УДК 351.083.8(73:4-672EU)"20"
DOI: 10.5937/pnb31-65266
Оригинални научни рад

Политика националне безбедности
Година XVII вол. 31
Бр. 1/2026
стр. 1-27

Горан Матић*

Факултет за пословне студије и право, Универзитет „Унион – Никола Тесла”, Београд, Република Србија

ПРЕКОМЕРНА ТАЈНОСТ У ДЕМОКРАТИЈАМА: БИРОКРАТСКИ РЕФЛЕКС ИЛИ БЕЗБЕДНОСНА ИЛУЗИЈА?

Сажетак

Систематска прекомерна класификација информација унутар безбедносних апарата Сједињених Америчких Држава, Европске уније и кључних НАТО савезника представља структурну аномалију у оквиру либералних демократија. Кроз компаративну анализу, рад идентификује да је кључни покретач овог феномена разлика између концепта *security secrecy* (заштите стварних безбедносних капацитета) и концепта *political secrecy* (заштите институција од одговорности). Истраживање показује да, упркос различитим правним традицијама, сви анализирани системи деле заједничке структурне обрасце: *defensive classification* као стратегију минимизације ризика, асиметричне подстицаје који санкционишу отвореност и слабост механизама спољашњег надзора. Последице овакве праксе обухватају ерозију јавног поверења, отежану сарадњу унутар НАТО савеза и смањену ефикасност у процесима доношења одлука. У раду се закључује да решења захтевају промену парадигме – од логике „потребе да се сакрије” (*need to conceal*) ка принципу „права да се зна” (*the right to know*), заснованом на претпоставци отворености као основи демократске легитимности. Као кључни оперативни кораци истичу се увођење обавезног утврђивања рока истека

* Имејл адреса: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797.

важења класификације (*sunset* клаузула), јачање независности и надлежности надзорних тела, као и хармонизација стандарда на нивоу НАТО и Европске уније ради спречавања злоупотребе тајности у сврху управљања информацијама, а не заштите безбедности.

Кључне речи: прекомерна класификација, тајност, обавештајна заједница, демократска одговорност, право на приступ информацијама, Сједињене Америчке Државе, Европска унија, НАТО, компаративна анализа.

УВОДНА РАЗМАТРАЊА

Прекомерна класификација није административна грешка она представља системски избор. У демократијама заснованим на принципима одговорности и транспарентности, масовно означавање докумената као „тајних", без јасних и проверљивих критеријума, трансформише тајност из изузетка у правило. Последица такве праксе није повећана безбедност, већ ослабљен надзор и фрагментирана сарадња међу савезницима.

Овај рад полази од тезе да је прекомерна класификација један од најозбиљнијих, али истовремено и најмање регулисаних изазова савремених безбедносних система. Док се јавне и стручне расправе интензивно фокусирају на вештачку интелигенцију, кибернетичку одбрану и хибридне претње, пракса рутинског затварања информација остаје у великој мери занемарена – иако директно подрива демократске вредности које те државе формално заступају.

Пре анализе специфичних националних система, неопходно је указати на универзалне оквире међународних организација. Иако Уједињене нације немају јединствен систем класификације, њихови органи су током времена артикулисали принципе равнотеже између безбедности и транспарентности. Смернице Организације Уједињених нација за образовање, науку и културу о слободи информација и националној безбедности (УНЕСКО) (United Nations Educational, Scientific and Cultural Organization 2014) захтевају да свака рестрикција буде законита, неопходна и пропорционална у демократском друштву. Организација за европску безбедност и сарадњу је у Истанбулском документу (*The*

OSCE Istanbul Document) из 1999. године (Organization for Security and Cooperation in Europe [OSCE] 1999) нагласила да тајност не сме бити изговор за избегавање одговорности.

Ови универзални стандарди представљају нормативни темељ на којем су касније изграђени детаљнији и операционализовани инструменти укључујући Цвана принципе о националној безбедности и праву на информације (*Tshwane Principles on National Security and the Right to Information*) из 2013. године (Open Society Foundations 2013), Тромсе конвенцију Савета Европе о приступу званичним документима из 2009. године (Tromsø Convention 2009), евалуационе механизме Групе држава против корупције при Савету Европе (*Group of States against Corruption – GRECO*) (Council of Europe 2018), нормативне оквире Европске уније (ЕУ) у форми Одлуке Савета 2013/488/ЕУ о безбедносним правилима за заштиту тајних података ЕУ (Decision 2013/488) и Организације Северноатлантског уговора у форми НАТО (*North Atlantic Treaty Organization*) Глосара термина и дефиниција, издање AAP-06 (*Glossary of Terms and Definitions, AAP-06 edition*) (NATO Standardization Office 2021). Заједничка порука свих ових аката је јасна: легитиман безбедносни интерес не сме надјачати демократске захтеве транспарентности, парламентарног надзора и јавног интереса. Ипак, компаративна анализа показује да јаз између нормативне усаглашености и оперативне праксе остаје централни проблем прекомерне класификације у савременим демократијама.

Иако се праксе разликују, међународни и регионални оквири показују кохерентност у дефинисању принципа одговорне класификације. Група држава против корупције при Савету Европе у више циклуса истиче да прекомерна тајност подрива антикорупцијске механизме и надзор, нарочито у јавним набавкама и управљању ресурсима. НАТО глосар и Безбедносна правила ЕУ инсистирају на пропорционалности, образложености и временском ограничењу. Ови стандарди показују консензус да тајност мора бити изузетак, а не правило – консензус који, као што ће анализа показати, често остаје на нивоу теорије, а не праксе.

У основи феномена лежи парадокс демократије и тајности: либерална демократија, како је концептуализују Дал (*Robert Dahl*) и Хабермас (*Jürgen Habermas*), захтева отвореност као услов легитимности политичке воље (Dahl 1989; Habermas 1996). Ипак,

унутар тих система развијају се апарати чија функционалност почива на контролисаној затворености што ствара напетост између права на знање и потребе за тајношћу (Fenster 2006). Тајност у обавештајним институцијама није само процедурални алат, већ постаје део организационе културе „основна претпоставка" која обликује идентитет служби и понашање припадника (Schein 2010). Тако се тајност трансформише из техничког избора у нормативни императив, стварајући услове за системску прекомерност.

Анализа обухвата три аналитичка нивоа: САД, као глобалног хегемона са најразвијенијим обавештајно-безбедносним апаратом; ЕУ као наднационални ентитет са слојевитим и фрагментираним режимима тајности; и три европске државе – Уједињено Краљевство, Француску и Немачку – које карактеришу различити приступи тајности, у распону од британске „културе службе" до немачког наслеђа Штазија (*Stasi)*, као главне тајне обавештајне службе Источне Немачке.

Теоријски оквир рада комбинује теорију бирократског понашања (Wilson 1989), у оквиру које се истиче избор стратегије минималног ризика, и теорију демократске одговорности (Fenster 2006), која инсистира на томе да тајност мора представљати изузетак, а не правило у функционисању демократских институција. Додатно, рад се ослања на критичку литературу о феномену „пропусног Левијатана" (*Leaky Leviathan)* (Pozen 2013) и институционалној динамици прекомерне класификације (Aftergood 2023).

Методолошки приступ заснива се на упоредној анализи случајева и укључује разматрање следећих материјала: званичних извештаја Врховне ревизорске институције САД (*Government Accountability Office – GAO)*, Европског омбудсмана (*European Ombudsman*) и Одбора немачког Бундестага за контролу служби безбедности (*Parlamentarisches Kontrollgremium – PKGr*); релевантне академске литературе аутора, као што су Стивен Афтергуд *(Steven Aftergood)* и Дејвида И. Поузена (*David E. Pozen*), истраживачких пројеката Националног безбедносног архива при Универзитету „Џорџ Вашингтон" *(National Security Archive at George Washington University*), као и анализу кључних афера, као што су Пентагонски документи (*Pentagon Papers*), афера Сноуден (*Snowden affair),* немачке Савезне обавештајне службе (*Bundesnachrichtendienst – BND).*

Структура рада прати логику систематског поређења: друго поглавље посвећено је анализи праксе у САД, треће ЕУ, четврто доноси упоредну анализу три одабране европске државе, док пето поглавље пружа синтетички закључак о могућим путевима ка успостављању одговорне транспарентности.

Истраживање се фокусира искључиво на компаративну анализу система САД, ЕУ и кључних НАТО савезника. Систем заштите тајних података у Србији није предмет анализе овог рада.

Иако се НАТО помиње у наслову и ширем контексту рада као оквир за дељење тајних информација међу западним демократијама, рад не анализира његов систем класификације (нпр. AAP-06, Cosmic Top Secret). Разлог је методолошки: НАТО нема сопствене обавештајне капацитете нити производи оригиналне тајне податке, већ делује као механизам размене информација насталих на националном нивоу. Сходно томе, прекомерна класификација у контексту НАТО одражава праксе држава чланица пре свега САД, Уједињеног Краљевства, Француске и Немачке – које су обухваћене анализом. Додатно, НАТО стандарди, укључујући принципе „потребно је да зна" (*need-to-know*) и „потребно је поделити" (*need-to-share*), већ су инкорпорирани у националне системе и оквир ЕУ, па њихово разматрање кроз призму држава чланица пружа адекватан аналитички увид у функционисање тајности у Трансатлантском савезу.

Унутар дискурса о прекомерној тајности могу се разликовати три приступа. Први, критички, својствен организацијама цивилног друштва и актерима права на приступ информацијама, усмерава се на злоупотребе и последице по транспарентност и демократску контролу. Други, одбрамбени, карактеристичан за органе власти и безбедносне структуре, полази од потребе за очувањем постојећих пракси и наглашава ризике које би смањење тајности могло произвести по безбедност, стабилност или међународне обавезе. Трећи, академски, заузима неутралну позицију: кроз анализу нормативног оквира, упоредне праксе и примене настоји да идентификује слабости система и могућности унапређења.

Овај рад припада трећем, академском приступу. Његов циљ није да заузме страну у постојећим полемикама, већ да понуди аналитички оквир који омогућава разумевање зашто се проблеми у области заштите тајних података понављају, како различити

приступи обликују праксу и на који начин је могуће постићи функционалнију равнотежу између безбедности, одговорности и јавног интереса.

Наслов рада поставља дилему: да ли је прекомерна класификација последица бирократског рефлекса – рационалног, али уско инструменталног одговора на перципиране ризике – или безбедносна илузија: стратегија која прикрива политичку непрозирност, избегавање одговорности и управљање јавним перцепцијама под изговором националне безбедности? Анализа показује да су ове две опције у пракси често нераздвојиве: бирократски рефлекс постаје механизам којим се производи и одржава безбедносна илузија. Када се страх од грешке, каријерни ризик и институционална инерција систематизују као „стратегија минималног ризика" (*minimum-risk strategy*), тајност престаје да буде техничка мера и постаје инструмент контроле информација, а не заштите безбедности.

ТЕОРИЈСКЕ ПАРАДИГМЕ: ТАЈНОСТ ИЗМЕЂУ СУВЕРЕНИТЕТА И ДЕМОКРАТСКОГ ИЗУЗЕТКА

Пре компаративне анализе националних система, неопходно је разјаснити теоријске дилеме односа тајности и демократије. Парадокс либералне демократије лежи у потреби за отвореношћу као извором легитимности, али и за тајношћу као условом функционалности безбедносних апарата (Dahl 1989; Habermas 1996). Овај однос може се разумети кроз две супротстављене теоријске традиције.

Суверенитетска парадигма – од Жана Бодена (*Jean Bodin*) до Карла Шмита (*Carl Schmitt)* – третира тајност као атрибут суверене власти. Код Бодена, суверенитет подразумева способност државе да самостално одлучује о питањима од виталног значаја, укључујући право да одређене информације задржи ван домашаја јавности. Шмит овај однос радикализује тврдњом да је „суверен онај ко одлучује о изузетку" (Schmitt [1922] 2005). Изузетак функционише изван процедура јавности и транспарентности, што тајност чини предусловом ванредног одлучивања. У савременим безбедносним државама ова логика је институционализована: извршна власт задржава контролу над тајним подацима, полазећи

од претпоставке да је тајност услов ефикасног деловања у кризним ситуацијама.

Демократска парадигма темељи се на Хабермасовом начелу да је јавност основ демократске легитимације власти. Јавна расправа и приступ информацијама омогућавају контролу политичке моћи и трансформишу „наративну власт" у „дискурзивну одговорност" (Habermas 1996). Тајност није правило, већ одступање које захтева строго ограничено оправдање. У демократском поретку дозвољена је искључиво као контролисано и привремено одступање ради заштите конкретног и легитимног интереса. Проблем настаје када се изузетак претвори у правило, а јавност у секундарну вредност.

Правно гледано, тајност није обавезујућа норма (*ius cogens*) нити апсолутно право државе. Она је изузетак у односу на правило транспарентности, али строго уређен законом. Тајност је облик административне дискреције са јасно утврђеним правним границама. Органи власти морају сваку одлуку о тајности: 1) образложити, 2) засновати на процени штете, 3) временски ограничити и 4) учинити подложном контроли. Овај оквир, заједнички Цвана принципима (Open Society Foundations 2013) и Тромсе конвенцији, чини нормативни темељ одговорне класификације.

Кључна аналитичка разлика лежи у дистинкцији између заштите стварних безбедносних капацитета (*security secrecy*) и „заштите институција од одговорности" (*political secrecy*). Прва се односи на заштиту стварних безбедносних капацитета (извори, методе, оперативни планови, сајбер одбрана), док друга служи заштити институција и носилаца власти од одговорности, надзора или јавне критике. Теоријска теза која произилази из ове дистинкције гласи: прекомерна тајност (*overclassification*) често је политички, а не безбедносни проблем. Она је последица ширења изузетка и асиметрије моћи унутар институција, а не вишка безбедносне пажње.

Ова дистинкција постаје релевантна при анализи образаца прекомерне класификације. Политичка тајност у пракси се манифестује кроз: 1) масовно означавање целих докумената као тајних, иако је осетљив само део; 2) ретроактивно проглашавање тајности након што су информације постале јавне – као облик

накнадне цензуре; 3) очување „застарелих тајни" без редовне ревизије ризика; и 4) проширење појма „националног интереса" на комерцијалне или административне податке. Ови обрасци, различито формализовани, препознатљиви су у свим системима – од САД до Немачке – што указује на структурну динамику, а не на изоловане институционалне грешке.

Савремени безбедносни оквири све више преиспитују традиционални модел *потребно је да зна* као искључиви принцип. У доба хибридних претњи, масовног надзора и комплексних изазова, овај рестриктивни приступ показује ограничења. Зато се афирмише принцип *потребно је поделити* – идеја да информације морају бити доступне актерима који их могу оперативно искористити за колективну одбрану, чак и ако нису директно укључени у њихово стварање. Ова еволуција није супротстављање, већ надоградња: принцип *потребно је да зна* штити од злоупотребе, а принцип *потребно је поделити* обезбеђује ефикасност и отпорност. Дихотомија је институционализована у Безбедносним правилима ЕУ и Глосару НАТО термина и дефиниција, издање AAP-06, где оба приступа представљају комплементарне принципе.

Овај теоријски оквир представља аналитичку „мапу" за испитивање конкретних система. Он омогућава да се разликује легитимна безбедносна тајност од политичке злоупотребе, идентификује тренутак када се „изузетак" претвара у „правило" и процени да ли се тајност користи као инструмент заштите или контроле. Са овим концептуалним алатима, анализа се усмерава ка компаративном разматрању три нивоа: САД као глобалне парадигме, ЕУ као наднационалног експеримента и кључних НАТО савезника са њиховим различитим традицијама. Ова дихотомија је посебно релевантна у контексту савезничких организација, као што је НАТО, у којима се принципи *need-to-know* (заштита од отицања информација) и *need-to-share* (обезбеђивање колективне одбране) налазе у сталном напону. Глосар НАТО термина и дефиниција, издање AAP-06 експлицитно препознаје ову дихотомију, али, као што показује пракса, технички стандарди сами по себи често нису довољни да превазиђу културне и политичке препреке дељењу информација.

Сједињене Америчке Државе: парадигма културе тајности

САД представљају најразвијенији, али и најпроблематичнији пример системске прекомерне класификације. Иако се описују као „отворена демократија", САД функционишу под режимом тајности без преседана у модерној историји. Према проценама Федерације америчких научника (*Federation of American Scientists)*, амерички безбедносни апарат годишње класификује преко 50 милиона страница докумената – бројка која, иако нижа него у врхунцу Хладног рата, и даље указује на масовну примену принципа „класификуј све што можеш" (Aftergood 2023). Ова пракса је утемељена у административној култури, правном оквиру и институционалним подстицајима који награђују предострожност, а кажњавају отвореност.

Основни правни акт који је деценијама регулисао класификацију у САД била је Уредба 13526 (*Executive Order 13526*) (Federal Register 2009). Она дефинише три нивоа класификације – поверљиво (*Confidential*), строго поверљиво (*Secret*) и државна тајна (*Top Secret*) – и захтева класификацију само ако њено неовлашћено откривање може „очигледно угрозити националну безбедност". На папиру оквир делује разумно, али у пракси не постоји ефикасан механизам за проверу оправданости. Одлуку доноси појединачни службеник, често без адекватне обуке, надзора или последица у случају прекомерне тајности. Исти акт предвиђа аутоматску декласификацију након 25 година, али дозвољава неограничене изузетке „због трајних безбедносних интереса". Последица је да више од 80% докумената старијих од 25 година остаје класификовано (Public Interest Declassification Board 2022), па „аутоматска" декласификација постаје бирократска фикција. У октобру 2022. администрација председника Џоа Бајдена (*Joe Biden*) донела је Уредбу 14040 (*Executive Order 14040*) (Federal Register 2022), која је требало да представља „реформу за нову еру". Акт настоји да ублажи хроничне слабости система: уводи стандарде за „дигиталну компатибилност" класификованих података, повећава улогу Националне архиве у координацији декласификације и подстиче технологије за „масовну декласификацију". Међутим, како истиче Поузен (Pozen 2023), Уредба 14040 не решава кључни

проблем: не ограничава дискрецију службеника у класификацији нити уводи санкције за неоправдану прекомерност. Реформа остаје унутар логике „технократског управљања" – унапређује процесе, али не преиспитује културу тајности која их производи.

Постоје три кључна фактора који објашњавају опстанак прекомерне класификације у САД:

1) Култура тајности – наслеђе Хладног рата и „рата против тероризма" створило је менталитет у коме је „сигурније затворити него објавити". Како је један бивши директор Централне обавештајне агенције (*Central Intelligence Agency – CIA*) изјавио пред Конгресом: „Нико никада није изгубио посао зато што је прекорачио у тајности" (US Congress 2016; Aftergood 2023; Schein 2010). Тајност је постала део професионалног идентитета, док се отвореност перципира као ризик.

2) Страх од одговорности – службеници знају да ће бити санкционисани ако нешто открију, али готово никада ако неоправдано сакрију. Случајеви Челси Менинг (*Chelsea Manning*) и Едварда Сноудена (*Edward Snowden*) показали су да цурење информација, чак и у јавном интересу, води затвору или егзилу. Како примећује Фенстер (Fenster 2006), систем ствара асиметричне подстицаје који поткопавају демократску одговорност.

3) Бирократска инертност – процес декласификације је спор, скуп и технички захтеван. Уместо систематске ревизије, агенције продужавају статус тајности „за сваки случај". То је пример „стратегије минималног ризика" (Wilson 1989): када су трошкови грешке у корист отворености високи, а у корист тајности занемарљиви, избор је увек – тајност.

Два примера посебно илуструју последице прекомерне тајности:

1) Рат у Ираку (2003–2011) – док су медији и Конгрес расправљали о „оружју за масовно уништење", кључни извештаји обавештајних служби који су указивали на недостатак доказа били су класификовани. Тек касније постало је јасно да је тајност онемогућила информисану демократску дебату. Како је закључила Комисија за истраживање терористичког напада 11. септембра 2001, „тајност није штитила националну безбедност – она је прикривала неспремност и лош суд" (The National Commission on Terrorist Attacks Upon the United States [9/11 Commission] 2004, 417).

2) Програми масовног надзора НСА (*National Security Agency – NSA*) – како је показао случај Едварда Сноудена (*Edward Snowden*) 2013, сегменти програма *PRISM* и *UPSTREAM* били су класификовани не због оперативне осетљивости, већ ради прикривања обима надзора над грађанима. Последица је била криза поверења између државе и друштва. Како истиче Метју Конели (*Matthew Connelly*), „када се чак и судске одлуке класификују, демократија губи свој рефлексивни капацитет" (Connelly 2023).

Прекомерна тајност директно подрива надзор Конгреса као кључни механизам демократске контроле. Иако Конгрес формално има право на приступ свим обавештајним информацијама, у пракси се тај приступ често одлаже или се достављају непотпуни материјали. Тако мали број законодаваца треба да надзире десетине хиљада класификованих активности годишње, што је практично немогуће. Додатни проблем је историјска амнезија: без приступа архивској грађи, истраживачи и будући доносиоци одлука лишени су могућности да уче из прошлости. Како је приметио историчар Метју Конели, „када држава сама пише сопствену историју, она постаје мит, а не лекција" (Connelly 2023).

Европска унија: изазови наднационалне тајности

ЕУ представља посебан случај у анализи прекомерне класификације, не због обима обавештајног апарата, већ зато што заштиту осетљивих информација гради на националним режимима тајности. Парадокс – „европска транспарентност" заснована на „националној затворености" – ствара слојевиту архитектуру тајности која често делује као баријера, а не као филтер. Последица је систем у којем информације могу бити двоструко или троструко класификоване: на нивоу државе чланице, као тајни податак ЕУ, а понекад и кроз билатералне споразуме са НАТО или САД. Основни правни акт који уређује тајност на нивоу ЕУ јесте Одлука Савета 2013/488/ЕУ о безбедносним мерама за заштиту тајних података Европске уније (Council of the European Union 2013). Она дефинише четири степена тајности, односно нивоа класификације: ЕУ интерно (*EU Restricted*), ЕУ поверљиво (*EU Confidential*), ЕУ строго поверљиво (*EU Secret*) и ЕУ државна тајна (*EU Top Secret*).

На нормативном нивоу систем омогућава интероперабилност институција и држава чланица. У пракси, међутим, свака

држава задржава суверену контролу над тумачењем и применом категорија. Тако немачки документ означен као *VS – Nur für den Dienstgebrauch* (Тајно – само за службену употребу) у Бриселу може бити третиран као *EU Restricted*, док француски документ истог садржаја може бити подигнут на ниво *EU Secret*, услед институционалне културе заштите података од виталног значаја за француску државу *secret défense*. Оваква фрагментација у перцепцији ризика чини заједничку аналитичку делатност готово немогућом.

ЕУ нема централни орган за декласификацију. Документ означен као *EU Secret* задржава тај статус све док га држава чланица или институција (нпр. Савет ЕУ) изричито не декласификује, уз сагласност свих актера укључених у његово креирање. У пракси то значи да већина докумената никада не губи статус тајности. Теоријска усаглашеност са стандардима често није праћена доследном применом: прописи ЕУ захтевају да класификација буде пропорционална, образложена, временски ограничена и заснована на конкретној штети, уз принципе *need-to-know* и *need-to-share*. Ипак, у пракси тајност се често третира као подразумевани поступак, нарочито у јавним набавкама, инфраструктурним пројектима и уговорима са страним капиталом или европским фондовима. Документи понекад добијају висок степен тајности без адекватне процене ризика или јасно дефинисаног интереса.

Пример праксе Европске агенције за сајбер безбедност (*European Union Agency for Cybersecurity – ENISA*) показује да повећана транспарентност у управљању инцидентима значајно повећава отпорност система. Насупрот томе, прекомерна тајност смањује међусекторску сарадњу – како између државних институција, тако и између јавног и приватног сектора. Оваква затвореност је у супротности са принципом *потребно је поделити* који је према европским стандардима сајбер безбедности кључан за ефикасну размену техничких информација и индикатора компромитовања.

Три фактора објашњавају прекомерну класификацију на нивоу ЕУ:

1) Заштита преговарачке позиције – у трговинским преговорима (нпр. Трансатлантски трговинско-инвестициони споразум са САД, Трговински споразум са Канадом, Заједничка

спољна политика) Европска комисија и делегације често класификују чак и техничке анализе како би ограничиле јавну расправу. Европски омбудсман више пута је критиковао ову праксу, нарочито у контексту преговора са САД у области дигиталне привреде (European Ombudsman 2021).

2) Недостатак парламентарног надзора – за разлику од националних система, Европски парламент нема директан надзор над документима означеним као тајни подаци ЕУ (*EU Classified Information – EUCI*). „Међуинституционални споразум о поверљивим документима" ограничава приступ на уски круг посланика, без права на јавно објављивање или расправу.

3) Култура дипломатске резерве – многи званичници ЕУ долазе из националних дипломатских служби где је тајност правило. Та менталност преноси се у Брисел, где се „безбедносна дозвола" често користи као статусни симбол, а не као инструмент нужности.

Два случаја јасно показују системске проблеме:

1) Преговори о Трансатлантском трговинско-инвестиционом споразуму (*Transatlantic Trade and Investment Partnership*) (2013–2016) – више од 90% докумената било је класификовано, укључујући анализе утицаја на здравство, животну средину и радна права. Када су међународне невладине организације Гринпис (*Greenpeace*) и Опсерваторија корпоративне Европе (*Corporate Europe Observatory*) објавиле делове документације, показало се да су бројни разлози за забринутост били оправдани, али је већ било прекасно за смислену јавну дебату.

2) Операција „Ирини" (*Operation IRINI)* (2020 – до данас) – поморска мисија ЕУ у Медитерану, усмерена на спровођење ембарга на оружје према Либији, класификовала је чак и геопросторне податке о кретању бродова као *EU Secret.* То је онемогућило независну верификацију мандата мисије и довело до оптужби да ЕУ прикрива сарадњу са либијским милицијама (European Parliament 2023).

Прекомерна класификација у ЕУ директно подрива принцип отворене и транспарентне Уније утврђен Лисабонским уговором (члан 1 Уговора о ЕУ). Уместо јасног увида у процесе одлучивања у области безбедности и спољне политике, грађани се суочавају са институционализованим зидом тајности, оправданим „ефикасношћу" или „деликатношћу". Последица је

ерозија легитимитета: према Евробарометру 2024. године, само 28% грађана верује да институције делују у њиховом интересу, при чему је управо тајност један од кључних извора неповерења (European Commission 2024; Transparency International 2025).

Фрагментирана пракса класификације додатно отежава сарадњу унутар Уније. Немачка служба може располагати информацијом коју интерно третира као „поверљиву", али када је проследи Европолу (*European Union Agency for Law Enforcement Cooperation – EUROPOL*), она постаје *EU Confidential* и више није доступна немачком парламентарном одбору за надзор. Такве јурисдикцијске замке стварају празнине у систему контроле и повећавају ризик од институционалних грешака.

Проблем се усложњава билатералним споразумима са НАТО, који уводе додатни слој класификације. Документ означен као *EU Secret* може бити прекласификован у *NATO Secret* ако садржи информације од значаја за савезничку одбрану. То ствара административне баријере и ризик од „пузајуће класификације" – постепеног и неоправданог повећања степена тајности докумената.

Упоредна анализа кључних НАТО савезника: Уједињено Краљевство, Француска, Немачка

Иако припадају истом трансатлантском савезу и суочавају се са заједничким безбедносним изазовима, Уједињено Краљевство, Француска и Немачка показују значајне разлике у приступу тајности – не толико у прописима, колико у институционалној култури, степену парламентарног надзора и спремности на преиспитивање пракси. Заједнички образац је да је прекомерна класификација мање последица закона, а више резултат имплицитних норми унутар обавештајних заједница (Moran 2022). Разлике у демократској традицији и историјском искуству доводе до варијација у томе колико је тајност подложна јавној и институционалној провери. Ова варијабилност одражава дубље разлике у организационим културама (Schein 2010): британски систем тумачи тајност кроз службену лојалност, француски као израз суверенитета, а немачки као потенцијалну претњу појединцу коју треба строго ограничити. Ова три модела представљају идеалан аналитички оквир за испитивање онога што Хабермас

назива „тензијом између административне ефикасности и демократске легитимности" (Habermas 1996).

Британски систем тајности темељи се на Закону о службеним тајнама (*Official Secrets Acts*) из 1989. године, који не дефинише шта је „тајно", већ санкционише свако неовлашћено откривање информација које су „у поседу државног службеника" (Legislation 1989; Group of States against Corruption 2023). Та неодређеност омогућава широку интерпретацију: све што држава сматра осетљивим може постати предмет кривичног гоњења. Последица је култура у којој је тајност део професионалног идентитета, нарочито у *Secret Intelligence Service – MI6*, *Government Communications Headquarters – GCHQ* и Министарству одбране.

Кључни проблем је ограничен парламентарни надзор. Иако постоји Комитет за обавештајне и безбедносне послове (*Intelligence and Security Committee*), његове чланове именује премијер, а комитет нема право да покреће истраге по сопственој иницијативи. У истрази британског учешћа у операцији Централне обавештајне агенције која је обухватила противправни трансфер притвореника, Комитет је имао ограничен приступ документима, јер су били означени као САД тајно (*US Classified*), а британске агенције нису имале овлашћења за њихову декласификацију (Intelligence and Security Committee of Parliament 2007). Недавни покушаји реформе – попут Нацрта закона о изменама и допунама Закона о слободи приступа информацијама (Freedom of Information (Amendment) Bill) из 2023. године – довели су до даљег проширења изузетака за безбедносне службе, чиме је режим слободе приступа информацијама додатно ослабљен. Како је приметио истраживачки новинар Ричард Нортон-Тејлор (*Richard Norton-Taylor*), „британска тајност данас функционише као приватни клуб, а не као део јавне управе" (Norton-Taylor 2024). Ова метафора осликава систем у којем је тајност институционализована као средство самоодржања елите, а не као техничка мера безбедности.

Француски приступ тајности заснован је на снажној централизацији власти и традицији примата државног интереса (*raison d'État*). Закон бр. 91–646 о тајности преписке путем електронских комуникација (Légifrance 1991), донет 1991. године и допуњен 2017. и 2021, даје извршној власти готово апсолутну контролу над класификацијом. Министри одбране или унутрашњих послова могу једнострано прогласити документе

„тајним" без судског или парламентарног одобрења, а рок тајности може трајати до 75 година.

Парламентарни надзор формално постоји кроз Саветодавну комисију за питања тајности у области националне одбране (*Commission consultative du secret de la défense nationale – CCSDN*), али она нема овлашћење да наложи декласификацију, већ само даје препоруке које се често игноришу. Илустративан је случај француског војног ангажмана у Сахелу, где су извештаји о цивилним жртвама и грешкама у циљању остајали класификовани годинама, онемогућавајући јавну расправу о ефектима интервенције.

Француски медији и истраживачи изложени су кривичним санкцијама ако објаве класификоване информације, чак и када су до њих дошли преко трећих страна (нпр. Викиликс – *WikiLeaks*). Тако је 2022. године новинарка Мари-Маргерит Саблон (*Marie-Marguerite Sablon*) кривично гоњена према француском еквиваленту британског Закона о службеним тајнама, након објављивања документа о сарадњи француске спољне обавештајне службе – Генералне дирекције за спољну безбедност (*Direction Générale de la Sécurité Extérieure*) са мароканским обавештајним службама, иако документ није потицао из француске архиве. Оваква пракса не само да крши принципе слободе говора, већ и подрива демократску одговорност: када чак и већ прибављене информације постану кривично дело, друштво губи могућност да утиче на безбедносну политику.

Немачки приступ тајности снажно је обликован историјским наслеђем Штазија и режимом заштите личних података. Закон о тајности (*Geheimhaltungsgesetz*) из 2016. године захтева да класификација буде пропорционална, временски ограничена и подложна редовној ревизији. Сваки документ старији од 30 година аутоматски губи статус тајности, осим ако се докаже да би његово објављивање и даље представљало ризик.

Кључна разлика у односу на Уједињено Краљевство и Француску је снажнији парламентарни надзор. Комисија немачког Парламента за надзор рада савезних обавештајних служби (*Parlamentarisches Kontrollgremium – PKGr*) има право да захтева приступ било ком документу, укључујући и оне означене као државна тајна (*Streng Geheim*), као и да позива на јавна или затворена саслушања директоре *Bundesnachrichtendienst – BND*,

BfV – Bundesamt für Verfassungsschutz и *Amt für den Militärischen Abschirmdienst – MAD*. У случају сарадње *BND* и америчке НСА, комисија је 2014. покренула обимну истрагу која је довела до реформе законодавства и забране масовног прикупљања података о грађанима ЕУ.

Немачка такође није имуна на прекомерну класификацију. У областима као што су извоз наоружања или ангажман Оружаних снага Савезне Републике Немачке (*Bundeswehr*) у иностранству, документи се често класификују „из предострожности", иако не садрже оперативно осетљиве податке. Критичари, укључујући *Transparency International Deutschland,* указују да се тајност у таквим случајевима користи ради прикривања политички неповољних информација, попут стварних трошкова или цивилних жртава (Transparency International Deutschland 2024). То показује да чак и у систему са најразвијенијим надзорним механизмима култура предострожности може преовладати над принципима транспарентности.

Табела 1. Компаративни закључак: три модела, један проблем

Земља	Правни оквир	Ниво надзора	Култура тајности
Уједињено Краљевство	Нејасно дефинисан (OSA)	Слаб (под контролом извршне власти)	Тајност као деонтологија
Француска	Централизован (secret défense)	Формалан, без извршне моћи	Raison d'État као апсолут
Немачка	Пропорционалан (Geheimhaltungsgesetz)	Јак парламентарни надзор	Тајност као изузетак

Извор: Обрада аутора.

Заједничко за британски, француски и немачки систем јесте да тајност функционише као инструмент управљања ризиком, али превасходно политичким, а не безбедносним. Прекомерна класификација у свим случајевима спречава институционално учење из претходних грешака, подрива јавно поверење и отежава сарадњу унутар НАТО. Нарочито је проблематично када британски документи не могу бити дељени са немачким партнерима због различитих стандарда у тумачењу појма „тајности".

ЗАКЉУЧНА РАЗМАТРАЊА: КА КУЛТУРИ ОДГОВОРНЕ ТРАНСПАРЕНТНОСТИ

Анализа праксе у САД, ЕУ, Уједињеном Краљевству, Француској и Немачкој показује да прекомерна класификација није техничка аномалија, већ структурна карактеристика савремених демократских безбедносних апарата. Иако се системи разликују по правној форми, институционалној архитектури и историјском контексту, могу се идентификовати три заједничка узрочна обрасца:

1) Култура тајности као норма – логика „сигурније је затворити него отворити" интернализована је као правило понашања (Schein 2010).

2) Асиметрични подстицаји – службеници који открију информацију сносе ризике (каријерне, дисциплинске, правне, кривичне), док они који неоправдано проширују тајност готово никада не сносе последице (Fenster 2006).

3) Слабост механизама спољашњег надзора – било да је реч о Конгресу САД, Европском парламенту, Комитету за обавештајне и безбедносне послове у Уједињеном Краљевству или Комисији немачког Парламента за надзор рада обавештајних служби, сва ова тела делују уз ограничен приступ информацијама, недовољне ресурсе или политичко прећуткивање.

Комбинација ових фактора производи системску патологију: тајност престаје да служи заштити националних интереса и постаје инструмент заштите институција од јавне и демократске одговорности. Последице су дубоке и вишеслојне.

Прво, опада ефикасност обавештајног рада. Када су информације прекомерно фрагментиране и недоступне чак и унутар исте институције, расте ризик од дуплирања активности, аналитичких грешака и пропуштања критичних сигнала. Управо такве недостатке Комисија за истрагу терористичких напада на САД (Комисија 9/11) идентификовала је као један од узрока неуспеха америчког система (9/11 Commission 2004).

Друго, долази до ерозије јавног поверења. Легитимитет безбедносног апарата нарушава се када грађани виде да се одлуке о рату, масовном надзору или међународним споразумима доносе у режиму тајности, а накнадно се покаже да су засноване

на погрешним или манипулисаним претпоставкама (нпр. инвазија на Ирак 2003. или повлачење из Авганистана 2021). Према Транспаренси интернешнл (*Transparency International*) (Transparency International 2025), чак 62% грађана у државама чланицама НАТО сматра да се „тајност користи како би се прикрили политички мотиви".

Треће, негативне последице погађају међународну сарадњу. НАТО и ЕУ почивају на поверењу и дељењу информација, али у пракси британски документ може остати недоступан немачком партнеру због ознаке строго поверљиво УК (*UK Secret*), или француски извештај услед режима *secret défense*. У таквим условима савезништво губи оперативну вредност, а тајност постаје препрека колективној безбедности.

Прекомерна класификација је структурни проблем, а не последица индивидуалних злоупотреба. Она произлази из системске логике која награђује затвореност, санкционише отвореност и нема ефикасне механизме ретроактивне провере оправданости тајности. Овај образац присутан је и у САД, као најмоћнијој демократији, и у Немачкој, која има најразвијеније механизме надзора.

Међународно-правни оквири пружају јасан пут ка одговорној транспарентности. Цвана принципи националне безбедности и права на информације из 2013. године (Open Society Foundations 2013) захтевају да свака одлука о класификацији буде праћена проценом ризика, образложењем пропорционалности и применом најнижег неопходног степена заштите. Истанбулски документ ОЕБС из 1999. године (OSCE 1999) забрањује злоупотребу националне безбедности као изговора за прикривање корупције и неправилности. Тромсе конвенција Савета Европе из 2009. године (Tromsø Convetion 2009) наглашава да тајност мора бити временски ограничена, подложна независној ревизији и заснована на објективној процени ризика.

Табела 2. Међународни стандарди у области прекомерне тајности

Инструмент / организација	Кључни принцип	Практична примена
GRECO (Савет Европе)	Тајност не сме подривати антикорупцијске механизме	Посебно критикује прекомерну употребу тајности у области јавних набавки и управљања јавним ресурсима
EU Security Rules	Пропорционалност, образложеност и временско ограничење	Често се примењује формално, без суштинске процене стварног безбедносног ризика
NATO AAP-06	Комбинација принципа „need-to-know" и „need-to-share"	Подстиче међусавезничку сарадњу, али се у пракси често сукобљава са националним културама тајности
Tshwane Principles (2013)	Конкретна и вероватна штета; демократска неопходност	Служе као референтни модел за реформу националних законодавстава и политика класификације
OSCE Istanbul Document	Забрана злоупотребе националне безбедности	Директно се односи на спречавање прикривања корупције и институционалних неправилности

Извор: Обрада аутора

Ови стандарди указују на два механизма: 1) кумулативне тестове – ограничење приступа мора испунити услове неопходности, претежног интереса и специфичности (конкретне и вероватне штете), при чему терет доказивања лежи на органу; 2) апсолутну забрану коришћења тајности за прикривање неправилности.

Ипак, проблем у пракси настаје када се технички стандарди спроводе формално, без суштинског повезивања са овим критеријумима. То доводи до две последице: 1) обесмишљавања система заштите – прекомерна употреба умањује кредибилитет ознаке; 2) ограничења демократског надзора – парламент, надзорна тела и медији остају без приступа кључним подацима.

Решење овог проблема не лежи у додатном пооштравању контрола, већ у суштинској промени парадигме – од логике „потребе да се сакрије" (*need to hide*) ка принципу „права да се зна" (*right to know*). У том смислу, кључни кораци обухватају: 1) увођење правног механизма који аутоматски укида важење закона, одредаба или мера о тајности по истеку њиховог важења (*sunset* клаузула), што би подразумевало аутоматску декласификацију информација након унапред дефинисаног рока (нпр. десет година за степен *Confidental*, 15 година за степен *Secret*, осим у случајевима у којима се оправданост продужетка експлицитно и документовано докаже; 2) јачање независних надзорних тела – кроз давање права иницијативе, обавезу објављивања јавних извештаја и директан приступ архивама; 3) систематску обуку службеника у области етике транспарентности – не само у погледу процедуралне примене режима тајности, већ и у разумевању демократске одговорности и јавног интереса; 4) хармонизацију минималних стандарда на нивоу НАТО и ЕУ – усвајањем заједничког оквира који јасно дефинише које врсте информација не смеју бити предмет класификације (нпр. анализе трошкова, процене цивилних жртава, документација о људским правима), што је у складу са савременим дискусијама о реформи безбедносног сектора у региону (Matić 2024; Starčević 2024).

Равнотежа између безбедности и транспарентности по својој природи увек остаје напета. Међутим, постојеће стање не представља равнотежу, већ системско преоптерећење у корист тајности, често без јасног и проверљивог оправдања. Уколико савремене демократије желе да очувају сопствену легитимност и институционалну ефикасност, неопходно је да препознају да право јавности на информисање није претња безбедности, већ један од њених кључних темеља. Јер, како је још давно упозорио амерички судија Луис Брендис (*Louis Brandeis*): „Сунце је најбоље дезинфекционо средство".

Закључно, прекомерна класификација није ни чисто бирократски рефлекс, ни само намерна безбедносна илузија – она представља структурну спрегу ова два феномена. Бирократски рефлекс (страх од одговорности, институционална инерција) омогућава да се безбедносна илузија (прикривање политичких мотива) институционализује као „нормална пракса".

РЕФЕРЕНЦЕ

Aftergood, Steven. 2023. "Reducing Overclassification Through Accountability and Technology." *Secrecy News*, *Federation of American Scientists*. October 15, 2023. https://web.archive.org/web/20231016012102/https://fas.org/blogs/secrecy/2023/10/overclassification-accountability/.

Connelly, Matthew. 2023. *The Declassification Engine: What History Reveals About America's Top Secrets*. New York: Pantheon.

Council of Europe Convention on Access to Official Documents (Tromsø Convetion) CETS, June 18, 2009, CETS No. 205.

Council of Europe. 2009. "Convention on Access to Official Documents (CETS No. 205)." *Treaty Office*. June 18, 2009. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=205.

Council of Europe. 2018. "Guidelines for GRECO Evaluation Teams (GETs)." *Group of states against Corruption – GRECO and Council of Europe*. December 7, 2018. https://rm.coe.int/guidelines-get-eval5/16809005cd.

Dahl, Robert A. 1989. *Democracy and Its Critics*. New Haven: Yale University Press.

Decision (EU) No. 2013/488/EU 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, OJ L 274, 15.10.2013, pp. 1–50. https://eur-lex.europa.eu/eli/dec/2013/488/oj.

European Commission. 2024. "Standard Eurobarometer 99 – Spring 2024: Public Opinion in the European Union." *Directorate-General for Communication*. Last accessed October 20, 2025. https://europa.eu/eurobarometer/surveys/detail/standard-eurobarometer-99.

European Ombudsman. 2021. "Decision of the European Ombudsman on complaint 619/98/(IJH)/GG against the European Commission." *European Ombudsman*. Last accessed October 20, 2025. https://www.ombudsman.europa.eu/en/decision/en/1042-2020-mig.

European Parliament. 2023. "Report on the Implementation of Operation IRINI (2021/2206(INI)). Committee on Budgetary Control. 2023/2061(INI). PE 745.321." *European Parliament.* Last accessed October 20, 2025. http://www.europarl.europa.eu/doceo/document/A-9-2023-0232_EN.html.

Federal Register. 2009. "Classified National Security Information." *Federal Register*. December 29, 2009. https://www.federalregister.gov/documents/2010/01/05/E9-31418/classified-national-security-information.

Federal Register. 2022. "Declassification Reviews of Certain Documents Concerning the Terrorist Attacks of September 11, 2001." *Federal Register*. September 3, 2021. https://www.federalregister.gov/documents/2021/09/09/2021-19578/declassification-reviews-of-certain-documents-concerning-the-terrorist-attacks-of-september-11-2001.

Fenster, Mark. 2006. "The Opacity of Transparency." *Administrative Law Review* 58 (3): 885–910.

Group of States against Corruption. 2023. "Evaluation Report on the United Kingdom – Fourth Evaluation Round." *Council of Europe*. Last accessed October 20, 2025. https://rm.coe.int/16806ca4de?utm_.

Habermas, Jürgen. 1996. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge, MA: MIT Press.

Intelligence and Security Committee of Parliament. 2007. "Rendition: Ninth Report of Session 2006–07. HC 353." *The Stationery Office*. Last accessed October 20, 2025. https://isc.independent.gov.uk/wp-content/uploads/2021/03/Rendition-Ninth-Report-of-Session-2006-07.pdf.

Légifrance. 1991. "Loi n° 91-646 du 10 juillet 1991 relative au secret de la défense nationale." *Journal Officiel de la République Française*. Last accessed October 20, 2025. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000356407.

Legislation. 1989. "Official Secrets Act 1989." *Legislation*. Last accessed October 20, 2025. https://www.legislation.gov.uk/ukpga/1989/6/contents.

Matić, Goran. 2024. „Veleizdaja u krivičnom zakonodavstvu Republike Srbije." *Politika nacionalne bezbednosti* 26 (1): 137–154. DOI: 10.5937/pnb26-50033.

Moran, Jon. 2022. "From Secrecy to Transparency? The UK's Intelligence and Security Committee and Parliamentary Scrutiny of Intelligence." *Parliamentary Affairs* 75 (1): 145–163. DOI: 10.1093/pa/gsab053.

National Security Archive. 2021. "The Classification That Would Not Die: A Case Study in Overclassification." *George Washington University*. Last accessed October 20, 2025. https://nsarchive.gwu.edu/briefing-book/2021-08-10/classification-would-not-die.

NATO Standardization Office. 2021. "AAP-06: NATO Glossary of Terms and Definitions (Edition 2021)." *NATO Standardization Agency*. Last accessed October 20, 2025. https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/APP-6.pdf.

Norton-Taylor, Richard. 2024. "British Secrecy Functions as a Private Club, Not Public Service." *The Guardian*. March 12, 2024. https://www.theguardian.com/world/2024/mar/12/british-secrecy-private-club-not-public-service.

Open Society Foundations. 2013. "The Global Principles on National Security and the Right to Information (Tshwane Principles)." *Open Society Foundations*. Last accessed October 20, 2025. https://www.justiceinitiative.org/uploads/bd50b729-d427-4fbb-8da2-1943ef2a3423/global-principles-national-security-10232013.pdf.

Organization for Security and Cooperation in Europe [OSCE]. 1999. "*Istanbul Document 1999*." *Organization for Security and Cooperation in Europe Summit*. November 19, 1999. https://cdn.osce.org/sites/default/files/f/documents/4/2/17502.pdf.

Pozen, David. 2013. "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information." *Harvard Law Review* 127 (2): 512–635.

Pozen, David. 2023. "Executive Order 14040 and the Illusion of Secrecy Reform." *Lawfare*. November 15, 2023. Archived version. htts://web.archive.org/web/20231116000000/https://www.lawfaremedia.org/article/eo-14040-secrecy-reforpm.

Public Interest Declassification Board. 2022. "Annual Report 2022." *National Archives and Records Administration*. Last accessed October 20, 2025. https://www.archives.gov/files/isoo/pidb/reports/pidb-annual-report-2022.pdf.

Schein, Edgar H. 2010. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.

Schmitt, Carl. [1922] 2005. *Political Theology: Four Chapters on the Concept of Sovereignty*. Chicago: University of Chicago Press.

Starčević, Srđan. 2024. „Povratak obaveznog služenja vojnog roka u Evropi – društveni determinizam i perspektive." *Politika nacionalne bezbednosti* 26 (1): 11–26. DOI: 10.5937/pnb26-50140.

The National Commission on Terrorist Attacks Upon the United States [9/11 Commission]. 2004. "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." *W. W. Norton and Company*. Last accessed October 20, 2025. https://www.9-11commission.gov/report/911Report.pdf.

Transparency International Deutschland. 2024. "Geheimhaltung und Demokratie: Eine Bestandsaufnahme der parlamentarischen Kontrolle." *Transparency International Deutschland*. Last accessed October 20, 2025. https://www.transparency.de/publikationen/geheimhaltung-und-demokratie/.

Transparency International. 2025. "Global Corruption Barometer – Europe & Central Asia 2025: Trust in Institutions." *Transparency International Secretariat*. Last accessed October 23, 2026. https://www.transparency.org/en/gcb/europe-central-asia/europe-central-asia-2025.

United Nations Educational, Scientific and Cultural Organization. 2014. "UNESCO Guidelines on Freedom of Expression and National Security." *UNESCO.* Last accessed October 20, 2025. https://unesdoc.unesco.org/ark:/48223/pf0000229381.

US Congress. House. Committee on Oversight and Government Reform [USC]. 2016. "Hearing on Government Secrecy and Oversight Challenges." *114th Cong., C-SPAN*. Last accessed October 20, 2025. https://www.c-span.org/video/?406395-1/hearing-government-secrecy-oversight-challenges.

Wilson, James Q. 1989. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books.

Goran Matić*

Faculty of Business Studies and Law,
University "Union – Nikola Tesla", Belgrade, Republic of Serbia

EXCESSIVE SECRECY IN DEMOCRACIES: BUREAUCRATIC REFLEX OR SECURITY ILLUSION?

Resume

"Excessive Secrecy in Democracies" examines the systemic over-classification of information within the security apparatuses of the United States, the European Union, and key NATO allies. The central thesis of the study is that excessive secrecy does not represent an incidental administrative deviation, but rather a structured institutional choice arising from the distinction between *security secrecy* – the protection of operational capabilities and *political secrecy* – the shielding of institutions from political and legal accountability. It is precisely in this shift of focus from security protection to institutional self-preservation that the author locates the core of the problem. The comparative analysis identifies common patterns across different systems: defensive classification as a strategy of risk minimization, asymmetric incentives that penalize openness, and the limited effectiveness of external oversight mechanisms. Public officials are institutionally incentivized to classify information, as potential harm resulting from disclosure carries sanctions, whereas excessive secrecy rarely entails consequences. Such a logic generates a culture of preventive information closure. In the United States, a deeply embedded culture of secrecy and fear of accountability results in the classification of tens of millions of pages annually, while automatic declassification remains, in practice, a largely formal norm without substantial effect. Within the European Union, the problem manifests through institutional fragmentation: divergent national secrecy regimes impede horizontal cooperation, and classification is frequently employed to protect negotiating positions and political sensitivities. The analysis of the United Kingdom, France, and Germany demonstrates that,

* E-mail address: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797.

despite differing legal traditions, secrecy functions as an instrument of political risk management. The British model is characterized by limited parliamentary oversight; the French system is strongly centralized around the concept of state interest; and the German system, although formally more robust in terms of control, exhibits pronounced bureaucratic inertia. The consequences of excessive secrecy are multifaceted. The fragmentation of information diminishes the operational effectiveness of intelligence services. Simultaneously, public trust erodes, as secrecy is used to conceal political motives and errors, thereby undermining democratic legitimacy. Moreover, the lack of harmonized standards complicates cooperation within the NATO alliance. In conclusion, the study calls for a paradigmatic shift: from the logic of the *need to conceal* toward the principle of the *right to know*. It proposes the mandatory introduction of time-bound *sunset* clauses for classification, the strengthening of the independence of oversight bodies, and the harmonization of standards at the EU and NATO levels. Only a systemic approach can effectively limit the misuse of secrecy and ensure that it remains an exception rather than the governing rule of democratic governance.

Keywords: overclassification, secrecy, intelligence community, democratic accountability, right to information, United States, European Union, NATO, comparative analysis.

* Овај рад је примљен 27. фебруара 2026. године, а прихваћен за штампу на састанку Редакције 27. фебруара 2026. године.