šteta mora biti stvarna, ozbiljna i neposredna),
- **test pretežnosti:** da li bi šteta od otkrivanja bila veća od dobiti za javni interes?

Bez ove procedure, odluka o tajnosti nema pravnu težinu i ne može biti dugoročno održiva.

4. Obrazloženje i dokumentacija

- Odluka o tajnosti mora biti formalno obrazložena, u skladu sa Uredbom o označavanju. Obrazloženje sadrži:

- naziv dokumenta i opis sadržaja koji se štiti,
- predloženi stepen tajnosti,

- procenu moguće štete,
- pozivanje na član 8. Zakona,
- proveru da sadržaj ne spada u kategorije zabranjene za tajnost (član 3),
- rok trajanja tajnosti,
- predviđeni datum revizije.

Katalozi tajnih podataka mogu olakšati rad organa, ali **oni sami moraju biti rezultat rizične procene, a ne administrativna rutina.**

5. Prestanak tajnosti – jednako važan kao njeno uvođenje

Ozbiljan slab prostor u praksi državnih organa jeste odsustvo sistematskog deklasifikovanja. Zakon propisuje da tajnost prestaje:

- po isteku roka (do 30 godina za državnu tajnu),
- nakon nastupanja događaja na koji se odnosila (npr. završetak operacije, ugovora, projekta),
- po rešenju Poverenika ili suda.

Ipak, mnogi dokumenti ostaju „tajni“ i nakon što više ne postoji nijedan razlog za to, što podriva kredibilitet celog sistema.

6. Gde počinju zloupotrebe? - Zloupotreba nastaje onda kada tajnost postane sredstvo političke ili institucionalne kontrole informacija. Najčešći modeli su:

- prekomerno označavanje („sve je tajno“),
- retroaktivno označavanje nakon objavljivanja u medijima,
- klasifikacija radi izbegavanja parlamentarnog ili javnog nadzora,
- masovno skrivanje ugovora u odbrani, energetici i infrastrukturi,
- produžavanje tajnosti bez nove procene rizika.

Tajnost tada više ne štiti državu, već štiti aktera koji želi da izbegne pitanja.

7. Ključ je u balansu - Cilj nije ukinuti tajnost, već je **vratiti njenoj izvornoj funkciji**. U demokratskom poretku:

- tajnost je opravdana kad štiti državu,
- ali je nelegitimna kada štiti vlasti od javnosti.
- Zato je neophodno:
- da svaka odluka o tajnosti bude zasnovana na proverljivoj proceni rizika,
- da obrazloženje bude zapisano i dostupno Povereniku,
- da deklasifikacija bude rutinska, a ne izuzetak,

- da se ojačaju nadzorni mehanizmi (Poverenik, Kancelarija, Direkcije).

Ovo nije kritika bezbednosnog sistema – već predlog funkcionalne reforme u kojoj režim tajnosti postaje precizan, kontrolisan, vremenski ograničen i usmeren na zaštitu države, a ne političke moći.

B) Prestanak tajnosti i deklasifikacija: legitimnost sistema zavisi od vremena

Jedan od najčešće zanemarenih elemenata režima tajnosti jeste njegova **vremenska ograničenost**. Tajnost nije trajno stanje, ona mora imati jasno definisan rok trajanja i uslove pod kojima prestaje. Ipak, u praksi širom regiona, posebno u Srbiji, Bosni i Hercegovini i Crnoj Gori, ova faza ostaje nedovoljno primenjena. Rezultat je dugotrajno zadržavanje dokumenata u statusu „tajno“ i onda kada pravni i bezbednosni osnovi za klasifikaciju više ne postoje.

Kada i kako tajnost treba da prestane? - Prema Zakonu o tajnosti podataka, tajnost prestaje:

- **po isteku zakonskog roka** (do 30 godina za „državnu tajnu“, kraće za niže stepene),
- **nastupanjem događaja** na koji se tajnost odnosila (završetak projekta, realizacija operativnog plana),
- **odlukom Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka**
- **rešenjem Poverenika ili suda,**
- **rešenjem organa koji je dokument odredio tajnim ili klasifikovao**, nakon nove procene rizika.

To znači: *svaki tajni dokument mora biti predmet redovnog preispitivanja*, ne samo prilikom određivanja tajnosti, već i tokom celokupnog perioda njenog važenja.

Gde leži problem u praksi? - Umesto da bude sistemski i rutinski proces, deklasifikacija je u mnogim zemljama regiona:

- zaboravljena – dokumenti ostaju „tajni“ i nakon što su postali istorijski materijal,
- neformalna – bez nove procene rizika ili validnog obrazloženja,
- popravna – pokreće se tek posle žalbi, medijskog pritiska ili skandala,
- nepotpuna – dostavlja se „redigovana“ verzija sa gotovo potpuno prekrivenim sadržajem.

Čak i kada Poverenik naloži prestanak tajnosti ili deklasifikaciju (kao u predmetima PV-9 u Srbiji, BVM u Hrvatskoj ili u slučaju „Belasica“ u Severnoj Makedoniji), organi često formalno ispune obavezu, ali suštinski ne omoguće pristup podacima. U takvim situacijama „pravo na pristup informacijama“ postaje samo formulacija, a ne stvarno pravo.

Zašto je prestanak tajnosti ili deklasifikacija neophodna?

1. Čuva verodostojnost režima tajnosti - Tajnost je snažna samo kada je izuzetak i kada je vremenski ograničena. Kada je trajna - ona se pretvara u instrument upravljanja informacijama, a ne u instrument zaštite države.

2. Omogućava demokratski nadzor - Deklasifikovani dokumenti omogućavaju naknadni uvid u:

- političke odluke,
- korupcijske mehanizme,
- finansijske zloupotrebe,
- propuste u upravljanju krizama.

Bez toga, institucionalna prošlost postaje „mrtva zona“ u kojoj se ništa ne može analizirati i iz koje se ništa ne može naučiti.

3. Podržava istorijsko, akademsko i reformsko istraživanje - Arhivska građa je neophodna za naučna istraživanja, institucionalnu evaluaciju i procese pomirenja. U mnogim državama regiona, međutim, tajnost se ne ukida ni nakon nekoliko decenija - iako događaji odavno pripadaju istorijskom arhivu.

4. Ispunjava međunarodne standarde - EU i NATO imaju stroge mehanizme automatske deklasifikacije po isteku roka. Dok su ovi mehanizmi u Rumuniji i Bugarskoj već deo redovne administracije, u državama zapadnog Balkana uglavnom su zapostavljeni.

Šta u regionu funkcioniše dobro?

- **Slovenija:** Poverenik redovno preispituje odluke i efikasno nalaže deklasifikaciju.
- **Hrvatska:** Ured Vijeća za nacionalnu sigurnost ima ovlašćenja za iniciranje provera, ali ih koristi povremeno.
- **Severna Makedonija:** Nove zakonske izmene uvode automatsku deklasifikaciju - važan pomak, mada primena još nije ujednačena.

Šta je neophodno uraditi?

1. Uvesti obaveznu, automatski prestanak tajnosti ili deklasifikaciju – ona formalno u propisima postoji ali se u praksi ne primenjuje dosledno. Po isteku roka tajnost mora prestati, osim ako organ ne donese novu, obrazloženu odluku o produženju.

2. Uvesti javni rok revizije - Svaki dokument sa oznakom tajnosti mora imati datum revizije — najkasnije na svakih pet godina.

3. Objavljivati godišnje izveštaje o prestanku tajnosti ili deklasifikaciji – Poverenik, Direkcije i nadzorna tela treba da objavljuju podatke o:

- broju dokumenata kojima je prestala tajnost, odnosno deklasifikovanih,
- razlozima za deklasifikaciju,
- stepenu dostupnosti (celokupno/delimično).

4. Pooštriti kontrolu nad „redigovanim“ dokumentima - Dostavljanje potpuno prekrivenih dokumenata mora biti predmet pravne ocene, a ne tehničkog tumačenja.

5. Edukovati službenike o prirodi privremenosti tajnosti - Uporno shvatanje da je „tajno“ isto što i „trajno“ predstavlja strukturni problem koji se rešava samo sistemskim obukama.

Zaključak: tajnost koja nestaje je jača od tajnosti koja traje

Tajnost koja nikada ne prestaje - gubi smisao. Sistem u kome se informacije ne vraćaju u javnu sferu osuđuje sam sebe na neprozirnost i institucionalno slabljenje.

Zato je prestanak tajnosti (deklasifikacija) jednako važna kao i određivanje tajnosti (klasifikacija). Ona je dokaz:

- da institucije kontrolišu svoje informacione tokove,
- da poštuju zakon,
- da država nema strah od transparentnosti, čak ni onda kada je neprijatna.

Cilj nije da sve bude uvek dostupno. Cilj je da ništa ne bude trajno sakriveno. U modernoj demokratiji, legitimitet režima tajnosti ne meri se time koliko smo dokumenata zaključali - već *time kada, kako i u kojoj meri ih otvaramo.*