



**ТАЈНИ ПОДАЦИ, ЈАВНА ПОЛИТИКА И
БЕЗБЕДНОСНА ПОЛИТИКА:**

**СТУБОВИ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ
РЕПУБЛИКЕ СРБИЈЕ**

Скрипта

Проф.др Горан Д. Матић

Београд
2025. година

САДРЖАЈ

Уводна разматрања	3
Уопштено о јавним политикама	4
Савремени изазови	5
Разлика између политике и јавне политике	6
Образовна политика	6
Здравствена политика	6
Социјална политика	6
Економска политика	6
Политика заштите животне средине	6
Енергетска политика	7
Политика безбедности и јавног реда	7
Одбрамбена и спољна политика	7
Транспортна и саобраћајна политика	7
Политика запошљавања и тржишта рада	7
Културна политика	7
Пољопривредна и рурална политика	7
Политика информационог друштва и дигитализације	7
Урбана политика и политика становања	7
Национална безбедност као јавна политика	8
Обавештајно-безбедносна политика – окосница очувања националне безбедности	11
Улога Савета за националну безбедност и Бироа за координацију у обавештајно- безбедносној политици Републике Србије	14
Улога Канцеларије Савета за националну безбедност и заштита тајних података у контексту Закона о тајности података	17
Јавне политике и штићени подаци у Републици Србији	18
Штићени подаци – општи оквир	19
Класификовани подаци – погрешна употреба у пракси	21
Категорије штићених података	23
Јавне политике и управљање штићеним подацима	24
Тајни подаци у функцији безбедносне политике као облика јавне политике	27
Одређивање степена тајности података	31
Методологија за процену и одређивање степена тајности података	34
1. Основни принципи	35
2. Законско искључење од могућности означавања података као тајних	36
3. Процена потребе за заштитом података	37
4. Процена могуће штете – критеријуми за одређивање степена тајности	38
5. Баланс интереса – примена јавног интереса	40
6. Документација – образложење одлуке о тајности	42
Политичка одговорност носилаца највиших функција у раду са тајним и страним тајним подацима	47
Кључни елементи одговорности	47
Кривично дело неовлашћеног одавања тајних података – преглед члана 98. Закона о тајности података	48
Непажња (нехат)	50
Правна и безбедносна важност кривичног дела из члана 98. Закона о тајности података	51
Упоредни осврт: Међународна пракса	52
Сличности и разлике између одређених кривичних дела у српском законодавству	52

Сличности и разлике између кривичног дела из члана 98. Закона о тајности података и кривичног дела шпијунаже из члана 315. Кривичног законика.....	54
Прекршајна одговорност одговорног лица у органу јавне власти и руковаоца тп.	55
1. Прекршајна одговорност одговорног лица у органу јавне власти (члан 99).....	55
2. Прекршајна одговорност руковаоца тајних података (члан 100 у вези са чланом 34)...	56
Прекршајна одговорност у систему заштите тајних података.....	57
Радно-дисциплинска одговорност због непоштовања процедура у раду са тајним подацима	58
1. Увод: Обавезе у раду са тајним подацима	58
2. Правни основ радно-дисциплинске одговорности	58
3. Етички кодекси и професионалне обавезе	59
4. Последице непоштовања процедура	60
5. Превенција и одговорност	60
Одговорност за накнаду штете у раду са тајним подацима	60
1. Правни оквир за одговорност за штету	60
2. Одговорност запослених и државних службеника	61
2.1. Лична одговорност.....	61
2.2. Солидарна одговорност државе и запосленог.....	61
3. Одговорност правних лица.....	61
3.1. Јавни органи и институције	61
3.2. Приватна правна лица.....	61
4. Посебни случајеви у државним службама	62
4.1. Војска и безбедносне службе.....	62
4.2. Полиција.....	62
4.3. Државна управа.....	62
5. Врсте штете и начин накнаде	62
6. Превентивне мере и смањење ризика.....	62
7. Одговорност за накнаду штете у раду са тајним подацима обухвата:	62
Допринос организације у настанку штетног догађаја у раду са тајним подацима	63
Организациона одговорност.....	63
Процедурални пропусти	63
Технички и кадровски пропусти	63
Утицај на одговорност физичких и правних лица	63
Кривична одговорност.....	63
Прекршајна одговорност	64
Радно-дисциплинска одговорност.....	64
Одговорност у поступку накнаде штете (Закон о облигационим односима)	64
Закључна разматрања: Тајни подаци, јавна политика и безбедносна политика као стубови националне безбедности Републике Србије	65
О АУТОРУ	67

Уводна разматрања

Национална безбедност представља један од најважнијих темеља стабилности, сигурности и развоја сваке државе. У Републици Србији, три кључна стуба – тајни подаци, јавне политике и безбедносна политика – играју неприкосновену улогу у очувању виталних националних интереса и заштити грађана. Њихова међусобна повезаност и интеграција кроз институционалне механизме омогућавају ефикасно функционисање система националне безбедности у условима савременог доба.

Јавне политике представљају инструменте кроз које држава одговара на сложене друштвене изазове. Делују као механизми за очување стабилности, унапређење образовања и здравства, развој економије, заштиту животне средине и реаговање на безбедносне ризике. У том контексту, тајни подаци добијају посебну важност јер обезбеђују критичне информације за планирање и имплементацију мера које штите територијални интегритет, уставни поредак и друге виталне интересе државе.

Савет за националну безбедност и Биро за координацију рада служби безбедности играју кључну улогу у управљању системом националне безбедности. Њихово деловање обухвата анализу, интеграцију и заштиту тајних података, као и синхронизацију одлука на највишем нивоу власти. Канцеларија Савета за националну безбедност и заштиту тајних података осигурава примену Закона о тајности података, чиме доприноси очувању интегритета информација и транспарентности институционалних процеса.

Тајни подаци не представљају само средство оперативног деловања, већ имају снажну правну и политичку димензију. Њихова адекватна заштита захтева успостављање јасних процедура, као и развој културе одговорности и транспарентности у јавним институцијама. Успостављање баланса између потребе за тајношћу и захтева за јавним увидом кључно је за јачање поверења грађана у институције и очување демократских вредности.

Овај текст анализира улогу тајних података у функцији јавних и безбедносних политика, истражујући њихов значај у изградњи стабилности, отпорности и сигурности Републике Србије. Кроз разматрање институционалних механизма, правних оквира и стратешких докумената, представља се свеобухватан приступ који је неопходан за одрживи развој и сигурност државе у условима глобалних и регионалних изазова.

Уопштено о јавним политикама

Политика представља процес доношења одлука који се односи на организовање, управљање и расподелу моћи унутар једне заједнице, најчешће у оквиру државе. Она обухвата начине на које појединци и групе утичу на доношење одлука, спровођење власти и формулисање правила и закона. Политика се бави питањима ко управља, како управља и у чијем интересу. Према Т. Дуге-у, политика се може дефинисати као „шта год влада одлучи да ради или не ради“ (*public policy is whatever governments choose to do or not to do*).

Политика може бити:

- **партијска или изборна политика**, која обухвата деловање политичких странака, изборе, кампање и борбу за власт;
- **међународна политика**, која се бави односима између држава, дипломатијом, спољном политиком и глобалном безбедношћу;
- **економска политика**, која се односи на управљање националном привредом, буџетом, порезима и тржиштем;
- **јавна политика**, као посебна област, фокусирана на формулисање и спровођење конкретних мера и програма који решавају друштвене проблеме у интересу грађана.

За разлику од опште политике, јавна политика представља организован, стручан и институционализован одговор државе на конкретна питања у друштву – попут здравства, образовања, безбедности, заштите животне средине или социјалне заштите. Док се партијска политика бави освајањем власти, јавна политика се бави управљањем и решавањем стварних проблема, кроз доношење и примену закона, програма и стратегија.

Јавне политике представљају скуп одлука, мера и активности које доносе државне институције ради решавања друштвених проблема и унапређења општег добра. Оне обухватају различите области као што су образовање, здравство, економија, заштита животне средине и безбедност. Како наводе Howlett, Ramesh и Perl (2009), јавне политике се не одвијају у празнини, већ унутар „подсистема политика“ (*policy subsystems*), где различити актери покушавају да утичу на исход.

Историјски гледано, појам јавних политика се развијао постепено. Иако су још у старим цивилизацијама постојале одређене форме управљања и уређивања јавног живота – попут закона у Хамурабијевом законнику или у римском праву – савремено разумевање јавне политике појављује се у контексту модерне државе. Са настанком националних држава у 17. и 18. веку, а нарочито током 19. и 20. века, почиње систематски развој институција које формулишу и спроводе јавне политике. Развој социјалне државе после Другог светског рата убрзао је увођење структурисаних политика у здравству, образовању, социјалној заштити и другим областима.

Као научна дисциплина, проучавање јавних политика се формира у Сједињеним Америчким Државама средином 20. века, са тежњом да се државна активност анализира на основу доказа, а не искључиво политичких идеологија. Овај приступ, познат као „*evidence-based policy*“, све више добија на значају у савременим системима управљања.

Процес креирања јавних политика, познат као „*политички циклус*“, обухвата неколико фаза:

- **Идентификовање проблема** (постављање на дневни ред) – Препознавање друштвених изазова који захтевају интервенцију државе.
- **Формулисање решења** – Израда могућих приступа и избора конкретне мере или програма.
- **Легитимизација** – Усвајање политике од стране надлежних органа (нпр. парламент, влада).
- **Имплементација** – Спровођење политике у пракси кроз институције и јавну администрацију.
- **Евалуација** – Процена ефикасности, утицаја и потребе за ревизијом политике.

Овај процес је динамичан и укључује различите актере, укључујући изабране званичнике, државне службенике, стручњаке, невладине организације, медије и грађане. Њихово деловање често зависи од политичког, економског и друштвеног контекста.

Јавне политике се могу класификовати према врсти интервенције:

- **Директне мере**, као што су закони, регулативе и нормативни акти.
- **Индиректне мере**, као што су порези, субвенције, економски подстицаји или информативне кампање.

Циљ сваке политике је да утиче на понашање појединаца и организација у правцу који је у складу са друштвеним интересима, уз уравнотежено коришћење ресурса и очување вредности попут правде, солидарности и слободе. Према Howlett-у, добри процеси јавних политика захтевају комбиновање аналитичке рационалности и политичке реалности.

У савременом добу, доносиоци одлука све више користе податке и технологију за креирање политика заснованих на доказима. Овај приступ омогућава прецизније дефинисање проблема и ефикасније спровођење решења, уз праћење исхода кроз мерење утицаја и индикаторе успеха. У том контексту, растућа употреба дигиталних алата и „отворених података“ (open data) доприноси транспарентности и ефикасности.

Савремени изазови

Технократија vs. демократија: Како осигурати да стручњаци не доминирају над гласом грађана?

Криза поверења: Недостатак транспарентности у доношењу одлука (нпр. нејасни критеријуми за доделу државних средстава).

Глобални утицаји: Притисак међународних институција (ЕУ, ММФ) на домаће политике.

Укључивање грађана и транспарентност у процесу доношења јавних политика доприносе већем поверењу у институције и бољем прилагођавању политика стварним потребама друштва. Партиципативни модели управљања, јавне расправе и отворени подаци све више постају стандард у савременој демократији.

Разлика између политике и јавне политике

Политика (општи појам)	Јавна политика
Борба за моћ и утицај.	Управљање ресурсима и решавање проблема.
Идеолошка оријентација (нпр. левица/десница).	Технократски приступ (нпр. здравствена реформа).
Примарни актери: политичке странке.	Примарни актери: државне институције, стручњаци.

Области јавних политика - Јавне политике обухватају широк спектар области које се односе на уређење друштвених односа, заштиту јавног интереса и обезбеђивање предуслова за одржив, инклузиван и праведан развој. Свака од ових области представља специфичан друштвени изазов или потребу на коју државни органи, институције и други носиоци јавних овлашћења одговарају кроз стратегије, планске документе, прописе, програме и институционалне механизме. У наставку су систематизоване најважније области јавних политика:

Образовна политика

Уређује систем предшколског, основног, средњег и високог образовања, као и стручног усавршавања и концепт целоживотног учења. Усмерена је на обезбеђивање квалитетног, инклузивног и доступног образовања за све категорије становништва.

Здравствена политика

Обухвата организовање здравственог система, унапређење јавног здравља, мере превенције и контроле болести, финансирање здравствених услуга и функционисање здравственог осигурања, са циљем обезбеђивања одрживог и ефикасног здравственог система.

Социјална политика

Усмерена је на заштиту и подршку социјално угроженим и осетљивим категоријама становништва, развој система социјалне заштите, пензијског и инвалидског осигурања, као и на мере смањења сиромаштва, неједнакости и социјалне искључености.

Економска политика

Обухвата фискалну, монетарну, трговинску, индустријску и развојну политику, са циљем унапређења макроекономске стабилности, раста, запошљавања, инвестиција и конкурентности домаће привреде.

Политика заштите животне средине

Регулише очување природних ресурса, борбу против климатских промена, управљање отпадом, заштиту квалитета ваздуха, воде и земљишта, као и промоцију принципа циркуларне економије и одрживог развоја.

Енергетска политика

Односи се на регулисање производње, преноса, дистрибуције и потрошње енергије, енергетску безбедност, повећање енергетске ефикасности и убрзан прелазак на обновљиве изворе енергије.

Политика безбедности и јавног реда

Обухвата мере заштите грађана, превенцију и сузбијање криминала, укључујући организовани криминал и тероризам, као и реформу сектора полиције, правосуђа и унутрашњих послова ради јачања владавине права.

Одбрамбена и спољна политика

Усмерена је на заштиту суверенитета и територијалног интегритета државе, одржавање и развој одбрамбених капацитета, као и на међународне односе, спољну трговину, дипломатију и сарадњу са међународним организацијама.

Транспортна и саобраћајна политика

Уређује развој и одржавање путне, железничке, ваздушне и водне инфраструктуре, побољшање безбедности саобраћаја, као и унапређење одрживих видова превоза и урбане мобилности.

Политика запошљавања и тржишта рада

Регулише радне односе, мере активне политике запошљавања, заштиту права запослених, као и развој људског капитала кроз унапређење знања, вештина и компетенција радне снаге.

Културна политика

Обухвата очување и унапређење културне баштине, подршку уметничком стваралаштву, културним индустријама и институцијама, заштиту језичког и културног идентитета, као и слободу медија и културног изражавања.

Пољопривредна и рурална политика

Усмерена је на развој пољопривредне производње, осигурање безбедности хране, подршку руралним заједницама, очување пољопривредног земљишта и промоцију одрживих агроекономских пракси.

Политика информационог друштва и дигитализације

Регулише развој дигиталне инфраструктуре, електронске управе, приступ интернету, заштиту података и сајбер безбедност, као и унапређење дигиталних услуга у јавном сектору.

Урбана политика и политика становања

Обухвата урбано планирање, развој и управљање јавним просторима, стамбену политику, одрживи развој насеља и инфраструктурну повезаност у градским и приградским подручјима.

Све наведене области јавних политика међусобно су повезане и условљене, те захтевају интерсекторску сарадњу и координисан приступ. Успешност у једној области често зависи од ефикасности у другим. Добро осмишљене, инклузивне и транспарентно спроведене јавне политике омогућавају држави да адекватно одговори на комплексне изазове савременог доба, унапреди квалитет живота грађана и подстакне дугорочни друштвени и економски развој.

Национална безбедност као јавна политика

Национална безбедност представља једну од кључних области јавне политике чија је примарна сврха очување територијалног интегритета, суверенитета, уставног поретка и виталних интереса државе. Као свеобухватан концепт, она обухвата широк спектар аспеката који су од суштинског значаја за стабилност и функционисање друштва. У основи националне безбедности лежи интеграција војних, политичких, економских, енергетских, сајбер, здравствених и еколошких елемената, чије међусобно деловање доприноси јачању отпорности државе према унутрашњим и спољним претњама.

Као јавна политика, национална безбедност мора бити заснована на јасно дефинисаним стратешким приоритетима који одражавају виталне интересе државе и одговор на савремене изазове. У том смислу, она интегрише механизме заштите критичних инфраструктура, одбране од хибридних претњи и развој способности реаговања на кризне ситуације. Тајни подаци играју кључну улогу у обезбеђивању ефикасности мера националне безбедности, омогућавајући правовремено и прецизно одлучивање на основу поузданих информација.

У том контексту, национална безбедност се јасно дефинише као један од основних инструмената јавне политике који је дубоко повезан са принципом транспарентности и заштитом тајних података. Док транспарентност осигурава поверење грађана у институције, заштита класификованих информација штити виталне интересе државе. Успостављање баланса између ова два принципа је од суштинског значаја за легитимност система националне безбедности.

Безбедносна политика као област јавне политике захтева јасан правни оквир и координацију институција, укључујући Савет за националну безбедност и Биро за координацију рада служби безбедности. У Србији, њихова улога доприноси не само очувању националног суверенитета, већ и изградњи друштвене отпорности кроз јачање механизма превенције и брзог реаговања.

Закључно, национална безбедност као јавна политика није само инструмент за заштиту државе од спољних и унутрашњих претњи, већ и средство за унапређење стабилности и развоја друштва. Њена успешна имплементација зависи од интеграције различитих области и актера, као и од сталног унапређивања стратегија које одговарају на сложене изазове савременог доба.

Политика националне безбедности је скуп усмерених активности, стратегија, закона и мера које држава спроводи ради превенције и одговора на претње. Она обухвата:

- Процену безбедносних ризика и претњи, како спољних тако и унутрашњих;
- Усклађивање и координацију безбедносних сектора (војске, полиције, обавештајних служби и других);
- Законодавни и институционални оквир за деловање у кризним и ванредним ситуацијама;
- Унапређење отпорности друштва на све облике угрожавања, укључујући тероризам, хибридне претње и сајбер нападе;
- Заштиту критичне инфраструктуре и комуникационих система;

- Обезбеђивање јавног реда, мира и заштите грађана.
- Улога појединачних политика у систему националне безбедности

Политика одбране - је усмерена на обезбеђивање војне спремности и заштите државе од спољне оружане агресије. Обухвата:

- развој и опремање оружаних снага,
- стратешко планирање и мобилизацију,
- учешће у међународним мисијама и савезима (нпр. Партнерство за мир),
- цивилну заштиту у условима рата и ванредног стања.

Спољна политика - подржава националну безбедност кроз дипломатске односе, економску сарадњу, међународне споразуме и учешће у безбедносним структурама. Њена улога је:

- изградња и одржавање савезништава и стратешких партнерстава,
- спречавање међународних конфликта кроз дипломатију,
- утицај на регионалну и глобалну стабилност.

Политика јавне безбедности - Ова политика обухвата активности полиције, безбедносних служби и других тела која се баве очувањем унутрашње безбедности. Кључни елементи укључују:

- борбу против криминала, тероризма и екстремизма,
- контролу граница и миграција,
- заштиту јавног реда и мира,
- реаговање у ванредним ситуацијама и катастрофама.

Сајбер безбедност и савремене претње - У савременом дигиталном добу, сајбер безбедност је постала саставни и неодвојиви део политике националне безбедности. Она укључује:

- заштиту информационих система државе и критичне инфраструктуре (енергетика, транспорт, здравство, комуникације),
- борбу против сајбер криминала и дигиталног шпијунажа,
- подизање свести и едукацију грађана и институција,
- сарадњу са међународним партнерима у борби против глобалних сајбер претњи.

Национална безбедност захтева интердисциплинарни и међуресорни приступ. Ниједна институција не може самостално да гарантује безбедност – неопходна је сарадња:

- између министарстава (одбране, унутрашњих послова, спољних послова, правде, здравља и др.),
- између државног и локалног нивоа,
- између јавног и приватног сектора,
- са грађанским друштвом и међународним партнерима.

Стратегија националне безбедности - Стратегија националне безбедности је основни документ који дефинише најважније аспекте очувања државних интереса, приоритете, претње и механизме заштите националне сигурности. Овај документ служи као свеобухватни оквир који усмерава све секторске стратегије, политике и мере које држава предузима за очување своје стабилности, суверенитета и виталних вредности.

Стратегија националне безбедности заузима посебно место у систему јавних политика, јер интегрише различите области као што су одбрана, јавни ред, економска сигурност, заштита животне средине, сајбер безбедност и међународни односи. Кроз овај документ, држава формулише своје одговоре на комплексне безбедносне изазове модерног доба, укључујући глобалне хибридне претње, организовани криминал, тероризам и климатске промене.

У Републици Србији, **Стратегија националне безбедности** се редовно ажурира како би одразила актуелни геополитички контекст, развој домаћих и међународних околности, и потребе друштва. Њено ажурирање укључује анализу безбедносних ризика, процену претњи и дефинисање конкретних корака за њихово ублажавање. У том процесу учествују кључне институције као што су Савет за националну безбедност, Биро за координацију рада служби безбедности и други државни органи.

Приоритети националне безбедности одређују области од суштинског значаја за државу, као што су очување територијалног интегритета, уставног поретка, безбедност грађана, одрживи економски развој и заштита природних ресурса. Претње националној безбедности дефинишу спољни и унутрашњи фактори који могу угрозити стабилност државе, укључујући тероризам, организовани криминал, сајбер нападе, хибридне претње и природне катастрофе.

Циљеви националне безбедности формулишу дугорочне и краткорочне циљеве који усмеравају деловање државних органа, са акцентом на превенцији ризика и јачању система отпорности. Инструменти заштите укључују свеобухватан сет мера, механизма и ресурса, попут законодавства, оперативних процедура, међународне сарадње и укључивања грађана у систем безбедности.

Посебан значај стратегије огледа се у њеној улози координатора различитих актера. Документ омогућава синхронизовано деловање институција, интеграцију капацитета на националном и локалном нивоу, као и сарадњу са међународним партнерима. Таква интегрисана перспектива је неопходна за успех у савременом динамичном и комплексном безбедносном амбијенту.

У будућности, Стратегија националне безбедности мора наставити да се прилагођава новим изазовима, као што су напредак технологије, унапређење сајбер безбедности и очување природних ресурса. Њен развој мора бити заснован на доказима, партиципативном приступу и поштивању демократских принципа. Кроз ефикасну имплементацију стратегије, Србија ће моћи да обезбеди дугорочну стабилност и заштити интересе својих грађана.

Национални интерес и безбедносна политика - Питање националног интереса једне државе није лако дефинисати, јер одговор на њега зависи од историјског контекста, вредносног система друштва, опажања јавности и интерпретације доносилаца одлука. Национални интерес добија пуно значење само уколико се сагледава у ширем историјском смислу, као резултат историјских тежњи једне нације.

Према Стратегији националне безбедности Републике Србије, кључни национални интереси обухватају:

- очување суверености, независности и територијалне целовитости;
- унутрашњу стабилност и безбедност;
- заштиту српског народа где год он живи, као и националних мањина и њиховог идентитета;
- мир и стабилност у региону и свету, европске интеграције и чланство у ЕУ;
- економски развој и очување животне средине и ресурса државе.

На тим основама гради се безбедносна политика, као посебна јавна политика усмерена ка очувању виталних вредности друштва:

- Индивидуалне вредности – људска права, слободе, приватна својина;
- Вредности група – права и положај мањина, избеглица, особа са инвалидитетом;
- Националне вредности – уставни поредак, јавни ред, суверенитет, природна добра;
- Међународне вредности – очување међународног мира, стабилних односа и поштовање међународног права.

Савремени безбедносни амбијент - На обликовање безбедносне политике утичу бројни општи и специфични фактори:

- историјско наслеђе и геополитички положај;
- процеси транзиције и вредносне трансформације;
- друштвена и економска развијеност;
- природни и кадровски ресурси;
- искуства државне управе;
- културни и верски образац друштва;
- степен развијености цивилног сектора и медија.

Обавештајно-безбедносна политика – окосница очувања националне безбедности

Обавештајно-безбедносна политика представља кључан сегмент опште безбедносне политике сваке државе и осигурава свеобухватан и проактиван приступ заштити виталних националних интереса. Њено деловање обухвата систематско прикупљање, анализу, обраду и коришћење обавештајних података који су од пресудног значаја за доношење стратешких одлука и реаговање на безбедносне изазове.

Суштина обавештајно-безбедносне политике лежи у правовременом препознавању и ефикасном супротстављању безбедносним ризицима, претњама и изазовима који могу угрозити стабилност, суверенитет, уставни поредак и основне вредности државе. Ова политика се ослања на координисану сарадњу између различитих безбедносних служби, укључујући обавештајне агенције, полицију, оружане снаге и правосудне институције.

Обавештајно-безбедносна политика покрива широк спектар активности, укључујући борбу против тероризма, сајбер претњи, организованог криминала, страних утицаја и хибридних ризика. Поред тога, посебан акценат ставља се на заштиту критичне инфраструктуре, информационих система и осигурање енергетске и економске стабилности. Она такође игра кључну улогу у изградњи друштвене отпорности, превенцији криза и унапређењу јавне безбедности.

Ефикасност обавештајно-безбедносне политике зависи од сталне процене безбедносног амбијента, прилагођавања савременим изазовима и увођења иновација у методологији рада безбедносних служби. Ова политика мора бити дубоко интегрисана у правни и институционални систем државе, ослањајући се на принципе професионализма, транспарентности и законитости.

На крају, обавештајно-безбедносна политика представља стратешки инструмент који омогућава држави да благовремено идентификује ризике, реагује на претње и осигура своју стабилност, суверенитет и безбедност грађана. Њена улога је незаменљива у динамичном и непредвидивом безбедносном окружењу савременог доба.

Обавештајно-безбедносна политика се заснива на:

- планираном деловању служби безбедности и обавештајних служби, у оквиру закона и у складу са демократским контролним механизмима;
- континуираном процесу процене безбедносног амбијента, укључујући унутрашње и спољне факторе;
- заштити државе, друштва и грађана од класичних и нових безбедносних претњи, као што су тероризам, сајбер напади, организовани криминал, екстремизам и страни утицаји.

Основи обавештајно-безбедносне политике

Обавештајно-безбедносна политика се заснива на препознавању и превенцији претњи које могу угрозити државу и друштво, а међу њима су:

- унутрашњи конфликти и насилне промене уставног поретка;
- етнички и верски екстремизам;
- тероризам и организовани криминал;
- трговина људима и миграције;
- пролиферација оружја;
- загађење животне средине и индустријски акциденти;
- сајбер криминал и безбедносне претње у дигиталном простору;
- масовни немири и социјална патологија.

Циљеви обавештајно-безбедносне политике

Основни циљеви ове политике укључују:

- стабилан међународни положај државе (спољна безбедност),
- очување реда и сигурности унутар државе (унутрашња безбедност),
- заштиту живота и имовине грађана (јавна безбедност),
- заштиту основних људских права и слобода,
- очување темељних функција друштва.

Безбедносна политика данас посебно мора укључити и сајбер безбедност, као кључну област заштите дигиталног простора, критичне инфраструктуре и комуникационих система, што постаје све значајније у условима савремених глобалних претњи и хибридних ризика.

Обавештајно-безбедносна политика у Србији

Обавештајно-безбедносна политика Републике Србије регулисана је кроз интеграцију рада различитих институција које делују на заштити националне безбедности. Савет за националну безбедност има стратешку и саветодавну улогу, док Биро за координацију служи као оперативно тело за координацију рада служби безбедности. Влада Републике Србије, као извршни орган, обезбеђује ресурсе и усмерава спровођење тих политика. Овај систем

омогућава интегрисани приступ у борби против безбедносних изазова, као и одговорност свих актера у обезбеђивању сигурности и стабилности државе.

У Републици Србији, обавештајно-безбедносна политика се реализује кроз институције попут:

- Безбедносно-информативне агенције (БИА),
- Војнобезбедносне и Војнообавештајне агенције у оквиру система одбране,
- Министарства унутрашњих послова и других надлежних органа.

Она је усмерена на очување:

- уставног поретка и територијалне целovitости Републике Србије,
- унутрашње стабилности, јавног реда и сигурности грађана,
- спољнополитичке и економске позиције државе у регионалном и глобалном контексту.

Посебан фокус обавештајно-безбедносне политике у Србији усмерен је ка:

- спречавању терористичких и субверзивних активности,
- праћењу страних утицаја и деловања обавештајних структура страних држава,
- борби против организованог криминала и корупције,
- заштити информационих система и развоју сајбер безбедности као приоритета у дигиталном добу.

Ова политика је у Србији правно и институционално утемељена, али и снажно условљена безбедносним изазовима у региону Западног Балкана, глобалним хибридным претњама и потребом за усклађивањем са европским и међународним стандардима.

Влада Републике Србије, као носилац извршне власти, игра кључну улогу у спровођењу националне безбедносне политике. Њена примарна одговорност огледа се у имплементацији стратешких докумената и акционих планова које усваја Савет за националну безбедност. Ови документи представљају основу за формулисање и спровођење мера које осигуравају стабилност, сигурност и виталне интересе државе.

Као извршни орган, Влада се активно бави правном и административном регулативом која уређује рад служби безбедности и читавог система националне безбедности. Ово укључује припрему и доношење прописа који омогућавају ефикасно функционисање институција задужених за одбрану, јавну безбедност и заштиту критичне инфраструктуре.

Поред тога, Влада Републике Србије има обавезу да обезбеди неопходне ресурсе и подршку институцијама које се баве питањима националне безбедности. То подразумева како материјалне тако и кадровске ресурсе, потребне за успешно функционисање безбедносних служби, као и развој стратегија и механизма за супротстављање модерним безбедносним претњама.

Влада, такође, врши континуирани надзор над спровођењем безбедносне политике на терену. На овај начин се осигурава да мере које су усвојене на стратешком нивоу буду доследно примењене и да доносе жељене резултате у пракси. Надзорна улога Владе доприноси координацији и синхронизацији деловања различитих институција које учествују у систему националне безбедности.

Управо кроз ове активности, Влада Републике Србије игра незаменљиву улогу у осигуравању стабилности државе и заштити њених грађана, док се истовремено прилагођава савременим изазовима и променама у глобалном безбедносном окружењу.

Министарства као сегменти извршне власти - У оквиру Владе Републике Србије, министарства представљају кључне сегменте извршне власти, задужене за креирање и спровођење ресорних и националних политика. Њихов рад омогућава ефикасно функционисање државне управе кроз дефинисање стратешких циљева, припрему законодавних оквира и реализацију конкретних програма и мера.

Министарство одбране игра кључну улогу у систему националне безбедности. Оно је задужено за планирање, развој и функционисање оружаних снага, као и за припрему и извршење одбрамбених стратегија. Министарство одбране се такође бави питањима цивилне заштите и међународне војне сарадње, укључујући учешће у мировним мисијама.

Министарство унутрашњих послова одговорно је за обезбеђивање јавног реда и мира, заштиту безбедности грађана и борбу против криминала. Ово министарство такође управља питањима граничне контроле, управљања миграцијама и реаговања у ванредним ситуацијама. Оно координише рад полиције и других безбедносних служби које делују унутар државе.

Министарство спољних послова је задужено за креирање и спровођење спољне политике Републике Србије. Оно води дипломатске односе, учествује у међународним организацијама, склапа споразуме и промовише интересе Србије у иностранству. Ово министарство игра кључну улогу у одржавању регионалне и глобалне стабилности кроз дипломатију и међународну сарадњу.

Министарство финансија управља економским ресурсима државе, укључујући израду и спровођење буџета, пореску политику и јавне финансије. Ово министарство прати економске токове, обезбеђује стабилност привреде и спроводи мере за јачање економског раста и одрживог развоја.

Поред ових ресорних министарстава, у оквиру Владе делују и друга министарства са специфичним надлежностима, попут Министарства здравља, Министарства просвете, Министарства заштите животне средине и других. Сва министарства имају јединствене функције, али и међусобно координишу своје активности како би осигурала свеобухватно и ефикасно управљање државом.

Министарства раде у складу са стратегијама и циљевима које поставља Влада, доприносећи стабилности, развоју и јачању капацитета Републике Србије. Њихова улога је незаменљива у креирању јавних политика које одговарају на актуелне друштвене и економске изазове, као и у њиховој доследној примени на терену.

Улога Савета за националну безбедност и Бироа за координацију у обавештајно-безбедносној политици Републике Србије

Обавештајно-безбедносна политика Републике Србије представља важан сегмент шире безбедносне политике и обухвата интеграцију и координацију рада различитих институција и служби које се баве националном безбедношћу. Ова политика је у Србији регулисана Законом о основама уређења служби безбедности, који прецизно дефинише структуру и надлежности органа одговорних за националну безбедност, као и начине на који се обавештајно-безбедносне службе координишу и управљају.

Основи обавештајно-безбедносне политике су утемељени не само у Закону о основама уређења служби безбедности, већ и у другим стратешким документима попут Стратегије националне безбедности и Стратегије одбране. Ови документи обезбеђују свеобухватан оквир за дефинисање циљева, процену ризика и примењивање конкретних мера које доприносе заштити виталних интереса државе и њених грађана.

Поред директног утицаја на безбедносне аспекте, обавештајно-безбедносна политика је интегрисана и у друге области јавне политике, као што су спољна политика и јавна безбедност. Њена улога у спољној политици огледа се кроз дипломатску подршку и координацију безбедносних активности у међународном контексту. У домену јавне безбедности, обавештајно-безбедносне службе помажу у превенцији криминала, заштити грађана и реаговању на кризне ситуације.

Делимично, обавештајно-безбедносна политика укључује и аспекте спровођења казнене политике кроз учешће безбедносних служби у законом дефинисаним кривичним поступцима. Ово укључује пружање релевантних информација и доказа, анализу безбедносног амбијента и подршку правосудним органима у процесима кривичног гоњења.

Кроз интеграцију различитих стратешких докумената, области јавне политике и институционалних механизма, обавештајно-безбедносна политика Републике Србије пружа систематски и свеобухватан одговор на сложене безбедносне изазове и значајно доприноси очувању стабилности и развоја државе.

Савет за националну безбедност је највише саветодавно тело у Републици Србији за питања националне безбедности. Овај Савет има кључну улогу у дефинисању и усмеравању националне безбедносне политике државе, као и у координацији рада свих релевантних институција које се баве безбедносним изазовима. Савет за националну безбедност има задатак да усмерава стратегију националне безбедности и прати све аспекте који се односе на безбедност Републике Србије.

Чланови Савета за националну безбедност:

- Председник Републике
- Председник Владе
- Министар одбране
- Министар унутрашњих послова
- Министар правде
- Начелник Генералштаба Војске Србије
- Директори безбедносних служби (БИА, ВБА и ВОА)

Учествовање у раду Савета: Чланови Савета могу позвати и старешине других државних органа и институција као и друге релевантне личности које нису формални чланови Савета (на пример, старешине органа у оквиру Министарства спољних послова, јавни и специјални тужилац, директор полиције). Председник Републике може на своју иницијативу, или на иницијативу члана Савета, позвати на седнице Савета руководиоце других државних органа и институција, као и друге људе који нису чланови Савета (као што су Републички јавни тужилац, специјални тужилац, директор полиције).

Кључне надлежности Савета:

- Усмеравање националне стратегије безбедности.
- Координација рада свих институција које се баве националном безбедношћу.
- Припрема стратешких докумената из области безбедности.
- Разматрање питања и предлога у вези са одржавањем и унапређењем безбедносне политике.
- Биро за координацију рада служби безбедности

Према Закону о основама уређења служби безбедности, Биро за координацију рада служби безбедности је посебно тело које има улогу у координацији рада свих безбедносних служби у Републици Србији. Биро је задужен за обезбеђивање ефикасне размене информација између различитих служби и планирање мера за одговор на безбедносне изазове. Он такође игра важну улогу у спровођењу одлука Савета за националну безбедност.

Чланови Бироа:

- Секретар Савета за националну безбедност
- Директор Безбедносно-информативне агенције (БИА)
- Директор Војнообавештајне агенције (ВОА)
- Директор Војне безбедносне агенције (ВБА)

Учествовање у раду Бироа:

У раду Бироа учествују и представници Министарства спољних послова, директор полиције, начелници полицијских управа, Републички јавни тужилац, директор Управе царина и руководиоци других државних органа и институција. Они учествују у раду Бироа по позиву, а њихово укључивање је неопходно за координацију и ефикасно управљање безбедносним изазовима.

Основне функције Бироа:

- Координација рада служби безбедности.
- Анализа безбедносних претњи и креирање одговора на њих.
- Припрема информација за Савет за националну безбедност.
- Спровођење политике безбедности на оперативном нивоу.

Ова два тела, Савет за националну безбедност и Биро за координацију рада служби безбедности, играју кључну улогу у обавештајно-безбедносној политици Републике Србије, обезбеђујући ефикасну комуникацију и координацију између различитих институција, као и брзо и ефикасно одговарање на безбедносне изазове са којима се држава сусреће.

Улога Канцеларије Савета за националну безбедност и заштиту тајних података у раду Савета и Бироа за координацију у обавештајно-безбедносној политици Републике Србије

Канцеларија Савета за националну безбедност и заштиту тајних података игра кључну улогу у координацији и оперативној подршци Савету за националну безбедност. Као административно и оперативно тело, Канцеларија има задатак да обезбеди континуитет рада Савета, пружа стручну помоћ и организује радне групе које се баве актуелним безбедносним

питањима. Канцеларија такође има задатак да припрема све потребне материјале, извештаје и анализе које Савет користи у доношењу стратешких одлука.

Основне функције Канцеларије Савета за националну безбедност:

- Подршка у раду Савета за националну безбедност: Канцеларија припрема радне састанке, документе, и записнике са седница, као и све стручне анализе и процене које су потребне Савету за доношење одлука.
- Координација између институција: Канцеларија обезбеђује комуникацију и координацију између различитих чланова Савета за националну безбедност, као и између њихових органа и служби.
- Организација и припрема стратешких докумената: Канцеларија је задужена за припрему стратешких и оперативних докумената који се односе на безбедност Републике Србије, укључујући безбедносне планове и извештаје.
- Припрема информација за Биро за координацију служби безбедности: Канцеларија такође игра важну улогу у припреми података и анализа који се користе од стране Бироа за координацију рада служби безбедности. Она обезбеђује да све релевантне информације буду доступне свим укљученим странама, у складу са прописима о заштити тајних података.
- Канцеларија као веза између Савета и оперативних тела: функционише као канал за брзу и ефикасну размену информација између Савета, Бироа за координацију, и других безбедносних служби. Канцеларија се такође бави координацијом оперативних активности које се односе на безбедност, као што су аналитички извештаји и припрема предлога за оперативне кораке који треба да буду усвојени од стране Савета и Бироа.

Улога Канцеларије Савета за националну безбедност и заштита тајних података у контексту Закона о тајности података

У извршној власти Републике Србије, Канцеларија савета има статус стручне службе Владе директно везане за председника Владе. Канцеларија Савета има веома важну улогу у контексту Закона о тајности података, који дефинише правила за одређивање, означавање, обраду и заштиту тајних података. Канцеларија не само да учествује у координисању рада Савета и Бироа, већ и осигурава да све активности и одлуке Савета и Бироа буду у складу са правилима заштите тајних података, као и са стандардима који произилазе из овог Закона.

Основне функције Канцеларије Савета у области заштите тајних података:

Примена Закона о тајности података: Канцеларија је одговорна за осигурање да све класификоване информације које се разматрају или користе у раду Савета буду обрађене у складу са прописима о заштити тајних података. То укључује примену прописаних степена тајности података и процедура за њихову заштиту.

- Координација са надлежним органима за заштиту тајних података: Канцеларија као орган надлежан за стручни надзор примене мера заштите тајних података, сарађује са Министарством правде, које је надлежна за инспекцијски надзор над спровођењем Закона о тајности података.

- Управљање и координација поступком издавања безбедносних сертификата за физичка и правна лица, као и примене мера заштите тајних података: Канцеларија координира овај процес у складу са законом, одређујући који подаци треба да буду обележени као интерно, поверљиво, строго поверљиво или државна тајна. Овај процес је важан за обезбеђивање да сви тајни подаци буду заштићени на одговарајући начин.
- Обучавање и подизање свести о заштити тајних података: Канцеларија организује обуку и информисање органа јавне власти и правних лица о прописима који регулишу заштиту тајних података, као и о најбољим праксама за њихову заштиту.
- Заштита тајних података у процесу размене информација: Канцеларија обезбеђује да размена тајних информација између различитих државних органа, буде у складу са прописима о заштити тајних података. Ово подразумева сигурне канале комуникације и адекватну евиденцију о обради података.

Јавне политике и штићени подаци у Републици Србији

У савременом друштву које све више зависи од података, ефикасне и легитимне јавне политике не могу бити остварене без одговорног управљања информацијама. Тиме се подразумева не само заштита података, већ и њихова доступност и транспарентност, који су основ за пуну функционалност сваке јавне политике. Република Србија је кроз свој правни и институционални оквир дефинисала више категорија података који подлежу заштити, али је изузетно важно разумети њихову међусобну разлику како би јавне политике биле усклађене са важећим прописима и добром управом.

Јавне политике у Републици Србији, као и у већини других земаља, укључују низ мера и принципа који се односе на доступност и заштиту информација. Са развојем дигиталних технологија и брзим напредовањем на плану електронског управљања, питање заштите података постаје све важније, нарочито када су у питању подаци који су од значаја за безбедност државе или приватност појединца. У овом контексту, важност управљања штићеним подацима и њихова корелација са отвореним подацима добија посебан значај, јер јавне политике морају успоставити равнотежу између транспарентности и заштите од злоупотреба, као и осигурати да сви подаци, било да су јавни, штићени или тајни, буду адекватно управљани.

Тема која се бави односом јавних политика и отворених или јавних података, као и њихове корелације са штићеним и тајним подацима, представља веома важан аспект у савременим друштвима. У овом контексту, јавне политике које се односе на транспарентност, отвореност података, и доступност информација јавности, у великој мери зависе од начина на који се управља са подацима који су, са друге стране, заштићени или класификовани као тајни. Овде треба истакнути важност одговорног управљања подацима, како би се обезбедила сигурност, али и право грађана на информације.

Отворени подаци се у многим демократским друштвима сматрају основом за транспарентност и развој јавног сектора. Они укључују податке који су доступни свим грађанима без посебних ограничења, чиме се омогућава већа ангажованост јавности у процесима доношења одлука и бољу информисаност. Међутим, када се ради о подацима који су класификовани као штићени као и тајни, постоји осетљиви баланс који треба одржати између потребе за транспарентношћу и обавезом заштите националне безбедности или приватности појединца.

Штићени подаци – општи оквир

Штићени подаци представљају широк правни и организациони појам који обухвата све информације које нису јавно доступне и чија је заштита неопходна ради очувања безбедности, приватности, пословне конкурентности или других важних интереса. Ови подаци могу бити заштићени различитим правним механизмима, укључујући законе, подзаконске акте, интерне прописе, уговоре или етичке кодексе. У зависности од правног оквира који примењује Република Србија, штићени подаци могу бити класификовани у различите категорије, при чему свака има своје специфичности у погледу обраде, складиштења и приступа. Овај систем класификације помаже у управљању информацијама на начин који балансира транспарентност и потребу за заштитом осетљивих података.

Корелација између јавних, штићених и тајних података игра кључну улогу у савременом дигиталном окружењу, где подаци представљају један од највреднијих ресурса. Класификација података према нивоу осетљивости и ризика који њихово обелодањивање може донети омогућава стварање безбедносних механизма који штите како националне интересе, тако и приватност грађана. Информације квалификоване као „штићене“ или „тајне“ најчешће се односе на националну безбедност, економску стабилност или личне податке појединаца, због чега је њихова обрада строго регулисана прописима и безбедносним процедурама. Насупрот томе, јавни подаци су намењени слободној употреби, али њихова доступност може бити ограничена у складу са степеном осетљивости. Док су неке информације попут статистичких података широко доступне, подаци који се тичу безбедности грађана, јавне инфраструктуре или критичних сектора могу захтевати додатне мере заштите.

Неопходно је успоставити јасан и функционалан оквир за управљање подацима, који ће истовремено обезбедити приступ јавним информацијама од значаја за грађане, али и гарантовати заштиту штићених и тајних података. У том процесу, регулаторна тела играју кључну улогу у утврђивању критеријума класификације података, док јавне институције сnose одговорност за њихову правилну обраду и чување. Поред тога, неопходно је развијати свест грађана о значају безбедности података, како би се осигурала одговорна употреба информација и спречиле потенцијалне злоупотребе. Успостављање усклађеног система за управљање подацима доприноси бољој транспарентности, ефикаснијој заштити поверљивих информација и већем поверењу јавности у институције које рукују подацима.

Дигитални подаци и сајбер безбедност постају централна тема у ери технолошког напретка, где управљање подацима постаје све сложеније и захтева свеобухватан приступ. Дигитални подаци, који обухватају све информације сачуване у електронском формату, чине суштински део јавних политика, отворених информација, али и система заштите поверљивих и тајних података. С обзиром на све већу зависност од дигиталних технологија, безбедност ових података постаје један од најважнијих изазова. Сајбер безбедност, као критичан аспект информационе сигурности, подразумева примену мера које обезбеђују сигурност дигиталних система и спречавају злоупотребе, компромитовање података и кибер-нападе који могу угрозити приватност, институције и националну безбедност.

Јавни подаци у дигиталном формату морају бити адекватно заштићени, како би се очувала њихова тачност, интегритет и безбедност. Истовремено, потребно је осигурати њихову доступност за потребе аналитике, истраживања и образовања, чиме се унапређује развој дигиталних политика и иновација. Ово захтева системску подршку институција које управљају подацима, као и стручњака за сајбер безбедност који примењују напредне технике

шифровања, приступне контроле и аутентификације. Поред тога, одговорно коришћење јавних података од стране грађана и организација доприноси бољем разумевању ризика и очувању безбедности дигиталног окружења.

Штићени и тајни подаци захтевају посебан режим заштите, који укључује примену најсавременијих мера енкрипције, ограничења у приступу и стриктне системе провере аутентичности корисника. Ови подаци се користе у државним, војним, комерцијалним и приватним секторима који рукују осетљивим информацијама, па су механизми њихове заштите од кључне важности. Додатно, безбедносни протоколи за размену и складиштење података морају бити строго дефинисани, како би се спречиле неовлашћене манипулације или злоупотребе поверљивих информација.

Кључни изазов у дигиталном добу је стварање равнотеже између транспарентности јавних података и потребе за заштитом штићених и тајних информација. Док отворени подаци представљају основу за демократско друштво, научна истраживања и иновације, истовремено је неопходно осигурати безбедност података који имају значај за националну безбедност или приватност појединаца. Политике које регулишу овај баланс морају бити јасне, транспарентне и усаглашене са најновијим стандардима у области сајбер безбедности. Само кроз сталну модернизацију и унапређење система управљања подацима могуће је изградити отпорност на нове претње које се јављају са развојем технологије.

Вештачка интелигенција (АИ) и управљање подацима: нове могућности и изазови
Са напретком технологије и дигитализацијом свих аспеката друштва, вештачка интелигенција (АИ) постаје кључни фактор у управљању подацима. АИ се користи за анализу великих количина информација, аутоматизацију процеса обраде и предикцију трендова, што значајно утиче на управљање како јавним, тако и штићеним подацима. Њена улога је двострука – с једне стране, омогућава лакшу доступност јавних података и њихову корисну анализу, а с друге стране, доприноси заштити поверљивих информација кроз напредне алгоритме и системе безбедности.

Јавни подаци и АИ: отвореност и доступност

Јавни подаци, који укључују статистику, социоекономске индикаторе, демографске информације и научна истраживања, постају све више доступни захваљујући АИ технологијама. Алгоритми машинског учења омогућавају бољу организацију, анализу и визуелизацију информација, чиме се подаци користе ефикасније за доношење јавних политика, економски развој и научна истраживања. Међутим, иако АИ олакшава приступ подацима, неопходно је осигурати да алгоритми функционишу у складу са принципима транспарентности и етичке употребе информација.

Штићени подаци и АИ: изазови безбедности

Обрада штићених и тајних података уз помоћ АИ система захтева високе стандарде безбедности. Ови подаци могу укључивати личне информације, корпоративне стратегије, државне поверљиве документе или безбедносне информације. АИ може побољшати заштиту таквих података кроз аутоматске системе детекције претњи, енкрипцију и управљање приступом. Ипак, постоје ризици – ако се алгоритми не надгледају правилно или ако нема јасних регулација, могуће је да се осетљиви подаци злоупотребе или да дође до неовлашћеног приступа.

Изазов „Биг дата“: управљање огромним количинама информација

Концепт „Биг дата“ односи се на огромне количине дигиталних података које се генеришу свакодневно, било кроз индустрију, јавне системе или појединачне кориснике. АИ има способност да ефикасно анализира ове податке, идентификује обрасце и доноси предиктивне закључке. Међутим, проблем настаје када се подаци не управљају правилно – неконтролисано прикупљање информација може довести до нарушавања приватности, проблема са безбедношћу и непредвиђених ризика за кориснике. Такође, велика количина података може изазвати потешкоће у њиховом складиштењу и обради, што захтева све напредније инфраструктуре за управљање.

Баланс између иновација и регулације

Да би се обезбедило ефикасно управљање јавним и штићеним подацима, као и феноменом „Биг дата“, потребно је пронаћи баланс између иновација и регулације. Напредак вештачке интелигенције доноси велике користи, али је истовремено неопходно развијати механизме за надзор, транспарентност и заштиту података. Само кроз усклађену сарадњу између технолошких компанија, регулаторних тела и јавности могуће је изградити одржив и безбедан дигитални екосистем.

Тајни подаци – подаци од интереса за Републику Србију

Тајни подаци представљају подкатегорију штићених података која има значај за националну безбедност, одбрану, спољну политику или друге виталне интересе Републике Србије. Према Закону о тајности података („Сл. гласник РС“, бр. 104/2009), тајни подаци подлежу строгој класификацији која је заснована на четири нивоа тајности:

- **Државна тајна** – подаци чије откривање може нанети неотклоњиву штету националним интересима.
- **Строго поверљиво** – подаци чије откривање може изазвати тешку штету националним интересима.
- **Поверљиво** – подаци чије откривање може изазвати штету националним интересима.
- **Интерно** – подаци чије откривање може нанети штету за рад органа јавне власти који их је одредио.

Ови подаци се морају обрађивати у складу са стриктним мерама физичке, техничке и организационе заштите. Неовлашћено руковање тајним подацима подразумева кривичну одговорност.

Класификовани подаци – погрешна употреба у пракси

Класификација и разврставање података у Републици Србији представља темељни предуслов за правилно поступање са информацијама, обезбеђење њихове заштите, као и унапређење транспарентности и правне сигурности у раду јавних органа. У пракси се често среће неоснована употреба термина „*класификовани подаци*“ као општег назива за *тајне податке*, што је у супротности са нормативним оквиром Републике Србије. За разлику од англосаксонског система, у ком се користи појам *classification* у смислу тајности, у српском правном систему примењује се институционализовани поступак *одређивања степена тајности података*, како је прописано Законом о тајности података („Сл. гласник РС“, бр. 104/2009).

У складу с тим, појам „класификовани подаци“ није правно валидан у српском контексту и његова употреба у службеним, стручним и нормативним документима није препоручљива. Уместо тога, потребно је користити термин „*тајни подаци*“, са јасно одређеним степеном тајности (*интерно, поверљиво, строго поверљиво и државна тајна*), у складу са прописаним критеријумима.

Прецизно дефинисање и коришћење исправних термина у правном систему је важно не само за усклађеност са постојећим прописима, већ и за избегавање погрешних тумачења у институционалним и међународним оквирима. Стварање унифицираног приступа класификацији података и њиховој заштити доприноси транспарентности, ефикасности и безбедности у поступању са информацијама од националног значаја.

Штићени подаци у Србији обухватају различите категорије информација које су законом, подзаконским актима или интерним прописима заштићене од неовлашћеног приступа, обраде, откривања или злоупотребе. Њихова заштита је кључна за очување безбедности, приватности и јавних интереса. Ове податке можемо поделити у две главне групе:

- Подаци који су законом заштићени
- Њихово откривање или злоупотреба носе кривичну или прекршајну одговорност.

Административни и осетљиви подаци

Иако нису формално означени као тајни, њихова обрада и приступ подлежу посебним правилима.

Правилно поступање са подацима у Републици Србији подразумева иницијалну радњу – њихово разврставање у одговарајуће категорије заштићених података или класификацију, у складу са важећим законима. Основне категорије података у правном систему Републике Србије обухватају:

- **Тајне податке**, који се штите на основу степена тајности одређеног у складу са законом;
- **Личне податке**, чија је обрада регулисана Законом о заштити података о личности;
- **Пословне тајне**, које се штите ради очувања тржишне позиције правних и физичких лица;
- **Професионалне тајне**, обухватају информације које стручна лица не смеју откривати без изричитог одобрења, као што су нотарске, свештеничке, адвокатске, новинарске и лекарске тајне и слично;
- **Јавне податке**, који су доступни свим грађанима у складу са правом на приступ информацијама од јавног значаја;
- **Архивску грађу**, која се чува, обрађује и користи у складу са Законом о архивској грађи и архивској делатности.

Поред набројаних категорија постоје и друге категорије штићених података. Оваква систематизација омогућава ефикасно управљање подацима, јасну расподелу одговорности и примену одговарајућих мера заштите у складу са специфичностима сваке категорије података.

Остале категорије штићених података

Поред класификованих и тајних података, штићени подаци обухватају и друге категорије које су заштићене специјалним правним режимима:

- Банкарска и фискална тајна – регулисана Законом о банкама и пореским прописима.
- Здравствени подаци – регулисани Законом о правима пацијената.
- Подаци у јавним набавкама – када је предвиђена посебна заштита и поверљивост, коју не треба бркати са степеном тајности поверљиво по Закону о тајноти података.
- Подаци о малолетницима – регулисани кривичним и породичним законодавством.
- Архивска грађа – посебно регулисана роковима приступа и дигитализацијом.
- Административни и осетљиви подаци – као што су подаци о безбедности инфраструктуре, полицијске процене, еколошки подаци и слично.

Категорије штићених података

I. Подаци који су законом заштићени:

Тајни подаци

- ❖ Ознаке степена тајности: *Државна тајна, Строго поверљиво, Поверљиво, Интерно.*
- ❖ Уређени Законом о тајности података.

Подаци о личности

- ❖ Регулисани Законом о заштити података о личности.
- ❖ Укључују идентификационе податке и информације о приватности грађана.

Пословна тајна

- ❖ Дефинисана Законом о привредним друштвима.
- ❖ Обухвата информације од тржишне вредности.

Банкарска и фискална тајна

- ❖ Регулисана Законом о банкама и Законом о порезу на додату вредност.
- ❖ Укључује податке о финансијским трансакцијама и обавезама.

Здравствени подаци

- ❖ Заштићени Законом о здравственој заштити и Законом о правима пацијената.
- ❖ Укључују медицинску документацију.

Судски, тужилачки и прекршајни подаци

- ❖ Регулисани законима о судским поступцима.
- ❖ Обухватају истраге, доказе, сведочења и пресуде.

Поверљиви подаци у јавним набавкама

- ❖ Регулисани Законом о јавним набавкама.
- ❖ Укључују осетљиве информације о понуђачима и процедурама.

Професионалне тајне

- ❖ Адвокатске, лекарске, новинарске и друге професионалне поверљиве информације.

Подаци о малолетницима

- ❖ Регулисани Кривичним закоником и Законом о заштити права детета.
- ❖ Укључују личне податке и судске поступке.

Пореска тајна

- ❖ Регулисана Законом о пореском поступку и администрацији.

II. Административни и осетљиви подаци:

Отворени подаци

- ❖ Јавно доступни подаци објављени од стране државних органа.

Подаци за сарадњу са ЕУ

- ❖ Регулисани споразумима са Европском унијом.

Подаци о безбедности инфраструктуре

- ❖ Витална инфраструктура, енергетика и саобраћај.

Оперативни подаци полиције и јавне безбедности

- ❖ Аналитички извештаји и процене.

Еколошки подаци

- ❖ Податке о загађењу и заштити животне средине.

III. Архивска грађа:

Архивска грађа је део културног наслеђа и обухвата:

- ❖ **Јавну архивску грађу доступну након истека рокова** (70 година од настанка, или 100 година од рођења лица).
- ❖ **Затворену грађу са ограниченим приступом** (нпр. материјали служби безбедности, поверљиви документи).

Напомене:

- Обухвата историјску, војну и културну документацију.
- Дигитализација омогућава приступ осетљивим материјалима без угрожавања оригинала.
- Надлежност: Државни архив Србије и Војни архив.

Јавне политике и управљање штићеним подацима

Управљање штићеним подацима у оквиру јавних политика представља један од најважнијих аспеката одговорног и транспарентног управљања информацијама. Правилна примена система заштите штићених података није само законска обавеза, већ и предуслов за очување поверљивости, безбедности и интегритета институционалних и личних информација. У савременом окружењу где се информације све више дигитализују, и где је ризик од њихове злоупотребе већи него икада, посебно је важно да јавне политике које се базирају на обради података буду усклађене са нормативним оквиром који регулише заштиту података. Ово је неопходно како би се осигурало да су процеси обраде, приступа и чувања података у складу са највишим безбедносним стандардима. Јавне политике морају се разматрати не само кроз законске оквире, већ и кроз етичке стандарде који обезбеђују праведност, транспарентност и

заштиту основних људских права, као што су право на приватност и право на приступ информацијама.

Кључни елементи управљања штићеним подацима укључују:

- **Идентификацију правног режима података**, односно утврђивање категорије информација које подлежу посебној заштити. Ово може обухватати личне податке, пословне информације, поверљиве државне документе или тајне податке релевантне за националну безбедност. Важно је да свака категорија података буде јасно дефинисана, јер тачно идентификовање врсте података који се штите омогућава прецизно одређивање мера заштите, као и одговорности које произилазе из њиховог управљања.
- **Одређивање степена заштите података** врши се у складу са законским критеријумима и прописима који дефинишу ниво поверљивости и доступности информација. У оквиру заштите тајних података, означавање степена тајности се врши према прописима дефинисаним Законом о тајности података (Сл. гласник РС, бр. 72/2009), а подаци могу бити категорисани као интерно, поверљиво, строго поверљиво или државна тајна, у зависности од њихове осетљивости и могућих штетних последица по интересе републике Србије услед неовлашћеног откривања. Ниво заштите се утврђује на основу процене ризика који се односе на настанак штете или угрожавање безбедности, интереса или угледа правних и физичких лица, као и националне безбедности. Штићени подаци, иако нису класификовани као тајни, подлежу посебним правним режимима заштите. Ова категорија укључује личне податке, у складу са Законом о заштити података о личности (Сл. гласник РС, бр. 87/2018), пословне тајне, финансијске и здравствене податке, као и административне информације намењене искључиво службеној употреби. За њихову заштиту примењују се различите мере, укључујући ограничења приступа, енкрипцију, као и примену правних механизма који обезбеђују контролисану размену података. Законски прописи утврђују како и под којим условима се могу размењивати такви подаци, с посебним нагласком на заштиту права на приватност и поверљивост података. Процес одређивања нивоа заштите мора бити заснован на јасним правним и безбедносним критеријумима, уз примену система процене ризика, који осигурава да се подаци правилно категоризују и да се примењују адекватне мере заштите. Поред националних прописа, потребно је узети у обзир и међународне стандарде за заштиту података, јер дигитализација и глобализација подразумевају све већи степен повезаности различитих регулаторних система. Србија је такође обавезана да се усагласи са Општом уредбом о заштити података (GDPR) Европске уније, која представља оквир заштите података на међународном нивоу, како би се осигурао висок ниво заштите права лица чији се подаци обрађују.
- **Примену мера заштите**, које укључују техничке и организационе мере попут енкрипције, контроле приступа, система аутентификације и процедура заштите током размене информација. Ове мере морају бити у складу са законским обавезама и најбољим праксама у области информационе безбедности. Поред тога, континуирано тестирање и обнављање безбедносних мера је од кључне важности, јер се технологије и методе напада стално развијају. Такође, неопходно је осигурати да постоје добре процедуре за управљање инцидентима који се односе на заштиту података, као и механизми који омогућавају брзу и ефикасну реакцију у случају кршења безбедности.
- **Спречавање злоупотребе тајности**, при чему је посебно важно да се системи за класификацију података не користе за прикривање корупције, неправилности у трошењу јавних средстава или онемогућавање јавне контроле. Неправилна примена

концепта тајности података може угрозити транспарентност и поверење грађана у јавне институције, због чега је неопходна строга примена механизма надзора и одговорног управљања подацима. У овом контексту, велика одговорност лежи у рукама надлежних органа који требају бити не само технички обучени, већ и етички посвећени очувању јавног интереса и осигурању да тајни подаци не буду злоупотребљени ради личних или политичких интереса.

- **Транспарентност и етичка примена јавних политика у области управљања подацима** – Док је неопходна заштита осетљивих информација, истовремено је важно обезбедити јасан и праведан оквир који омогућава јавну контролу и приступ релевантним информацијама. Ефикасно управљање штићеним подацима мора узети у обзир принципе транспарентности, етичности и законске усаглашености, како би се избалансирао потреба за безбедношћу са правом јавности да буде информисана о важним аспектима рада јавних институција. Тиме се обезбеђује да јавност не само да има права на приступ информацијама, већ и да се оне обрађују у складу са највишим правним и етичким стандардима. Принцип транспарентности треба да буде интегрисан у све фазе обраде података, од њихове класификације до одређивања мера заштите и размене информација.

Такође, важно је нагласити да заштита података није само правни оквир, већ и питање етичке одговорности јавних органа. Управљање подацима мора бити вођено поштовањем људских права и одговорности према грађанима, како би се избегао било какав облик злоупотребе или манипулације подацима који могу нарушити поверење грађана у јавне институције.

Препоруке за јавну управу

Како би се осигурало правилно управљање подацима, препоручује се:

- Обезбедити стручну обуку запослених у јавним органима о разликама између штићених, тајних и других осетљивих података.
- Усвојити интерне акте који прецизирају поступање са различитим категоријама података.
- Ојачати надзорне механизме у вези са злоупотребом ознака тајности.
- Спровести ревизију праксе означавања документације као поверљиве, нарочито у јавним набавкама.
- Подржати дигитализацију и безбедно управљање подацима кроз е-управу.

Управљање штићеним и тајним подацима није само правно-техничко питање, већ је кључно за добру управу, борбу против злоупотреба и изградњу поверења грађана у институције. Разграничење између јавних, отворених, штићених и тајних података омогућава ефикасно доношење одлука и одржавање националних интереса, али и заштиту права грађана на приватност и безбедност. Јасна класификација података и поштовање правних оквира је предуслов за успешну и одговорну јавну управу.

У контексту свеобухватне дигитализације и све већег ослањања на податке у процесу креирања и имплементације јавних политика, од изузетног је значаја да се направи јасна разлика између отворених, штићених и тајних података. Посебну пажњу потребно је посветити прецизном коришћењу појмова у складу са важећим прописима Републике Србије. У пракси се, међутим, све чешће појављује погрешна употреба појма „класификовани подаци“ (енг. *classified data*), који није у складу са домаћим правним системом. Тај појам се неретко

користи као општи израз за тајне податке, без поштовања прописаног поступка одређивања степена тајности. У правном поретку Републике Србије не постоји категорија „класификовани подаци“, већ се подаци који се штите због интереса државе означавају једним од четири нивоа тајности, у складу са Законом о тајности података. Некритичко преузимање страних термина и модела, без нормативног упоришта, доводи до правне несигурности, неуједначене праксе и потенцијалног угрожавања основних права и интереса државе. Управо зато је неопходно да институције и појединци који поступају са подацима од јавног значаја доследно примењују домаће прописе и развијају капацитете за правилно управљање подацима у дигиталном добу.

Тајни подаци у функцији безбедносне политике као облика јавне политике

Принцип транспарентности представља темељ демократског друштва, омогућавајући грађанима да имају увид у активности и одлуке власти. Он је кључан за изградњу поверења у институције и јачање њихове одговорности према јавности. У савременим демократским системима, транспарентност није само законска обавеза већ и морална дужност која омогућава учешће грађана у процесима доношења одлука, као и критичко испитивање активности државних органа.

Упркос значају транспарентности, она не може бити апсолутна. У одређеним ситуацијама, откривање осетљивих информација може угрозити националну безбедност, стабилност међународних односа или саму безбедност друштва. Тајност информација постаје неопходна када њихово обелодањивање може довести до значајних штетних последица по виталне интересе државе. Ово поставља сложен задатак пред државне органе да балансирају између права јавности на информисаност и потребе за заштитом критичних података.

Неправилно означавање података као јавних може узроковати озбиљне ризике, укључујући угрожавање националне безбедности или нарушавање међународних односа. С друге стране, прекомерно означавање података као тајних може довести до слабљења јавног надзора, чиме се повећава ризик од корупције и злоупотребе власти. Овај сукоб транспарентности и тајности наглашава потребу за пажљиво утврђеним процедурама које регулишу поступање са информацијама.

Зато је од кључне важности успостављање јасних, законских и транспарентних процедура које омогућавају правилно одређивање степена тајности података. Ове процедуре морају дефинисати под којим условима се подаци могу обележити као тајни и када је њихово обелодањивање оправдано. Само кроз овако регулисан систем могу се постићи истовремено транспарентност власти и заштита интереса државе.

Континуирано унапређивање ових процедура је од суштинске важности за одржавање поверења јавности у рад државних институција. Правилно утврђен баланс између транспарентности и тајности осигурава демократско функционисање друштва и одрживост система националне безбедности.

Тајни подаци играју кључну улогу у функцији безбедносне политике као облика јавне политике. Безбедносна политика обухвата стратегије, мере и механизме којима држава штити основне вредности као што су територијални интегритет, уставни поредак, живот и здравље грађана, као и економска и енергетска стабилност. У овом контексту, тајни подаци служе као основно средство за планирање, координацију и спровођење безбедносних мера. Њихова употреба омогућава државним органима да реагују правовремено и ефикасно, уз истовремено очување националних интереса.

Заштита тајних података није искључиво техничко питање, већ има дубоку политичку и правну димензију. Успостављање легитимних критеријума за означавање степена тајности података, њихова доследна примена и институционална контрола играју централну улогу у обезбеђивању транспарентности јавне управе и одговорности у систему националне безбедности. Пажљиво управљање овим аспектом омогућава држави да одржи равнотежу између потребе за тајношћу и демократских принципа јавног увида.

Поред нормативне утемељености, поступање са тајним подацима има снажну политичку димензију, нарочито када се односи на доношење одлука од јавног значаја. Тајни подаци често представљају основу за формулисање стратегија и мера које директно утичу на стабилност и сигурност државе. Зато је праведна и законита примена правила о тајности података од пресудног значаја за очување легитимности безбедносне политике и јачање поверења грађана у институције.

Правилно управљање тајним подацима омогућава ефикасну реализацију безбедносних мера и механизма, осигуравајући да јавне политике остану усмерене ка заштити основних вредности и виталних интереса државе.

Према Уредби о критеријумима за означавање степена тајности тајних података, тајни подаци могу се означити једним од следећих степена тајности:

1. ДРЖАВНА ТАЈНА – ако би њиховим откривањем настала најтежа штета по интересе Републике Србије, као што су:

- непосредна угроженост територијалног интегритета;
- трајно нарушавање уставног поретка;
- губитак великог броја живота;
- тешка штета по дугорочне економске интересе;
- обустава рада безбедносних служби;
- прекид међународне сарадње;
- тешко угрожавање способности одбране државе.

2. СТРОГО ПОВЕРЉИВО – ако би његовим откривањем, злоупотребом или уништавањем настала тешка штета која за последицу може имати:

- изузетно озбиљно угрожавање територијалног интегритета и суверености;
- озбиљно угрожавање демократских принципа;
- губитак живота у већем броју или претњу по здравље већег броја лица;
- тешку штету по средњорочне економске интересе;
- озбиљно угрожавање рада безбедносних и обавештајних служби;
- угрожавање кривичног гоњења и правосуђа;
- озбиљно угрожавање способности Војске и снага одбране;
- погоршање међународног положаја Србије.

3. ПОВЕРЉИВО – ако би његовим откривањем настала штета по интересе Републике Србије, која може довести до:

- угрожавања територијалног интегритета и суверености;
- угрожавања уставног поретка;
- претње по живот или здравље људи;

- штете по економске интересе;
- нарушавања рада служби безбедности;
- угрожавања кривичног гоњења и судских поступака;
- слабљења способности војске;
- поремећаја у међународној сарадњи;
- погоршања међународних односа;
- угрожавања јединства Владе;
- угрожавања енергетске безбедности;
- губитка културног наслеђа.

4. ИНТЕРНО – ако би његовим откривањем настала штета по рад органа јавне власти, као што су:

- смањење оперативних способности;
- угрожавање међународне сарадње органа јавне власти.

Одређивање степена тајности тајних података мора се темељити на конкретној процени штете која би могла настати услед неовлашћеног откривања, злоупотребе или уништавања информација. Прецизна процена ризика омогућава примену адекватних мера заштите, чиме се обезбеђује равнотежа између потребе за тајношћу и захтева за транспарентношћу у демократском друштву. Управо овај баланс представља суштински услов за очување сигурности и поверења грађана у институције.

Безбедносна политика као облик јавне политике захтева јасан правни и институционални оквир који регулише поступање са тајним подацима. Неадекватно означавање информација, било да је прекомерно или недовољно, може довести до озбиљних последица – од угрожавања интереса државе до кршења права грађана. Зато је у оквиру националне безбедности неопходно континуирано развијати и унапређивати културу заштите тајних података, засновану на принципима законитости, професионализма и јавног интереса.

Тајни подаци добијају значајну улогу не само у оперативним активностима државних органа, већ и као средство јавне политике. Ефикасно управљање и заштита ових података доприносе изградњи поверења у институције, јачању транспарентности и очувању стабилности у друштву. На овај начин, информације које су означене као тајне постају кључни ресурс за стратешко планирање и реализовање мера од виталног значаја.

Успостављање делотворног и транспарентног система заштите тајних података, који је истовремено отпоран на злоупотребе, представља темељ модерне безбедносне политике. Само кроз такав приступ могу се постићи национални безбедносни циљеви, уз истовремено очување основних права и слобода грађана у демократском друштву. Овај модел представља идеал коме свака држава тежи у условима савременог безбедносног окружења.

Закон о слободном приступу информацијама од јавног значаја представља основни правни инструмент који омогућава грађанима, медијима и другим заинтересованим странама да приступе информацијама које се односе на рад органа јавне власти. Ово право је један од темеља демократског друштва, јер јавности пружа могућност да врши надзор над радом власти, спречава злоупотребу моћи и осигурава транспарентност процеса доношења одлука. На овај начин се јача одговорност јавних институција и поверење грађана у систем.

Ипак, слободан приступ информацијама није апсолутан и може бити ограничен у случајевима када се ради о класификованим подацима који носе ознаку тајности. Ове информације, у складу са законом, не могу бити доступне јавности јер њихово обелодањивање може довести до озбиљних штетних последица по националну безбедност, економске интересе државе или јавну безбедност. Класификовани подаци се најчешће односе на области као што су безбедност, здравство, национална одбрана, правосуђе и други критични аспекти функционисања државе.

Заштита података који носе ознаку тајности је од суштинског значаја за очување виталних интереса државе и сигурности грађана. Закони и прописи који регулишу овај процес морају бити усклађени са међународним стандардима који осигуравају да се класификовани подаци штите на начин који је у складу са правима грађана и потребама државе. Истовремено, неопходно је обезбедити да се ограничења права на приступ информацијама користе у складу са принципима пропорционалности и законитости, како би се избегле злоупотребе и произвољност у примени.

Тајни подаци, јавне политике и безбедносна политика представљају неизоставне стубове националне безбедности Републике Србије. Њихова међусобна повезаност, као и интеграција кроз институционални оквир, чине основе за очување виталних интереса државе, одржавање стабилности и јачање поверења грађана у систем. Управо ова интеграција омогућава стратешко деловање које доприноси отпорности друштва на све сложеније безбедносне изазове.

Јавне политике су инструмент кроз који држава формулише одговоре на друштвене изазове и кризе. Обухватају области као што су здравство, образовање, енергетика и безбедност, а својим функционисањем директно утичу на квалитет живота грађана и стабилност државе. У контексту безбедносне политике, тајни подаци имају посебан значај јер омогућавају планирање и спровођење мера које штите територијални интегритет, уставни поредак, виталне ресурсе и критичну инфраструктуру.

Савет за националну безбедност и Биро за координацију рада служби безбедности играју централну улогу у управљању и координацији система националне безбедности. Њихова улога у интеграцији, анализи и заштити тајних података незаменљива је за усклађивање одлука и ефикасно реаговање на претње. Канцеларија Савета за националну безбедност и заштиту тајних података доприноси оперативној примени Закона о тајности података, чиме осигурава очување информација од виталног значаја и успостављање одговарајућих процедура у руковању класификованим подацима.

Значај тајних података огледа се у њиховој правној и политичкој димензији. Њихова адекватна заштита захтева не само доследну примену процедура, већ и развој културе одговорности и транспарентности у институцијама. Баланс између потребе за тајношћу и захтева за јавним увидом кључан је за очување демократских вредности и јачање поверења грађана у институције.

Безбедносна политика као јавна политика игра кључну улогу у савременом добу, нарочито у условима глобалних и регионалних хибридних претњи. Интеграција сајбер безбедности, заштите животне средине и других савремених аспеката омогућава држави да се прилагоди новим изазовима и унапреди своју стратегију националне безбедности. Тајни подаци служе као основа за ефикасно планирање и реализацију ових мера, чиме доприносе стабилности и даљем развоју јавних политика.

Закључно, успостављање ефикасног система заштите тајних података и координација јавних и безбедносних политика представљају темељ националне безбедности. Одговорност, професионализам и законитост у поступању са тајним подацима од пресудног су значаја за стабилност државе, заштиту права грађана и очување демократског поретка. Само добро усклађен, свеобухватан и транспарентан приступ може осигурати дугорочни развој и безбедност Републике Србије у изазовима савременог доба.

Одређивање степена тајности података

Процедура за означавање и одређивање степена тајности података представља кључни корак у заштити осетљивих информација, докумената и података, као и очувању интереса Републике Србије. Ова процедура има за циљ да обезбеди безбедност података, уз транспарентност и одговорност органа јавне власти. Као тајни податак може се 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. Поступак означавања и одређивања степена тајности у органима јавне власти у Републици Србији регулисан је Законом о тајности података и подзаконским актима, и обухвата следеће кораке:

Доношење формалне одлуке о тајности: Орган јавне власти је у обавези да донесе генеричну или појединачну писмену одлуку о одређивању степена тајности података, уз процену утицаја и потенцијалне штете по интересе Републике Србије у случају откривања, злоупотребе или уништења података. Тајност податка, под условима и на начин утврђен законом о тајности података, одређује овлашћено лице. При одређивању степена тајности податка, овлашћено лице одређује најнижи степен тајности који спречава настанак штете по интересе Републике Србије. Овлашћена лица која имају право да одређују степен тајности података према члану 9. Закона о тајности података су: председник Републике, председник Владе, руководиоца органа јавне власти, изабрани, постављени или именовани функционер органа јавне власти који је за одређивање тајних података овлашћен законом, односно прописом донесеним на основу закона, или га је за то писмено овластио руководиоца органа јавне власти, као и лице запослено у органу јавне власти које је за то писмено овластио руководиоца тог органа.

Идентификација категорија података: Подаци се анализирају како би се утврдило да ли испуњавају услове за означавање као тајни, укључујући прописима предвиђене категорије података, као и процену могућег утицаја на националну безбедност, јавни интерес, територијални интегритет и економске интересе. У овом кораку се такође разматра и општи значај података, као и последице које би њихово откривање могло имати на рад органа јавне власти.

Одређивање степена тајности: 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):

- ДРЖАВНА ТАЈНА - који се одређује ради спречавања настанка неотклоњиве тешке штете по интересе Републике Србије;

- **СТРОГО ПОВЕРЉИВО** - који се одређује ради спречавања настанка тешке штете по интересе Републике Србије;
- **ПОВЕРЉИВО** - који се одређује ради спречавања настанка штете по интересе Републике Србије; или
- **ИНТЕРНО** - који се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио.

Означавање података: Подаци добијају јасну ознаку која укључује степен тајности, начин престанка тајности, податке о овлашћеном лицу, датум означавања, назив органа који је донео одлуку и правну основу. Ознака мора бити видљива и у складу са прописаним стандардима у Уредби о начину и поступку означавања тајности података, односно документа („Службени гласник Републике Србије“ број 8/2001). Документ који садржи тајни податак означава се одговарајућим степеном тајности, изнад назива документа, на врху сваке странице, на средини. Ознака одговарајућег степена тајности на документу исписује се тамнијим словима већег формата од слова текста документа. Ако документ садржи више страница, свака страница се означава редним бројем странице у односу на укупан број страница. Сваки документ мора имати ознаку степена тајности на врху прве стране и спољне стране предњих корица ако оне постоје или на врху насловне стране. Ако документ нема насловну страну, прва страна ће се сматрати као насловна. Приликом означавања документа не сме доћи до уништења или оштећења тајног податка, односно документа на којем се он налази.

Евиденција и контрола: Тајни подаци се уписују у регистар и евиденцију тајних података ради праћења и контроле. Евиденција о тајним подацима води се одвојено од осталих евиденција органа јавне власти. Евиденција садржи: редни број, назив органа јавне власти, назив унутрашње организационе јединице органа јавне власти која је одредила степен тајности, садржај предмета, датум пријема предмета, класификациона ознака предмета, податке о уступању документа другом органу, податке о промени степена тајности, начин и датум престанка тајности, податак када је предмет архивиран и напомену. Орган јавне власти је у обавези да обезбеди адекватну административну, физичку и информациону безбедност.

Ревизија и ажурирање: Ознаке тајности се периодично преиспитују и ревидирају како би се утврдило да ли је потребно задржати, променити или укинути степен тајности, због временског ограничења, престанка тајности утврђивањем датума, наступањем одређеног догађаја и истеком рока. Одлука о опозиву тајности податка доноси се ако наступе чињенице и околности услед којих податак престаје да буде од интереса за Републику Србију.

Последице непоштовања процедура: Непоштовање прописаних процедура означавања и заштите тајних података може довести до озбиљних последица. Ове последице не обухватају само административне и организационе последице, већ могу бити и озбиљне правне и кривичне природе. У зависности од врсте прекршаја и тежине поступка, могу се применити различите казнене мере, укључујући санкције против органа јавне власти и одговорних лица, као и опасност по безбедност Републике Србије.

Казнене мере: У складу са Законом о тајности података, непоштовање процедура означавања, чувања и обраде тајних података може довести до различитих казnenих мера:

Прекршајне санкције се могу изрећи у случају када одговорна лица не испуне обавезе у погледу означавања, чувања или размене тајних података, или ако дође до њиховог неовлашћеног откривања. Прекршаји могу обухватити:

- Неадекватно означавање степена тајности.

- Недовољну заштиту тајних података.
- Неоправдано откривање података без одобрења или одлуке овлашћеног лица.

Кривичне санкције су озбиљније и применљиве су у случају кршења процедура које могу довести до значајне штете по безбедност Републике Србије. Члан 98. Закона о тајности података прописује кривично дело које укључује:

- Неовлашћено откривање тајних података: Лице које без овлашћења открије тајне податке или их користи у незаконите сврхе, може бити кривично гонјено.
- Злоупотреба тајних података: Лице које злоупотреби тајне податке, било да их дели, продаје или на неки други начин користи против националне безбедности, може бити осуђено на казне затвора.
- Недопуштена измена или уништавање тајних података: Лица која униште, измене или на неки начин ометају очување тајних података, као и лица која не предузму прописане мере заштите података, могу бити кривично санкционисана.

У складу са чланом 98. Закона, физичком лицу може се изрећи казна затвора до 5 година, зависно од природе дела. Утврђивање казне зависи од тога да ли је дошло до озбиљне штете по безбедност Републике Србије, односно да ли је дело довело до нарушавања националне безбедности.

Угрожавање безбедности

Непоштовање процедура означавања и заштите тајних података може директно угрозити националну безбедност, што може довести до:

Штете по безбедност Републике Србије: Откривање, злоупотреба или уништавање тајних података може нанети озбиљну штету одбрани, дипломатским и политичким односима или економским интересима земље.

Откривање података од војног или обавештајног значаја: Ако дође до откривања података који се односе на војне операције, обавештајну активност или стратегије одбране, то може довести до директне претње по сигурност земље и њених грађана.

Злоупотреба информација: Неовлашћени приступ тајним подацима може довести до извоза осетљивих информација и коришћења од стране странака које имају непријатељске намере према Србији.

Губитак поверења

Недостатак адекватне заштите тајних података може довести до значајног губитка поверења у органе јавне власти. Када грађани, правни субјекти или међународни партнери сазнају да се подаци који су од великог значаја за националну безбедност не чувају на адекватан начин, то може:

Нарушити углед органа јавне власти: Откривање пропуста у заштити тајних података може довести до негативних реакција јавности и партнерских земаља, што нарушава кредибилитет власти.

Нарушити однос са међународним партнерима: Недовољна заштита података може довести до кршења међународних споразума, што отежава сарадњу са иностранством.

Погоршање унутрашњег поверења: Институтима и грађанима може бити изгубљено поверење у способност органа јавне власти да адекватно управљају тајним подацима и да гарантују националну безбедност.

Правне импликације

Када дође до кршења процедура означавања и заштите тајних података, могу се покренути и правни поступци против одговорних лица:

Судски поступци: Ако се утврди да је поступак означавања или обраде података био незаконит, могу се покренути цивилни поступци, где се може захтевати одговорност за штету коју су органи јавне власти или њихови запослени нанели.

Прекршајни поступци: Уколико је дошло до прекршаја у смислу неправилног чувања или поступања са тајним подацима, могу се изрећи новчане казне или друге мере као што су упозорење или јавна опомена.

Поступци због повреда радне дисциплине: Одговорна лица која су прекршила процедуре могу бити предмет дисциплинских мера, као што су опомена, суспензија или отказ.

Поштовање процедура означавања и заштите тајних података није само законска обавеза, већ и морална и професионална одговорност свих запослених у органима јавне власти. Адекватна примена ових мера је основа за јачање поверења грађана, очување националне безбедности и интегритета државних институција, као и за заштиту од опасности које могу угрозити интересе Републике Србије. Свако кршење ових процедура представља значајан ризик који може довести до озбиљних последица, укључујући угрожавање сигурности земље, економског интегритета и међународних односа. Доследност у примени мера заштите тајних података осигурава стабилност, повећава међународни кредибилитет и јача безбедност државних институција, чиме се ствара чврст основ за адекватно реаговање на претње националној безбедности.

Методологија за процену и одређивање степена тајности података

Процена степена тајности података мора почивати на јасним и објективним критеријумима који спречавају злоупотребу тајности ради прикривања корупције, кршења људских права и незаконитог поступања. Основни принципи овог процеса подразумевају утврђивање реалне штете коју би откривање података могло проузроковати по безбедност државе, јавни ред, међународне односе или заштићене вредности. Истовремено, законска ограничења осигуравају да се тајност не користи као инструмент за ускраћивање информација од јавног интереса.

Изузетно је важно разликовати податке који заслужују заштиту од оних који морају бити доступни јавности. На пример, извештај о еколошкој хаварији или коруптивним радњама у јавним набавкама не сме бити означен као тајна, јер би то било супротно јавном интересу. С друге стране, критични безбедносни подаци, као што су војне стратегије или подаци о оперативним процедурама безбедносних служби, захтевају висок степен заштите како би се спречила потенцијална штета.

Одређивање степена тајности мора се заснивати на процени тежине могуће штете. У овом контексту, закон предвиђа четири нивоа тајности који се примењују у зависности од тога да ли би откривање података угрозило националну безбедност, функционалност државних

органа, дигиталну инфраструктуру или би изазвало само мање организационе поремећаје. Сваку одлуку о означавању тајности треба темељно документовати, уз јасно образложење засновано на процени штете, законској регулативи и роковима за ревизију тајности.

На крају, неопходно је осигурати баланс између потребе за заштитом података и јавног интереса. У случају дилеме, треба применити тест претежности јавног интереса како би се утврдило да ли је штета од објављивања већа од користи за јавност. То је кључни механизам којим се спречава неправилна примена тајности и обезбеђује транспарентност у раду јавних институција.

1. Основни принципи

Одређивање степена тајности података мора бити засновано на објективној процени штете коју би откривање тих података могло проузроковати безбедности Републике Србије, одбрани, спољнополитичким интересима, јавном безбедношћу или другим уставом заштићеним вредностима. Ова методологија се примењује приликом доношења појединачне одлуке о означавању тајног податка у складу са Законом о тајности података („Сл. гласник РС”, бр. 104/09, 36/11 и 88/19) и Уредбом о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА” и „СТРОГО ПОВЕРЉИВО” („Службени гласник РС”, број 46 од 24. маја 2013).

За податке који би могли проузроковати најтежу штету националној безбедности, територијалном интегритету или међународним односима, примењују се критеријуми наведени у Уредби за „ДРЖАВНУ ТАЈНУ”. Ово укључује документацију која садржи планове одбране, техничке карактеристике војне опреме и оперативне протоколе безбедносних служби. Овај степен тајности обухвата информације чије би откривање могло довести до значајних безбедносних ризика, нарушавања одбрамбених способности или компромитовања стратешких интереса државе.

„СТРОГО ПОВЕРЉИВО” обухвата податке чије би откривање озбиљно угрозило функционалност државних органа, спољнополитичке интересе или безбедносне операције. У ову категорију спадају подаци о идентитету тајних оперативаца, стратегије дипломатских преговора и техничке спецификације критичних комуникационих система. Овај степен тајности обезбеђује да се осетљиве информације користе само у строго контролисаним оквирима, како би се спречиле потенцијалне штете по институционалне структуре и спољнополитичке односе.

Одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у институцијама јавне власти регулисано је посебним уредбама које прецизирају критеријуме и процедуре означавања, чувања и приступа овим подацима. Ови прописи осигуравају да се информације класификују у складу са стварним ризицима и степеном штете коју би њихово откривање могло проузроковати, уз пуно поштовање транспарентности и јавног интереса.

Основна уредба која се примењује у органима јавне власти је Уредба о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” („Службени гласник РС”, бр. 79/2014-3), која је ступила на снагу 6. августа 2014. године. Ова уредба дефинише процедуре класификације и ревизије тајних података у државним институцијама, како би се обезбедило да само неопходни подаци добију одговарајући ниво заштите.

У Министарству одбране примењује се Уредба бр. 66/2014-4, која је ступила на снагу 7. јула 2014. године, а примењује се од 8. октобра 2014. Овај пропис утврђује како се подаци у области

одбране класификују, укључујући стратегије, оперативне процедуре и сигурносне мере критичне инфраструктуре.

Министарство унутрашњих послова следи критеријуме из Уредбе бр. 105/2013-7, која је ступила на снагу 7. децембра 2013. године, а примењује се од 8. марта 2014. године. Ова уредба обезбеђује правила за означавање поверљивих информација унутар полицијских структура, укључујући безбедносне протоколе, аналитичке извештаје и процедуре оперативне сарадње.

Канцеларија Савета за националну безбедност и заштиту тајних података руководи се Уредбом бр. 86/2013-3 од 8. октобра 2013. године, која прецизира методологију одређивања степена тајности података везаних за националну безбедност, стратешке процене ризика и процедуре заштите критичних ресурса.

Безбедносно-информативна агенција примењује Уредбу бр. 70/2013-6, која утврђује посебне критеријуме за означавање тајних података у домену безбедносних и контраобавештајних операција, оперативних метода и анализа безбедносних ризика.

Ове уредбе осигуравају да се тајност података у свим сегментима јавне управе примењује на основу јасно дефинисаних критеријума, уз сталну контролу и ревизију степена тајности података. Истовремено, законски оквир спречава злоупотребу тајности у прикривању информација од јавног интереса, чиме се обезбеђује баланс између безбедности и транспарентности, односно обезбеђују да се тајност података примењује у складу са јасно дефинисаним критеријумима, уз пуно поштовање јавног интереса и принципа транспарентности. Свакој одлуци о означавању степена тајности мора претходити темељна процена могуће штете и јасно образложење засновано на законским нормама. Такав приступ спречава злоупотребу тајности и осигурава легитимност и оправданост сваке ознаке тајности података у Републици Србији.

2. Законско искључење од могућности означавања података као тајних

Према члану 3. Закона о тајности података, постоје јасно прописана ограничења у погледу примене мере тајности на одређене врсте података. Ниједан податак не може бити означен као тајни ако би таквим означавањем било онемогућено или битно ограничено његово откривање, у случајевима када је реч о питањима од непосредног јавног интереса. У складу са тим, тајност не сме служити као основ за прикривање било ког од следећих случајева:

- **Покушај прикривања кривичног дела** – Означавање података као тајних не сме да буде злоупотребљено у циљу спречавања откривања, истраге или процесуирања кривичних дела, без обзира на то да ли су у питању појединци или носиоци јавних функција.
- **Кршење основних људских права и слобода** – Не постоји законска основа да се на податке који указују на повреду гарантованих права (нпр. право на живот, забрана тортуре, право на правично суђење и сл.) ставља ознака тајности. Напротив, такви подаци морају бити доступни ради заштите људског достојанства и владавине права.
- **Злоупотреба јавних овлашћења** – У ситуацијама у којима је реч о прекорачењу или злоупотреби службеног положаја, односно деловању супротном прописима, не може се ознака тајности користити да би се избегла одговорност или прикрила институционална неделотворност. Податак који указује на злоупотребу мора остати доступан у складу са законом.

• **Незаконито поступање или пропусти органа јавне власти** – Тајност се не може одредити у циљу прикривања незаконитих одлука, аката или пропуста у раду државних или других органа јавне власти. Услов за примену тајности јесте заштита легитимних интереса државе, а не прикривање незаконитости.

• **Угрожавање здравља људи, животне средине и безбедности** – Информације које се односе на загађење, хаварије, изложеност опасним материјама или друге околности које могу директно утицати на здравље становништва и безбедност, морају бити јавно доступне. Ускраћивање оваквих података путем ознаке тајности представљало би супротност јавном интересу и кршење основних принципа транспарентности.

Ова ограничења представљају суштински елемент баланса између потребе државе да заштити одређене податке ради безбедности, и права јавности на приступ информацијама које се тичу основних права, здравља, заштите животне средине и борбе против корупције. Свако означавање тајности које заобилази ова правила представља повреду закона и основних демократских начела.

Практични примери:

Пример	Образложење
Извештај о хаварији у државном постројењу која је довела до загађења воде или ваздуха у насељеном месту	Не може бити означен као тајна јер би то ограничило или онемогућило откривање информација од значаја за заштиту здравља људи, животне средине и безбедности становништва.
Службена белешка о поступању државног органа у случају незаконитог лишења слободе или онемогућавања приступа адвокату	Не може бити означена као тајна јер би то прикрило кршење основних људских права.
Извештај о интерној контроли у органу управе који указује на коришћење службеног положаја за приватну корист	Забрањено је означавање таквих докумената као тајних, јер би се тиме прикривала злоупотреба јавних овлашћења.
Документација која открива да је државни орган поступао противно закону (нпр. незаконито трошење буџетских средстава, незаконита решења или решавање по службеној дужности)	Не може се означити као тајна ако би се тиме прикрио противзаконити акт или поступање органа власти.
Извештај у ком се наводи опасност по безбедност људи услед неблаговременог реаговања надлежне службе (нпр. у случају елементарних непогода, хаварија, епидемија)	Не сме бити означен као тајан јер би то значило прикривање података од значаја за живот и здравље грађана.

3. Процена потребе за заштитом података

Први корак у поступку означавања је утврђивање да ли податак уопште треба да буде заштићен.

Питања која се постављају:

- Да ли би откривање података угрозило безбедност државе, јавни ред, или међународне односе?
- Да ли би откривање довело до ометања правосудних или безбедносних поступака?
- Да ли се ради о подацима који се односе на систем заштите података, оперативне процедуре, или критичну инфраструктуру?

Питање	Пример
Да ли би објављивање угрожавало безбедност државе?	Планови одбране – ДА
Да ли се ради о интерним информацијама без значаја?	Листа службених телефона – НЕ (осим у случају безбедносних служби)
Да ли се ради о доказима у поступку за кршење закона?	Извештај антикорупцијске јединице – НЕ СМЕ бити тајна

4. Процена могуће штете – критеријуми за одређивање степена тајности

Приликом одређивања тајног податка, ниво тајности мора бити у сразмери са тежином и вероватноћом штете која би могла настати уколико би податак био откривен неовлашћеном лицу. Закон о тајности података („Сл. гласник РС“, бр. 104/2009) прописује четири степена тајности, а сваки се примењује искључиво на основу објективне процене могуће штете по интересе Републике Србије.

1. ДРЖАВНА ТАЈНА

Највиши степен тајности. Примењује се у случајевима када би откривање података проузроковало најтежу штету по:

- националну безбедност,
- територијалну целовитост,
- уставни поредак,
- међународне односе Републике Србије.

Примери:

- Техничка документација и локације подземних или специјалних војних објеката,
- Оперативни планови у кризним ситуацијама,
- Стратегијски комуникациони системи и кодови.

2. СТРОГО ПОВЕРЉИВО

Означава се када би откривање података озбиљно угрозило:

- институционалну стабилност и рад органа власти,
- спољнополитичке и безбедносне интересе,
- односе са савезницима или међународним организацијама.

Примери:

- Сарадња са страним безбедносним или обавештајним службама,

- Идентитет и ангажовање оперативаца у иностранству,
- Тајне дипломатске комуникације.

3. ПОВЕРЉИВО

Примењује се када би откривање података проузроковало штету средњег интензитета, као што су:

- ометање рада органа управе,
- нарушавање безбедности информационих система,
- угрожавање интерних оперативних планова и процедура.

Примери:

- Интерни протоколи за заштиту дигиталне инфраструктуре,
- Упутства за поступање у ванредним ситуацијама,
- Радне анализе ризика унутар безбедносних служби.

4. ИНТЕРНО

Најнижи степен тајности. Односи се на податке чије би откривање изазвало мању или краткотрајну штету, без значајног утицаја на јавни интерес.

Примери:

- Радне белешке и интерне евиденције,
- Прелиминарни или припремни документи који нису званично усвојени,
- Унутрашња комуникација и предлози унутар служби.

Степен тајности **ИНТЕРНО** често се погрешно изједначава са штићеним подацима којима располаже орган јавне власти, а који нису обухваћени режимом Закона о тајности података. Иако оба типа података могу бити интерне природе и ограниченог приступа, само подаци који су означени у складу са законом као тајни и за које је извршена процена штете могу бити у систему тајности. Насупрот томе, штићени подаци се могу штитити другим прописима (нпр. законом о заштити података о личности, законом о архивској грађи, итд.) и не подлежу обавезама везаним за степене тајности као што су прописани у Закону о тајности података. Због тога је важно јасно разграничити ова два режима заштите.

Одређивање степена тајности мора бити утемељено на јасним и проверљивим критеријумима, заснованим на стварној процени могуће штете. Неопходно је избегавати произвољно или формално означавање, јер прекомерна или неоснована тајност може довести до ограничења јавног надзора и смањења одговорности органа власти. Свака одлука мора бити документована, пропорционална и временски ограничена, са обавезом периодичног преиспитивања оправданости тајности.

Примери из праксе

Пример 1: Злоупотреба тајности ради прикривања незаконитости

Једна општина је означила као *ДРЖАВНУ ТАЈНУ* набавку мобилних телефона за функционере, позивајући се на „безбедносне ризике комуникације“. У поступку контроле је утврђено да је тајност злоупотребљена ради прикривања ненаменског трошења буџетских

средстава. У складу са чланом 3. Закона о тајности података, такав податак се не може сматрати тајним.

Пример 2: Претежност јавног интереса

Документација у вези са уговарањем инфраструктурних радова на изградњи електране била је означена као *ПОВЕРЉИВО*. Међутим, невладина организација је захтевала увид у податке, позивајући се на право јавности да зна услове уговора финансираног из буџета. У спроведеном поступку по Закону о слободном приступу информацијама, орган је био дужан да примени тест јавног интереса, и део документације је декласификован јер објављивање не би проузроковало штету већу од користи за јавност.

Пример 3: Оправдана тајност у области националне безбедности

Планови евакуације и спискови критичне инфраструктуре у случају оружаног напада означени су као *СТРОГО ПОВЕРЉИВО*. У овом случају, процена штете од евентуалног откривања таквих података јасно указује на претежност интереса заштите националне безбедности у односу на право јавности на приступ.

Пример 4: Забуна између „интерно“ и других штићених података

Интерни извештај министарства о запосленима, који садржи агрегиране податке о радном учинку, био је означен као *ИНТЕРНО*. Иако није постојала формална процена штете нити утврђена основа за примену Закона о тајности података, орган је одбио да достави извештај, позивајући се на „тајност“. Независна контрола је утврдила да се ради о штићеним, али не и тајним подацима, и наложила да се подаци ставе на увид јавности у обиму који не садржи личне или осетљиве податке.

Ови примери показују да је одговорно поступање са подацима од значаја за Републику Србију могуће само уз јасно познавање законског оквира и етичког приступа који подразумева да се тајност не користи као механизам за скривање, већ као изузетак у заштити легитимних јавних интереса.

5. Баланс интереса – примена јавног интереса

Одређивање степена тајности података и процена штете по интересе Републике Србије, односно да ли одређени податак треба да буде означен као тајан, као и којим степеном тајности, врши се на основу процене могуће штете која би настала ако би податак постао доступан неовлашћеним лицима. Међутим, та процена није апсолутна и подразумева примену баланса интереса, односно вагање између потребе заштите интереса Републике Србије и јавног интереса за слободан приступ информацијама.

Према члану 8. Закона о тајности података, тајним податком може се одредити само онај податак:

- који је од интереса за Републику Србију,
- чијим би откривањем неовлашћеном лицу настала штета, и
- ако је потреба заштите тог интереса претежнија од интереса јавности да буде обавештена.

То значи да се за сваку конкретну информацију мора извршити тзв. тест претежности интереса, у коме се процењује:

- колика је могућа и конкретна штета по интересе државе у случају откривања податка;
- да ли је та штета стварна, озбиљна и непосредна;
- да ли постоји јавни интерес да информација буде доступна, нарочито ако се односи на злоупотребе, незаконитости, управљање јавним средствима, јавне набавке и сл.;
- да ли би прикривање информације било супротно циљевима транспарентности и демократског надзора.

Подаци на које се овај члан односи нарочито се тичу:

- националне и јавне безбедности, као и одбрамбених, безбедносних и обавештајних послова;
- спољнополитичких односа и међународне сарадње;
- система, уређаја, планова и структура у вези са горе наведеним пословима;
- научних, технолошких, економских и финансијских послова повезаних с наведеним интересима.

Закон изричито предвиђа, у члану 3, да тајним податком не може бити проглашен податак ради прикривања кривичног дела, злоупотребе положаја или другог незаконитог поступања органа јавне власти.

То значи да ниједна информација не може бити означена као тајна у циљу избегавања одговорности, прикривања неправилности или спречавања јавности да сазна за поступке од значаја за надзор над радом државе.

Одлука о означавању података као тајних мора бити резултат **објективне, пропорционалне и образложене процене**, засноване на конкретној претњи и могућој штети по интересе Републике Србије. У том процесу, **јавни интерес се не сме посматрати као супротност безбедности**, већ као њен саставни део и мерило оправданости ограничења права на приступ информацијама.

Примена **теста претежности интереса** није формалност, већ **обавеза која проистиче из закона и принципа добре управе**. Та одлука мора бити:

- **доказива** – заснована на проверљивим чињеницама и проценама;
- **пропорционална** – у мери у којој је стварно неопходно ограничити приступ;
- **временски ограничена** – са редовном ревизијом оправданости тајности.

Свака одлука о тајности мора имати **експлицитно и на закону засновано образложење**, како би се спречила појава такозване „*културе тајности*“, која угрожава транспарентност и умањује поверење јавности у институције.

Кључни принцип: Информације не припадају држави – држава их чува у име грађана. Због тога, свака одлука о проглашавању података тајним мора бити **оправдана не као инструмент моћи, већ као изузетак у функцији заштите општег интереса**.

Примери:

Ситуација	Одлука
Уговор о набавци оружја – део финансиран из буџета	Објавити финансијске податке; прикрити податке о тактичкој употреби
Извештај о незаконитом трошењу средстава у одбрани	Не сме бити означен као тајна
Техничке карактеристике система за надзор комуникација	Могу бити делимично тајни – али се мора проверити да ли је то оправдано и законито

6. Документација – образложење одлуке о тајности

Одлука о означавању података као тајних мора бити формално и материјално утемељена, у складу са Законом о тајности података. Свака таква одлука мора да садржи следеће елементе:

Назив документа или скупа података

Јасно и недвосмислено означавање садржаја који се ставља под режим тајности, укључујући бројеве аката, називе фајлова или јединствене ознаке система.

Предложени степен тајности

Један од четири законом предвиђена нивоа тајности: *ИНТЕРНО*, *ПОВЕРЉИВО*, *СТРОГО ПОВЕРЉИВО* или *ДРЖАВНА ТАЈНА*, у складу са проценом могуће штете.

Образложење засновано на процени штете

Конкретна процена врсте и тежине штете коју би откривање информације могло проузроковати интересима Републике Србије, уз објашњење зашто је тајност неопходна.

Упућивање на релевантне чланове закона

Навођење члана 8. Закона о тајности података као основа за означавање, као и других релевантних одредби које подупиру оцену (нпр. члан 14, члан 16, итд.).

Проверу искључености од тајности (чл. 3)

Изричито навођење да се не ради о податку чија би тајност служила прикривању кривичног дела, прекорачења овлашћења или злоупотребе службеног положаја. Ово је обавезан корак у поступку, и представља правну гаранцију против злоупотребе тајности.

Рок трајања ознаке тајности

Дефинисање максималног трајања тајности у складу са прописаним роковима за сваку категорију (нпр. 30 година за државну тајну), уз могућност ранијег укидања ако престану разлози за тајност.

Планирани рок за ревизију ознаке

Навођење датума или интервала када ће се одлука преиспитати, у складу са принципом привремености тајности и обавезом редовне ревизије. Овај рок не сме бити дужи од 5 година за већину нивоа тајности.

Оваква структура одлуке омогућава транспарентност, одговорност и законитост у поступку означавања података као тајних, чиме се унапређује поверење у институције и спречавају злоупотребе система заштите података.

Напомена: У органима јавне власти у којима се одређене категорије и врсте тајних података учестало појављују у пракси, ради смањења административног оптерећења и обезбеђивања доследности у примени, уобичајено је доношење **каталога тајних података**. Такав каталог представља интерни акт у којем су унапред дефинисани типови података и њихови одговарајући степени тајности (*интерно, поверљиво, строго поверљиво, државна тајна*).

Иако **Закон о тајности података** овакву праксу **не прописује, али је ни не забрањује**, услов њене законитости јесте да се сваки унети податак у каталог заснива на стварној процени штете у складу са чланом 8. закона, као и да се **каталог периодично преиспитује и ажурира**, у складу са чланом 14. закона и начелом привремености тајности.

Каталог тајних података **заменеује појединачну одлуку о одређивању степена тајности** за одређене врсте података који се редовно појављују у пракси, чиме се олакшава административни процес и обезбеђује доследност у примени. Иако **Закон о тајности података** не прописује, али ни не забрањује овакву праксу, важно је да се **каталог периодично преиспитује и ажурира** у складу са законским обавезама, нарочито у погледу процене штете и оправданости означавања одређених података као тајних. Оваква пракса треба да буде усмерена ка усклађивању са законима и принципима добра управе, те мора бити заснована на стварној потреби заштите одређених података.

Пример образложења:

Назив документа: План заштите критичне ИКТ инфраструктуре

Предлог степена тајности: Строго поверљиво

Образложење: Документ садржи опис рањивих тачака, мере заштите и критичне ресурсе који, уколико би постали доступни, могу бити искоришћени за угрожавање система. Укључује информације које се односе на специфичне техничке аспекте који су кључни за функционисање безбедносних и комуникационих мрежа. Њихово откривање могло би довести до озбиљних ризика по безбедност државних и приватних интереса, што оправдава потребу за високим степеном тајности.

Законска основа:

Члан 8.: регулише податке који се могу одредити као тајни. Према овом члану, податак се може означити као тајан ако би његово откривање неовлашћеном лицу нанело штету, а потреба заштите интереса Републике Србије превазилази интерес за слободан приступ информацијама од јавног значаја.

Члан 12.: регулише посебне случајеве одређивања и означавања тајних података. Према овом члану, овлашћено лице може одредити као тајни податак који је настојао обједињавањем или повезивањем података без ознаке тајности, ако овај комбиновани податак захтева заштиту. Такође, ако документ садржи податке различитих степена тајности, он се означава највишим степеном тајности и дужим роком чувања. Уколико само мањи део документа садржи тајне податке, тај део се издваја као посебан прилог.

Члан 13.: Овај члан регулише начин означавања тајних података и докумената, укључујући степен тајности, начин престанка тајности, податке о овлашћеном лицу и органу јавне власти. Влада прописује детаљан поступак означавања тајности.

Члан 14.: Овај члан утврђује четири степена тајности података: **Државна тајна, Строго поверљиво, Поверљиво и Интерно.** Степен тајности се одређује на основу процене ризика од штете по интересе Републике Србије. Ближе критеријуме за највише степене утврђује Влада, уз мишљење Савета за националну безбедност.

Члан 16.: Овај члан прописује да се рокови чувања тајности података морају одредити на основу процене штете која би могла настати њиховим откривањем. Рокови чувања тајности не могу бити дужи од 30 година, али се морају периодично преиспитивати. Подаци се морају поново оценити пре истека тог рока и у складу са чланом 19. и 20. закона, који прописују детаљне критеријуме за ревизију и престанак односно уклањање ознаке тајности.

Рок тајности: 10 година

Планирана ревизија: Након следеће техничке ревизије система (најкасније у року од 5 година)

Листа за процену одређивања степена тајности података:

1. Прелиминарна провера

Да ли податак спада у категорије изузете од тајности?

(Члан 3 Закона о тајности података)

Пример: Подаци који прикривају кривично дело, кршење људских права, злоупотребе јавних овлашћења.

Да ли постоји јавни интерес за откривање податка?

Пример: Информације о еколошким хаваријама, корупцији у јавним набавкама.

Да ли је овлашћено лице задужено за одлуку?

(Члан 9 Закона о тајности података)

Пример: Руководилац органа, председник Владе, лице које је писмено овлашћено.

2. Идентификација категорије података

Да ли се податак односи на:

- Националну безбедност?
- Јавну безбедност?
- Одбрану?
- Територијални интегритет?
- Дипломатске/међународне односе?
- Критичну инфраструктуру?

Да ли је податак везан за:

- Системе заштите података?

- Интерне процедуре органа?
- Припреме за ванредне ситуације?

3. Процена штете

Колико је озбиљна потенцијална штета?

- Државна тајна: Неотклоњива тешка штета (нпр. Планови одбране).
- Строго поверљиво: Тешка штета (нпр. идентитет прикривеног иследника или оперативаца).
- Поверљиво: Штета (нпр. протоколи заштите ИКТ).
- Интерно: Штета за рад, послове органа јавне власти (нпр. интерна евиденција).

Да ли је штета:

- Реална? *[Документован ризик]*
- Озбиљна? *[Угрожава функционалност државе]*
- Непосредна? *[Штета би наступила у року од 6 месеци]*

4. Тест претежности јавног интереса (члан 8. Закона о тајности података)

Да ли је заштита интереса Републике Србије претежнија (јача) од интереса за слободан приступ информацијама од јавног значаја?

Пример:

- Не: Ако се ради о непотпуној информацији о корупцији.
- Да: Ако се ради о детаљима Плана одбране.

Да ли се са података може делимично скинути ознака тајности?

Пример: Објавити финансијске детаље набавке, али зацрнити техничке спецификације.

5. Формална одлука о тајности

Обележите документ у складу са Уредбом о начину и поступку означавања тајности података, односно докумената (Сл. гласник Р. Србије бр. 8/2001):

- Степен тајности на врху сваке странице.
- Начин престанка тајности (нпр. "Тајност престаје 31.12.2030.").
- Подаци о овлашћеном лицу и органу.

Унесите податак у регистар тајних података:

- Редни број, датум, назив органа, лице које је одредило степен тајности, садржај, класификациони (редни) број и ознака тајности.

6. Контрола и ревизија

- Да ли је одређен рок за преиспитивање - ревизију тајности?
- Максимално: 30 година за државну тајну.

- Препоручено: 5 година за ниже степене.
- Да ли је обезбеђена безбедност податка?
- Физичка (осигурани ормари, контрола приступа).
- Дигитална (енкрипција, двослојна аутентификација).

7. Последице непоштовања

Да ли су запослени упознати са:

- Кривичним санкцијама за откривање тајних података?
- Прекршајним и дисциплинским казнама за неозначавање или погрешно означавање тајних података?
- Да ли постоји интерни механизам за пријаву злоупотребе?
- Унутрашња контрола у органу јавне власти?
- Одговорно лице за рад са тајним подацима?

Пример употребе листе:

- ✓ Податак: План евакуације грађана у случају природне катастрофе.
- ✓ Чек-листа:
- ✓ Прелиминарна провера: Није у члану 3 (не прикрива кривично дело).
- ✓ Идентификација: Односи се на јавну безбедност.
- ✓ Процена штете: Откривање би омело евакуацију → Строго поверљиво.
- ✓ Тест јавног интереса: Јавност има право да зна о постојању плана, али не и о тачним локацијама → делимично скидање ознаке тајности са документа.

Напомена: Редовно обучите запослене о процедурама — највећи ризик је људска грешка!

Политичка одговорност носилаца највиших функција у раду са тајним и страним тајним подацима

Правним системом Републике Србије предвиђено је да носиоци највиших функција у Републици Србији, као што су председник Републике, председник Народне скупштине, председник Владе, чланови Владе, као и функционери којима Уставом или законом нису одређени претпостављени, односно да су лично и политички одговорни за заштиту тајних података до којих долазе у обављању своје функције. Одредба члана 37. Закона о тајности података уводи изузетно важан стуб одговорности у систему заштите тајних података – политичку одговорност, која се разликује од дисциплинске, прекршајне или кривичне одговорности, тиме што се заснива на јавном поверењу и моралној одговорности за поверено вршење власти.

Кључни елементи одговорности

Непосредна лична одговорност - Носилац функције одговара лично, без обзира на то да ли су тајни подаци изворно домаћег или страног порекла. Није потребна посебна безбедносна провера, али се подразумева обавеза поступања у складу са законом и мерама заштите тајних података.

Одговорност за стране тајне податке - Ова норма се подједнако примењује и у случајевима поступања са страним тајним подацима који се Републици Србији достављају на основу међународних споразума. Носиоци највиших функција морају поступати с тим подацима у складу са прописаним степеном тајности и посебним условима који су дефинисани у међународноправним актима.

Нема имунитета од одговорности - Иако многи од ових функционера уживају имунитет у кривичном и парничном поступку, одговорност за заштиту тајних података има јавни и морални карактер, што значи да кршење те обавезе повлачи политичке последице – попут оставке, смене или губитка јавног поверења.

Јачање интегритета и безбедности - Овим се јасно наглашава да су државне функције неодвојиве од поштовања највиших стандарда у области заштите поверљивих информација, што је посебно важно у контексту сарадње са међународним партнерима и обавеза из међународних безбедносних споразума.

Значај за систем националне безбедности - Политичка одговорност у раду са тајним подацима има и превентивну и репутациону функцију. Она обезбеђује поштовање принципа одговорног управљања информацијама и тиме заштиту интереса националне безбедности Републике Србије и истовремено подржава поверење страних партнера у капацитете Републике Србије за заштиту тајних података у складу са међународним стандардима (NATO, EU, билатерални споразуми).

Упознавање са правима, обавезама и одговорностима у вези са тајним подацима - У складу са Законом о тајности података и другим релевантним прописима који уређују област поступања са тајним подацима у Републици Србији, упознајете се са својим правима, обавезама и одговорностима, и то:

1. Права - на приступ тајним подацима који су неопходни за обављање функције и радних задатака, у складу са принципом „*потребно да зна*“; и - на редовно усавршавање у области безбедности и заштите тајних података.
2. Обавезе - да се са тајним подацима поступа у складу са прописима, што подразумева њихово чување, обраду и пренос на безбедан начин; као и - редовног извештавања о свим безбедносним инцидентима или сумњама у вези са тајним подацима.
3. Санкције: У случају кршења прописа, лице сноси дисциплинску и прекршајну одговорност, а уколико се утврди да је његовим поступањем угрожена национална безбедност — и кривичну одговорност.

Поред наведеног, посебно се истичу следећи аспекти:

- **Заштита тајних података:** Као овлашћено лице за рад са тајним подацима, дужни сте да поступате у складу са прописима Републике Србије. То подразумева адекватну заштиту података од неовлашћеног приступа, као и спречавање било каквог неовлашћеног коришћења или откривања тих података.
- **Принцип „потребно да зна“:** Ваш приступ тајним подацима мора бити ограничен искључиво на оне информације, документе и податке који су вам неопходни за обављање службених задатака. Свако поступање ван овог оквира представља озбиљно кршење закона и правила о заштити тајних података.
- **Извршавање обавеза:** Бићете редовно обавештавани о свим променама у прописима који се односе на заштиту тајних података. Уколико дође до измена ваших радних обавеза, бићете благовремено информисани путем брифинга и обука, како бисте били у потпуности усклађени са новим захтевима и процедурама.
- **Права на обуку и подршку:** Имате право на сталну стручну обуку и подршку у области заштите тајних података. У случају било каквих недоумица у вези са приступом или поступањем са тајним подацима, имате право да затражите савет и консултације од надлежних лица у вашој организацији.
- **Приступ релевантним информацијама:** Имате право на благовремен, потпун и несметан приступ свим прописима, смерницама и другим релевантним информацијама које се односе на безбедност и заштиту тајних података.

Кривично дело неовлашћеног одавања тајних података – преглед члана 98. Закона о тајности података

Члан 98. Закона о тајности података („Службени гласник РС“, бр. 104/2009) утврђује кривично дело **неовлашћеног одавања тајних података**. Одговорност учиниоца зависи од одређеног степена **тајности података** који су откривени, као и од **мотива учиниоца**, било да је у питању намера, немар или други облици одговорности. Околности под којима је дело извршено додатно се узимају у обзир, посебно ако је откривање података проузроковало **значајне последице по националну безбедност или јавни интерес**. Кривично дело подразумева **строге санкције**, које могу укључивати затворске казне, у зависности од тежине повреде тајности. Закон посебно разматра случајеве када је одавање информација учињено **са намером** **наношења штете** или **стеченој користи**, што може довести до тежих казних мера.

Овај закон има за циљ заштиту тајних података и спречавање **неовлашћеног приступа** информацијама које су од суштинске важности за националну безбедност и одбрану државе.

Основни облик кривичног дела - Кривично дело неовлашћеног одавања тајних података постоји када лице, без овлашћења, непозваном лицу:

- саопшти,
- преда, или
- учини доступним
- податке или документа који:
- су му поверени, или
- до којих је дошло на други начин,
а који су означени степеном тајности „ИНТЕРНО“ или „ПОВЕРЉИВО“, у складу са Законом. За овакво понашање прописана је казна затвора у трајању од три месеца до три године.

Пример из праксе - Један од забележених случајева кршења овог закона односи се на **неовлашћено откривање поверљивих информација у медијима**. У конкретном случају, службеник једне државне институције је, без одобрења, проследио поверљиве документе новинару, који су касније објављени у јавности. Ови документи су садржали информације означене као „ПОВЕРЉИВО“, а њихово откривање је могло угрозити националну безбедност.

Суд је утврдио да је службеник **свестан последица** свог поступка и да је намерно поступио супротно законским одредбама. Као резултат, осуђен је на **једну годину затвора**, уз додатну меру **забране обављања послова који укључују руковање тајним подацима** у периоду од осам година.

Овај пример показује озбиљност кривичног дела и последице које могу настати услед неовлашћеног откривања тајних података.

Тежи облици кривичног дела – Када су повређени подаци вишег степена тајности, закон предвиђа строже казне које се одређују у зависности од ознаке тајности:

- „СТРОГО ПОВЕРЉИВО“ – затвор од шест месеци до пет година
- „ДРЖАВНА ТАЈНА“ – затвор од једне до десет година

Пример из праксе - У једном случају, високо ранжирани државни службеник је неовлашћено открио документе означене као „ДРЖАВНА ТАЈНА“ страним дипломатама. С обзиром на то да је откривање ових података могло имати директне последице по националну безбедност, поступак је оцењен као тежи облик кривичног дела.

Суд је утврдио да је радња била намерна, са свестом о могућим штетним последицама. Као резултат, службеник је осуђен на шест година затвора, уз трајну забрану обављања функција које подразумевају приступ поверљивим информацијама.

Овај случај наглашава озбиљност кривичног дела и указује на дужину казне у зависности од степена тајности нарушених података.

Посебно тешке околности - Ако је кривично дело учињено у посебно тешким околностима, закон предвиђа знатно строже казне. Тежина санкције зависи од мотива учиниоца и

потенцијалних последица откривања поверљивих информација. Посебно се истичу следеће ситуације у којима се примењују строжији критеријуми:

- из користољубља – када је податке открио ради личне или материјалне користи,
- ради објављивања или коришћења података у иностранству – што може угрозити националну безбедност,
- у време ратног или ванредног стања – када последице могу бити нарочито штетне.

Прописане казне према степену тајности података

- **„ИНТЕРНО“ / „ПОВЕРЉИВО“ – затвор од шест месеци до пет година**
- **„СТРОГО ПОВЕРЉИВО“ – затвор од једне до осам година**
- **„ДРЖАВНА ТАЈНА“ – затвор од пет до петнаест година**

Пример из праксе - У једном случају, запослени у државној институцији је, из користољубља, продао документа означена као „ДРЖАВНА ТАЈНА“ страним агентима. Радњом је угрожена оперативна безбедност критичних структура националне одбране. Суд је утврдио да је учинилац поступио са намером и свешћу о последицама, због чега је осуђен на десет година затвора. Уз затворску казну, изречена је забрана обављања јавних функција, као и конфискација незаконито стечене имовине.

Овај случај показује озбиљност кривичног дела и друштвену опасност коју носи неовлашћено откривање поверљивих података у посебно тешким околностима.

Непажња (нехат)

У ситуацијама када је неовлашћено откривање тајних података извршено из нехата, санкције су блаже него у случајевима намерног дела, али и даље представљају значајну правну последицу. У питању је облик кривичног дела који произилази из непажње или несмотреног поступања, а не из свесне намере да се тајни подаци учине доступним непозваним лицима.

Прописане казне у зависности од степена тајности података

- **„ИНТЕРНО“ / „ПОВЕРЉИВО“ – затвор до две године**
- **„СТРОГО ПОВЕРЉИВО“ – затвор од три месеца до три године**
- **„ДРЖАВНА ТАЈНА“ – затвор од шест месеци до пет година**

Пример из праксе - У једном случају, државни службеник је ненамерно оставио поверљиве документе у ненадзираној просторији, где су били доступни трећим лицима. Иако није било свесне намере да се тајни подаци открију, ситуација је резултирала њиховим неовлашћеним приступом и могућом злоупотребом.

Суд је утврдио да је учинилац поступио из крајње непажње, иако није имао намеру да угрози поверљивост података. Као последицу, службеник је осуђен на годину дана затвора, уз забрану обављања послова који укључују руковање тајним подацима у периоду од пет година.

Овај случај показује да нехајно поступање према поверљивим подацима такође носи кривичну одговорност и може резултирати значајним санкцијама, у зависности од степена угрожене тајности.

Правна и безбедносна важност кривичног дела из члана 98. Закона о тајности података

Кривично дело из члана 98. Закона о тајности података Републике Србије представља кључни механизам у систему заштите тајних података. Њиме се уређује одговорност за неовлашћено поступање са подацима којима је, у складу са законом, одређен степен тајности – ИНТЕРНО, ПОВЕРЉИВО, СТРОГО ПОВЕРЉИВО и ДРЖАВНА ТАЈНА.

Значај за правни систем и институционалну безбедност

Члан 98. предвиђа више облика овог кривичног дела – од основног облика, преко тежих форми, до нарочито тешких случајева – што омогућава примену казни у складу са последицама неовлашћеног откривања података. Ова правна разрађеност има директан утицај на:

- очување националне безбедности,
- заштиту система одбране,
- очување поверљивости у спољној политици,
- економску и дипломатску стабилност институција.
- Циљ законске регулативе
- Основни циљ овог кривичноправног института јесте:
- обезбеђење високог нивоа поверења у институције које рукују тајним подацима,
- превенција злоупотреба које би могле угрозити виталне интересе државе,
- заштита информација чије откривање може изазвати озбиљне безбедносне последице.

Санкције прописане овим чланом, у распону од новчаних казни до дугогодишњих казни затвора, зависе од степена тајности података, последица откривања и облика кривице (намерно или из нехата).

Упоредни осврт: Међународна пракса

Сличан правни механизам постоји у већини савремених држава. Упоредна анализа показује да постоје заједничке основе, али и разлике у приступу санкционисању повреда поверљивости:

Сједињене Америчке Државе – Espionage Act (1917): строго кажњава неовлашћено откривање или поседовање поверљивих информација, посебно уколико постоји намера наношења штете националној безбедности. Предвиђене су вишедеценијске казне затвора.

Уједињено Краљевство – Official Secrets Act: обухвата и намерне и нехатне радње које доводе до откривања тајни, а санкције зависе од функције починиоца и степена штете.

Савезна Република Немачка – Staatsgeheimnisverrat (StGB §§93-100): предвиђа тешке казне за откривање државних тајни, посебно ако су подаци доступни страним субјектима или медијима.

Кривично дело из члана 98. Закона о тајности података Србије представља окосницу у систему заштите података од значаја за државу. Његов значај није само у санкционисању, већ и у превентивној функцији – одвраћању од непрофесионалног или злонамерног поступања с поверљивим информацијама.

Иако су глобални правни оквири различити, сви имају заједнички циљ: заштиту интереса државе и њених грађана од безбедносних ризика проистеклих из неовлашћеног приступа тајним подацима.

Сличности и разлике између одређених кривичних дела у српском законодавству

У савременом друштву, управљање информацијама представља један од кључних изазова у области права и безбедности. Обрада и заштита података, било да су лични, пословни или државни, играју централну улогу у очувању приватности, спречавању злоупотреба и осигурању стабилности дигиталних и правних система. У српском кривичном законодавству постоје бројна кривична дела која санкционишу неовлашћено прикупљање, откривање или злоупотребу поверљивих информација. Овде ћемо упоредити кривично дело из члана 98. Закона о тајности података, неовлашћено прикупљање личних података (члан 146. КЗ), одавање пословне тајне (члан 240. КЗ), неовлашћен приступ заштићеном рачунару (члан 302. КЗ) и неовлашћено откривање тајне (професионалне тајне, члан 141. КЗ).

Сличности

Поверљивост података – Сва ова дела се односе на заштићене информације (лични подаци, пословне тајне, рачунарски системи, професионалне тајне).

Неовлашћено деловање – Сви ови преступи подразумевају неовлашћену радњу (прикупљање, откривање, приступ).

Субјект дела – У неким случајевима, извршилац може бити одређено лице (нпр. запослени који открије пословну тајну или лекар који открије здравствену тајну).

Штетне последице – Ови преступи могу имати штетне последице по појединце, компаније или државу.

Разлике

Објект заштите

- Члан 98. Закона о тајности података – штити државне тајне и поверљиве информације од националног значаја.
- Члан 146. КЗ (неовлашћено прикупљање личних података) – штити приватност и личне податке појединаца.
- Члан 240. КЗ (одавање пословне тајне) – штити пословне информације које имају комерцијалну вредност.
- Члан 302. КЗ (неовлашћен приступ рачунару/мрежи) – штити интегритет рачунарских система и електронску обраду података.
- Члан 141. КЗ (неовлашћено откривање професионалне тајне) – штити тајне из професионалног односа (нпр. медицинска, адвокатска тајна).

Субјект дела

- У члану 240. и 141. КЗ, извршиоци су често лица која су законски или уговорно обавезана на чување тајне (запослени, лекари, адвокати).
- У члану 302. КЗ, извршилац може бити било ко ко хакерским методама приступи заштићеном систему.

Намера и мотив

- Нека дела (нпр. откривање пословне тајне) могу имати економски мотив, док други (приступ рачунару) могу бити из сајбер-криминалних побуда.
- Откривање државне тајне (члан 98) често има везе са шпијунажом или безбедносним претњама.

Казна

- Најтеже казне су предвиђене за кривична дела против државних тајни (члан 98) и кибер-криминал (члан 302).
- Одавање пословне и професионалне тајне обично има блаже казне, али могу бити значајне ако је штета велика.

Закључак

Иако сва ова дела имају заједнички елемент – заштиту поверљивих информација – они се разликују по објекту заштите, субјекту, мотивима и казним последицама. Правна регулатива настоји да осигура баланс између права на приватност, пословних интереса и националне безбедности.

Сличности и разлике између кривичног дела из члана 98. Закона о тајности података и кривичног дела шпијунаже из члана 315. Кривичног законика

Закон о тајности података и Кривични законик Републике Србије предвиђају кривична дела која се односе на повреду поверљивости тајних података, са циљем очувања националне безбедности и стабилности институција. Иако оба дела штите исту правну вредност – тајне податке – они се разликују по облику извршења, степену друштвене опасности и тежини казни.

Сличности

Предмет заштите:

Оба кривична дела штите тајне податке који су законом или подзаконским актима означени ознакама „ИНТЕРНО“, „ПОВЕРЉИВО“, „СТРОГО ПОВЕРЉИВО“ или „ДРЖАВНА ТАЈНА“.

Последице откривања:

Неовлашћено откривање таквих података може изазвати озбиљне последице по националну безбедност, посебно у области одбране, спољне политике, безбедносних служби или кључних економских система.

Казнене мере:

Оба дела су кажњива затворским казнама, с тим што се висина казне одређује у зависности од степена ознаке тајности, мотива и околности под којима је дело учињено.

Разлике

- **Намерност дела:** Члан 98. Закона о тајности података обухвата и дела почињена из нехата, док је члан 315. Кривичног законика резервисан искључиво за намерна и свесна понашања усмерена ка одавању података страним субјектима.
- **Мотив и циљ:** Док се у делу из члана 98. мотив може кретати од немара, личне користи или пропуста, дело шпијунаже подразумева свестан ангажман у корист стране државе, организације или службе, често у контексту обавештајног рада.

- **Степен казне:** Шпијунажа носи значајно теже казне, почев од 3 до 15 година затвора, па и више у отежавајућим околностима, док казне за неовлашћено откривање података варирају од 3 месеца до 15 година, у зависности од врсте података и начина извршења.
- **Област примене:** Члан 98. се примењује на ситуације унутар државног система – када су подаци откривени домаћем лицу, медијима или јавности. Члан 315. се односи искључиво на међународни аспект – када подаци бивају пренети или доступни страним државама, агентима или организацијама, што представља тежи облик угрожавања безбедности.

Оба кривична дела имају суштинску улогу у систему заштите тајних података. Члан 98. Закона о тајности података служи као правни инструмент за санкционисање унутрашњих пропуста, немара или корупције у руковању поверљивим подацима. Насупрот томе, члан 315. Кривичног законика санкционише издају и сарадњу са страним субјектима, што представља најтежи облик повреде националне безбедности. Отуда и значајне разлике у тежини казни, обиму одговорности и безбедносним последицама.

Прекршајна одговорност одговорног лица у органу јавне власти и руковаоца тајних података

Прекршајна одговорност у области заштите тајних података уређена је Законом о тајности података, са циљем обезбеђивања законитог и безбедног поступања са поверљивим информацијама. Закон предвиђа новчане казне за одговорна лица у органима јавне власти и руковоце тајних података у случају непоштовања прописаних обавеза. Овај текст систематизује најважније прекршаје, правне основе и последице које произлазе из њих.

1. Прекршајна одговорност одговорног лица у органу јавне власти (члан 99)

Одговорно лице у органу јавне власти подлеже новчаној казни од 5.000 до 50.000 динара ако изврши неку од следећих радњи супротних Закону:

Кључни прекршаји:

Неправилно означавање тајности:

- Означавање података као тајних иако очигледно не постоји претња за заштићене интересе (чл. 8 ст. 2 тач. 4).
- Употреба непримереног степена тајности за документ (чл. 11 ст. 2).

Незаконито преношење овлашћења:

- Преношење овлашћења за одређивање степена тајности на неовлашћено лице (чл. 9 ст. 3).
- Непоштовање процедура приликом одређивања тајности:
- Доношење одлуке о тајности без образложења (чл. 11 ст. 4).
- Пропуштање да се опозове тајност по истеку рока или након настанка околности које су условиле престанак тајности (чл. 17, 18, 19).

- Неспровођење периодичне процене оправданости тајности (чл. 22).

Неиспуњавање обавеза према надлежним органима:

- Непоступање по решењу Повереника или одлуци суда о опозиву тајности (чл. 25).
- Необавештавање надлежног органа о промени степена тајности (чл. 28).

Неадекватна заштита тајних података:

- Неспровођење прописаних општих и посебних мера заштите (чл. 32, 33).
- Непоштовање процедура за издавање и обраду сертификата приступа (чл. 42 ст. 3 и чл. 82).
- Недостављање података на начин прописан законом (чл. 46).

Невођење прописане евиденције:

- Пропуштање евидентирања издатих сертификата (чл. 82 ст. 1).
- Неулагање решења у кадровски досије (чл. 82 ст. 2).
- Неспровођење контролних механизма:
- Неорганизовање унутрашње контроле над системом заштите тајних података (чл. 84 ст. 1).
- Невођење регистра страних тајних података (чл. 94 ст. 2).

2. Прекршајна одговорност руковоаца тајних података (члан 100 у вези са чланом 34)

Према члану 100 Закона о тајности података, руковалац тајних података може бити новчано кажњен са 5.000 до 50.000 динара уколико не предузме прописане мере заштите тајних података, у складу са чланом 34.

Ко је руковалац тајних података?

Руковалац тајних података може бити физичко лице или организациона јединица унутар органа јавне власти, које је званично овлашћено да, у складу са Законом о тајности података („Службени гласник РС“, бр. 104/2009 и 99/2023), предузима мере заштите тајних података.

Руковалац има одговорност да:

- приступа, рукује, чува, обрађује, преноси или уништава тајне податке у оквиру службених дужности;
- управља системом заштите података у оквиру свог делокруга;
- предузима све прописане техничке, организационе и безбедносне мере у складу са унутрашњим актима и законом.

Руковалац се именује у складу са специфичностима пословања органа, као и природом података који се обрађују.

Лице овлашћено као руковалац тајним подацима не може истовремено обављати послове унутрашње контроле, како би се избегло потенцијално сукобљавање интереса и обезбедила независност надзора.

Обавезе руковооца према члану 34:

Члан 34 Закона прописује да је сваки руковалац тајних података дужан да поступа у складу са мерама заштите, а те мере подразумевају:

- Примена одговарајућих техничких, организационих и физичких мера заштите података (у складу са актом о безбедносним мерама који доноси орган).
- Спречавање неовлашћеног приступа, коришћења, измене или уништавања тајних података.
- Поштовање ограничења приступа на основу издатог безбедносног сертификата.
- Чување тајних података у прописаним просторима и средствима за заштиту, попут закључаних ормара, сефова или заштићених информационих система.
- Обавештавање надређених или одговорног лица у случају инцидента или сумње у угрожавање тајности података.

Примери прекршајних радњи:

Руковалац може извршити прекршај уколико:

- Остави поверљиви документ незаштићен на радном столу или га понесе кући без одобрења и мере заштите.
- Пошаље тајни податак преко незаштићене електронске поште, мимо прописаних канала.
- Омогући неовлашћеном лицу увид у тајни документ, макар и ненамерно.
- Не закључа просторију или ормар у ком се чувају тајни подаци, остављајући их изложене.
- Уништи тајни документ на начин који није у складу са прописаном процедуром (нпр. бацањем у корпу уместо дробљења или спаљивања).
- Не пријави губитак или могуће откривање тајног податка, чиме онемогућава правовремену реакцију надлежног органа.

Последице: Овакве радње, иако често последица немара, директно доводе до угрожавања безбедности поверљивих информација, и самим тим угрожавају заштићене интересе Републике Србије. Због тога закон предвиђа прекршајну санкцију у циљу превенције, али и повећања свести о важности поштовања безбедносних мера.

Прекршајна одговорност у систему заштите тајних података

Прекршајна одговорност у области заштите тајних података има пре свега превентивну и дисциплинску функцију. Њена сврха је да:

- осигура доследну примену закона;
- унапреди безбедносну културу и свест у институцијама јавне власти;

- јасно дефинише последице за непоштовање утврђених правила и процедура.

Лица која у свом раду приступају тајним подацима – било као запослени, руководиоци или руковооци – морају поступати са високим степеном пажње, одговорности и законске дисциплине. Свако одступање од прописаних мера и процедура може довести до повреде тајности података, чиме се директно угрожавају сигурност система, поверљивост информација и национални интереси.

Доследна примена прекршајних одредби доприноси:

- јачању правне сигурности;
- транспарентности у поступању са подацима;
- изградњи одговорног и поузданог безбедносног система.

Напомена: Утицај прекршајне осуде на безбедносну проверу

Према критеријумима за безбедносну проверу, постојање правноснажне прекршајне осуде за дела предвиђена Законом о тајности података („Службени гласник РС“, бр. 104/2009 и 99/2023) представља:

апсолутну сметњу за издавање безбедносног сертификата.

У том смислу, лице које је осуђивано за прекршај из области заштите тајних података не може добити приступ тајним подацима, без обзира на испуњеност осталих услова. То правило служи као механизам заштите система и очувања интегритета органа који рукују поверљивим информацијама.

Радно-дисциплинска одговорност због непоштовања процедура у раду са тајним подацима

1. Увод: Обавезе у раду са тајним подацима

Сва лица која у оквиру службених дужности приступају, рукују, обрађују, преносе или чувају тајне податке, обавезна су да поштују следеће прописе и стандарде:

- Закон о тајности података („Сл. гласник РС“, бр. 104/2009)
- Интерне прописе и безбедносне процедуре институције
- Етичке кодексе (државних службеника, полицијских службеника, припадника војске)
- Законе који уређују дисциплинску одговорност у јавном сектору

Непоштовање ових обавеза представља повреду службене дужности и повлачи за собом радно-дисциплинску, а у тежим случајевима и кривичну одговорност.

2. Правни основ радно-дисциплинске одговорности

2.1. Закон о тајности података

Према члану 34. овог закона, руковалац тајним подацима обавезан је да примењује прописане мере заштите. Непоступање представља основ за покретање дисциплинског поступка.

Примери повреда:

- Остављање поверљивих докумената без надзора
- Непоштовање поступка класификације/декласификације
- Непажљиво руковање или откривање поверљивих информација
- Пропусти у физичкој или електронској заштити података

2.2. Закон о државним службеницима

Члан 103: Државни службеник дужан је да чува тајне податке до којих дође у обављању послова.

Члан 107: Кршење правила о тајним подацима представља тежу повреду службене дужности.

Могуће дисциплинске мере:

- Упозорење или опомена
- Новчана казна
- Премештај на мање одговорну позицију
- Раскид радног односа

2.3. Закон о Војсци Србије

Војна лица обавезна су да поштују прописане безбедносне процедуре, у складу са упутствима Генералштаба и Министарства одбране.

Последице повреда:

- Дисциплинске казне (укор, смањење чина)
- Разрешење дужности
- У тежим случајевима: покретање кривичног поступка (чл. 369. КЗ – одавање војне тајне)

2.4. Закон о полицији

Члан 188: Полицијски службеник дужан је да чува тајне податке и након престанка службе.

- Непоштовање обавеза може довести до:
- Губитка безбедносног сертификата
- Раскида радног односа

3. Етички кодекси и професионалне обавезе

Етички кодекси јавних службеника, припадника полиције и војске посебно истичу:

- Обавезу поштовања нивоа тајности
- Чување интегритета поверљивих информација
- Пријављивање безбедносних инцидената

Нарушавање етичких принципа може довести до:

- Губитка поверења за рад са тајним подацима
- Искључења из осетљивих или поверљивих задатака

4. Последице непоштовања процедура

Ниво повреде	Мере одговорности
Блажи прекршаји	Упозорење, додатна обука, новчана казна
Озбиљнији пропусти	Премештај, смањење платног разреда
Тешке повреде	Одузимање сертификата, отказ, кривични поступак

5. Превенција и одговорност

Рад са тајним подацима захтева висок ниво професионалности, дисциплине и личне одговорности. Организације су дужне да:

- Обезбеде редовну едукацију и обуку запослених
- Уведу и примењују јасне контролне механизме
- Спровode дисциплинске мере доследно и правовремено

Запослени који не поштује прописане обавезе ризикује не само радно-дисциплинске, већ и правне и безбедносне последице. Стога је неопходно поступати у складу са законом, интерним правилима и етичким стандардима, како би се очувала поверљивост и безбедност тајних података.

Одговорност за накнаду штете у раду са тајним подацима

1. Правни оквир за одговорност за штету

Руковање тајним подацима подлеже строгој правној регулативи која, поред кривичне и радно-дисциплинске, предвиђа и грађанскоправну одговорност за накнаду штете. Та одговорност проистиче из:

- Закона о облигационим односима (чл. 154–200)
- Закона о тајности података
- Посебних закона који уређују рад државних органа, војске и полиције

2. Одговорност запослених и државних службеника

2.1. Лична одговорност

Свако лице које кршењем процедура изазове штету приликом руковања тајним подацима може сносити личну одговорност. Према ЗОО, услови за одговорност су:

- Незаконита радња (пропуст или активност)
- Настанак штете
- Узрочна веза између радње и штете

Примери:

- Неовлашћено откривање тајних података
- Губитак или крађа носача података услед непажње
- Неспровођење прописаних мера заштите

2.2. Солидарна одговорност државе и запосленог

Ако је штета настала у оквиру службених активности, одговорност може бити подељена између запосленог и државе (или јавне установе). Држава има право на регресни захтев ако је запослени поступао:

- Са тежом непажњом
- Намерно
- У супротности са утврђеним процедурама

3. Одговорност правних лица

3.1. Јавни органи и институције

Државни органи могу бити одговорни за штету насталу услед:

- Неправилног доношења одлука о степену тајности
- Недовољне безбедносне заштите
- Недовољне контроле над запосленима

Пример: Ако дође до цурења тајних података услед пропуста у заштити ИТ система, одговоран је орган који је систем одржавао.

3.2. Приватна правна лица

Приватне фирме ангазоване у пословима са тајним подацима (нпр. обезбеђење, ИТ подршка) одговарају ако:

- Не поштују уговорне обавезе о заштити података
- Немају адекватне безбедносне протоколе
- Толеришу кршење процедура од стране својих запослених

Пример: Ако ИТ фирма занемари мере заштите сервера, па дође до хаковања и цурења података – може бити тужена за накнаду штете.

4. Посебни случајеви у државним службама

4.1. Војска и безбедносне службе

- Војна лица одговарају лично ако крше прописе
- Министарство одбране сноси одговорност за системске пропусте

4.2. Полиција

- Полицијски службеници одговарају за злоупотребу података
- Полицијска управа може бити солидарно одговорна

4.3. Државна управа

- Запослени одговарају за штету проузроковану непажњом
- Орган може бити одговоран за недостатак унутрашњих контрола

5. Врсте штете и начин накнаде

Штета може бити:

- Имовинска: директни финансијски губици
- Неимовинска: нарушење угледа, психолошке последице

Накнада се одређује:

- У складу са обимом и природом штете
- Може обухватити и изгубљену добит
- У случају грубе непажње – могућа је и казнена надокнада

6. Превентивне мере и смањење ризика

Ради избегавања одговорности, неопходно је:

- Успоставити јасне и доследне процедуре
- Редовно обучавати запослене
- Водити евиденцију приступа и руковања подацима
- Спровоодити контролне механизме и ревизије

7. Одговорност за накнаду штете у раду са тајним подацима обухвата:

- Личну одговорност запослених
- Солидарну одговорност државе и јавних институција
- Одговорност приватних партнера

Правилно руковање тајним подацима, доследно спровођење безбедносних мера и континуирана едукација представљају кључ заштите од правних последица. Сви који

учествују у процесу морају бити свесни својих обавеза и могућих последица непоштовања процедура.

Допринос организације у настанку штетног догађаја у раду са тајним подацима и утицај на одговорност

Рад са тајним подацима захтева висок ниво одговорности и поштовања прописаних мера безбедности, како појединаца, тако и организација. У случају настанка штетног догађаја – било да се ради о открићу, неовлашћеном коришћењу или губитку поверљивих информација – анализира се допринос како физичких лица (службеника или запослених), тако и организације у целини. Овај приступ има значајан утицај на одговорност у различитим правним сферама: кривичној, прекршајној, радно-дисциплинској и у поступку накнаде штете.

Организациона одговорност

Организација је дужна да обезбеди одговарајуће услове за заштиту тајних података, укључујући прописане процедуре, техничке и организационе мере, као и континуирану обуку запослених. Недовољна контрола, неправилна примена прописа, лоша безбедносна култура или недостатак надзора могу допринети настанку штетног догађаја.

Процедурални пропуси

Недостатак јасно дефинисаних процедура, неодговарајуће мере контроле приступа, или непоштовање принципа „потребно да зна“ од стране организације могу представљати основ за утврђивање њеног доприноса.

Технички и кадровски пропуси

Организација може бити одговорна ако није обезбедила адекватну заштиту инфраструктуре (нпр. заштита сервера, физичка заштита просторија) или ако није правилно одабрала и обучила кадрове који рукују тајним подацима.

Утицај на одговорност физичких и правних лица

Кривична одговорност

Физичка лица могу бити кривично одговорна за радње које доводе до неовлашћеног открића или злоупотребе тајних података. Организација, као правно лице, може бити санкционисана по основу одредби о кривичној одговорности правних лица, уколико је утврђено да је недостатак њених мера допринео почињењу кривичног дела.

Прекршајна одговорност

Према Закону о заштити тајних података и другим релевантним прописима, како појединци тако и организације могу бити кажњени за прекршаје, као што су непоштовање мера безбедности или неадекватна заштита података. Ово укључује новчане казне и друге административне мере.

Радно-дисциплинска одговорност

Запослени који не поступају у складу са прописаним обавезама у раду са тајним подацима могу бити предмет радно-дисциплинског поступка, што може довести до упозорења, суспензије или отпуштања. Организација је дужна да обезбеди јасна правила и дисциплинске мере.

Одговорност у поступку накнаде штете (Закон о облигационим односима)

Организација може бити одговорна за штету насталу због немара у обезбеђењу тајних података, а појединци могу бити сукцесивно одговорни ако се утврди да је њихова радња или пропуст директно изазвао штету. Накнада штете може обухватати материјалну и нематеријалну штету.

Допринос организације у настанку штетног догађаја у раду са тајним подацима има пресудан утицај на одговорност како појединаца, тако и саме организације. Законски оквир и унутрашње процедуре морају бити конципирани тако да минимизирају ризике, обезбеде јасну подјелу одговорности и омогуће ефикасан систем санкција и превенције. Само интегрисаним приступом, у коме организација и појединци делују у сагласности са прописима и безбедносним стандардима, може се успешно заштитити национална безбедност и интегритет поверљивих података.

Закључна разматрања: Тајни подаци, јавна политика и безбедносна политика као стубови националне безбедности Републике Србије

Кључна улога тајних података у националној безбедности

Тајни подаци представљају основни ресурс и средство у очувању и остваривању националне безбедности. Правилна заштита поверљивих информација осигурава континуитет и ефикасност државних функција, штити интересе Републике Србије и спречава потенцијалне претње које могу проистећи из злоупотребе или открића осетљивих података.

Јавна политика као оквир одговорности и транспарентности

Усмерена кроз јасне прописе и стратешке документе, јавна политика регулише поступање са тајним подацима и дефинише одговорности свих актера, посебно носилаца највиших државних функција. Политичка одговорност у раду са тајним подацима, заснована на јавном поверењу и моралном интегритету, игра кључну улогу у очувању легитимитета власти и поверења грађана.

Безбедносна политика као гарант системске стабилности

Безбедносна политика Републике Србије интегрише мере и процедуре заштите тајних података као неизоставни део ширег система одбране и безбедности. Усаглашеност са међународним стандардима (као што су NATO и EU) и билатералним споразумима јача капацитет Србије да одговори на савремене безбедносне изазове и омогућава поверење међународних партнера.

Интегритет, одговорност и континуирана едукација

Успостављање јасних стандарда у заштити тајних података подразумева одговорност појединаца и институција, од редовних службеника до највиших званичника. Континуирана стручна обука и ажурирање знања неопходни су за превенцију пропуста и инцидента који могу угрозити безбедност државе.

Превенција као кључни принцип

Политичка и дисциплинска одговорност, као и систем санкција, делују превентивно, смањујући ризик од злоупотребе и небригом по питању тајних података. Овај приступ омогућава брзу реакцију и отклањање безбедносних претњи у најранијој фази.

Синергија институција и међународна сарадња

Систем заштите тајних података не може деловати изоловано. Неопходна је координација свих безбедносних и државних органа, као и ефикасна сарадња са међународним партнерима, како би се обезбедила комплетна, свеобухватна и ефикасна заштита националних интереса.

Укратко, тајни подаци, јавна политика и безбедносна политика представљају темељне стубове националне безбедности Републике Србије. Само кроз доследно поштовање законских норми, политичку одговорност и стално унапређење безбедносних мера могу се осигурати стабилност, суверенитет и поверење у државне институције.

О АУТОРУ



Проф. др Горан Матић

Директор Канцеларије Савета за националну безбедност и заштиту тајних података Републике Србије, ванредни професор за област безбедност Универзитета УНИОН – „НИКОЛА ТЕСЛА” и стални судски вештак за безбедност информација.

Учествовао је у процесу израде предлога више закона, Стратегије за супротстављање и борбу против тероризма, Стратегије националне безбедности и Стратегије одбране и у раду Радних група Владе Републике Србије за имплементацију акционих планова за поглавља 10, 24 и 31 за приступање Републике Србије ЕУ.

Од 2015. до 2019. године руководио је Сталном мешовитом радном групом за борбу против тероризма (СМРГ) – формиране одлуком Бироа за координацију рада служби безбедности, од 2019/2021. године обављао и дужност заменика националног координатора Националног координационог тела (НКТ) за спречавање и борбу против тероризма Републике Србије.

У оквиру међународне сарадње Републике Србије на плану заштите тајности података учествовао је као шеф делегације у преговорима за потписивање 14 међународних споразума и био потписник више споразума које је Р. Србија потписала са међународним телима и страним државама у области заштите тајних података. Такође, са Мисијом ОЕБС-а у Београду учествовао је у више пројеката око заштите тајних података, сајбер безбедности и обраде и заштите личних података у сектору безбедности и одбране.

Од 2012. године учествује у раду Форума директора националних безбедносних органа за заштиту тајних података земаља Југоисточне Европе (SEENSA), као и у оквиру Иницијативе „6S” која окупља директоре националних безбедносних органа земаља региона.

Аутор је више објављених научних и стручних радова и учесник више научних конференција, као и научне монографије „Политички деликти – атентат и побуна” и коаутор књиге „Тактика и методика деловања обавештајно-безбедносних служби” у издању Медија центра Одбрана у Београду, и „Основи безбедности” у издању Факултета за пословне студије и право у Београд

Предавач је на основним академским студијама Војне академије Универзитета одбране и на Факултету за пословне студије и право Универзитета Никола Тесла Унион у Београду.

Гостујући је предавач на Факултету безбедности и Факултету организационих наука Универзитета у Београду, као и на Криминалистичко-полицијском универзитету, Академији за националну безбедност и на Високим студијама безбедности и одбране при Универзитету одбране у Београду. Поред тога предавач је на кратким струковним студијама на Факултету безбедности: "Заштита тајних података и пословне тајне" и "Заштита личних података" од 2022. године. Био је гостујући предавач на мастер студијама Универзитета у Београду – Тероризам, организовани криминал и безбедност до 2024. године

Акредитовани је предавач Националне академије за јавну управу. Учествоје је у раду посебних стручних тела те институције, и то као члан Сталне програмске комисије за електронску управу и дигитализацију (2022-2023) и Сталне програмске комисије за јавну управу (2023-2024).

Члан је Испитне комисије за државни испит (високо образовање) државних службеника и за комуналне милиционере у оквиру министарства државне управе и локалне самоуправе.

Председник је Савета „САМКБ – Српске асоцијације менаџера корпоративне безбедности” у Београду; члан удружења „ИТ вештак” у Београду и „Удружења за међународно кривично право” у Београду. У Привредној комори Србије и Привредној комори Београда више година изводи едукације на тему корпоративне безбедности и обраде и заштите података.