УДК 342.738+159.923:004.738.5
Doi:10.5937/nint52-59342
Прегледни научни рад

НАЦИОНАЛНИ ИНТЕРЕС
NATIONAL INTEREST
Година XXI, vol. 52
Број 3/2025
стр. 147-172

Горан Матић*

Канцеларија Савета за националну безбедност и заштиту тајних података

КУЛТУРА ТАЈНОСТИ У ДИГИТАЛНОМ ДОБУ: ИЗМЕЂУ НУЖНОСТИ, ЗЛОУПОТРЕБЕ И САЈБЕР БЕЗБЕДНОСТИ

Сажетак

Култура тајности представља институционализовани модел управљања информацијама, који се развија од античких цивилизација до савременог дигиталног доба. Иако је историјски била оправдана безбедносним и политичким интересима, често је служила као средство концентрације моћи и ограничавања демократског надзора. У Римском царству, подаци су се чували у формализованим архивама (*tabularia),* а кинеске династије Ћин и Хан успоставиле су бирократске механизме за заштиту поверљивих информација. Савремени облици, као што је *D-Notice* систем у Великој Британији, настављају традицију институционалне тајности, док дигиталне технологије омогућавају суптилније облике надзора — кроз алгоритме, масовно прикупљање података и класификовање јавних уговора. Злоупотребе попут софтвера *Pegasus* и активности узбуњивача, попут Едварда Сноудена (*Edward Snowden),* откривају рањивост приватности и изазивају шире друштвене дебате. Истовремено, правни инструменти попут Закона о слободном приступу информацијама у САД и иницијативе

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

за декласификацију докумената указују на настојања да се обезбеди јавни надзор. Овај рад анализира историјску еволуцију културе тајности, њену дигиталну трансформацију и савремене изазове у постизању равнотеже између легитимне заштите и транспарентности.

Кључне речи: политика, безбедност, култура тајности, сајбер безбедност, дигитално друштво, јавни интерес, заштита података, транспарентност.

УВОДНА РАЗМАТРАЊА

Култура тајности представља темељни елемент управљања информацијама, омогућавајући институцијама да контролишу приступ подацима и централизују моћ. Док је у традиционалним друштвима служила за очување ауторитета и заштиту од спољних претњи, у дигиталном добу она се трансформише кроз механизме сајбер-безбедности и алгоритамских система управљања. Историјски примери – од античких цивилизација до модерних држава – потврђују да је контрола информација одувек била инструмент политичке и безбедносне стратегије (Thompson 2000, 89–94). У Римском царству државне тајне су биле архивиране у институцијама попут Табуларијума на Римском форуму, са строго контролисаним приступом и функцијом чувања правних и административних докумената (MacMullen 1988, 15–22). Кинеске династије Ћин (*Qin*) и Хан (*Han*) успоставиле су централизовану контролу путем бирократских и правних механизама, који су укључивали строге казне за одавање поверљивих података. Династија Ћин је инсистирала на дисциплини и санкцијама, док је династија Хан развила институционализовани систем избора службеника, чиме је оснажена стабилност власти и учвршћена хијерархијска структура (Moran 2014, 95).

Култура тајности историјски је обликовала управљање информацијама – од сакривања знања у античким цивилизацијама до институционализоване тајности у модерним друштвима. У Европи, она добија форму кроз средњовековне ватиканске архиве и касније кроз обавештајне службе Британије и Француске, постајући кључни инструмент политичке и административне моћи. Немачка је развила ефикасне бирократске моделе контроле података који су током XX века еволуирали у оквиру индустријских и војних

структура, док је италијанска историјска динамика резултирала ограниченом и селективном транспарентношћу.

У Србији је култура тајности имала дугу традицију, од османских регулатива до модерних облика административне и политичке контроле информација. У XX веку, тајност је често била инструмент централизоване власти, али је истовремено еволуирала са развојем законодавства које се бави приступом информацијама. Дигитално доба додатно је усложило овај феномен, јер алгоритми и сајбер безбедносни механизми омогућавају не само заштиту података, већ и суптилне облике манипулације, постављајући нове изазове за транспарентност и јавну контролу.

Дигитална ера је донела двоструки изазов: технологија омогућава већу доступност информација, али истовремено ствара механизме за њихово сакривање и манипулацију. Алгоритми, шифровање и масовни надзор постали су алати за контролу информација, често без адекватног јавног надзора. Истраживања показују да прекомерна тајност у дигиталном простору може довести до концентрације моћи, док се оправдава потребом за сајбер безбедношћу (Zuboff 2019, 189).

Примери попут шпијунског софтвера *Pegasus* показују како дигитални надзор може угрозити основна права, док се класификација јавних уговора понекад користи као инструмент политичке контроле. Ови случајеви откривају да се традиционална тајност адаптира савременим технологијама, често без јасних механизама одговорности (Reporters without borders 2021, 12; Greenwald 2014, 89).

Пораст свести о ризицима прекомерне тајности подстиче расправе о правним реформама и одговорности. Док државе често ограничавају приступ информацијама позивајући се на безбедност, јавност све гласније захтева транспарентност и надзор над механизмима управљања подацима. Законске иницијативе попут Закона о слободном приступу информацијама (*Freedom of Information Act – FOIA*) у САД омогућавају увид у владине одлуке и јачају јавну контролу (Bok 1989, 143). Узбуњивачи попут Сноудена и судске одлуке, укључујући пресуде Европског суда за људска права, указују на неопходност независног надзора над системима дигиталног надзора (BBC 2018). Напетост између заштите и транспарентности остаје кључна тема овог истраживања.

ИСТОРИЈСКИ КОНТЕКСТ КУЛТУРЕ ТАЈНОСТИ

Концепт тајности као средства заштите осетљивих података присутан је у политичким и друштвеним структурама од најранијих цивилизација. У старом Египту и Месопотамији, знање о астрономији, медицини и писму било је резервисано за уске кругове, чиме се осигуравала моћ елите (Stevens 2013, 211).

У Римском царству, поверљиве информације чуване су у формално организованим архивима (*tabularia*), а приступ им је био строго контролисан. (Matthews 1989, 608). Тајност се наставила у средњем веку, када су монарси и верске институције регулисали проток информација како би очували политичку и религијску стабилност (Radić i Krunić 2017). Средњовековне државе користиле су кодиране поруке и повезане обавештајне мреже за одржавање политичке контроле.

Кина негује дугу традицију тајности у политичком и друштвеном животу, почев од доба Ратних држава (475–221. п.н.е.), када су владари примењивали строге мере за очување власти. Конфуцијанизам је истицао контролу информација као кључ управљања, а династије Ћин и Хан су системски институционализовале казне за откривање поверљивих података (Habberstad 2023, 1–22). Тајна друштва, попут Жутих турбана, Белог лотоса и Тријада, деловала су као паралелне структуре моћи, оспоравајући власт. Тријаде су почетком 20. века имале извесну политичку моћ. Врхунац су достигле 1911. године, када су помогле националистима у сламању последње кинеске династије Ћинг (*Quing*). После победе комуниста Мао Цедунга и сламања трговине опијумом, многе тријаде су побегле на Тајван, у Макао и Хонгконг. Када је ухапшен оснивач Када је ухапшен оснивач најмоћније тријаде „14К" генерал Куоминтанга Кот Суивонг, тријаде су изгубиле последњи трачак политичке мотивације и упловиле у криминал. У савременој Кини тајност остаје темељ политичког система – од Маове ере до данашњих дигиталних механизама надзора, у којима вештачка интелигенција и алгоритамска контрола служе централизованом управљању (Zuboff 2019, 312).

Велика Британија има дугу историју тајности у управљању информацијама, која сеже уназад до тјудорске ере (XVI век), када је краљица Елизабета I основала један од првих организованих обавештајних система у Европи. Њен шеф шпијуна, Френсис

Волсингем (1532–1590) користио је сложене мреже агената, шифроване поруке и технике пресретања комуникација, како би заштитио енглеску круну од страних претњи (Haynes, 2011). У XX веку, Велика Британија је формализовала своје обавештајне службе, оснивањем MI5 и MI6 1909. године. Током Другог светског рата, британска влада је користила локалитет Блечли Парк (*Bletchley Park)* као центар за дешифровање немачких кодова, што је био један од највећих успеха у историји обавештајних операција (Smith 2010, 120). У савременом добу, британска култура тајности наставља да се развија кроз механизме као што су *D-Notice* систем, који омогућава влади да спречи објављивање осетљивих информација у медијима (Moran 2014, 95).

Француска традиција тајности у управљању датира из периода „Старог режима" (*Ancien Régime)*, пре Француске револуције 1789. године, када су механизми попут печатних писама (*lettres de cachet)* омогућавали монарху да тајно затвара појединце без суда (Bauer 2023b, 329). У XVIII веку, раст јавног мњења довео је до критике тајности, посебно у вези са полицијским репресијама и симболиком затвора Бастиље (Bauer 2023a, 53). Иако је Француска револуција афирмисала транспарентност, период Терора (5.9.1793 – 27.7.1794) показао је како се и револуционарне власти могу ослонити на тајност ради репресије (Andress 2006). Након револуције, државна тајност наставила је институционални развој кроз службе попут Генералне управе за спољно обавештавање (*Direction générale de la sécurité extérieure – DGSE*). У савременом добу, тајност остаје кључна у сферама националне безбедности, али постоје и правни оквири, попут Закона о приступу административним документима (*Loi sur l'accès aux documents administratifs*) који регулишу приступ јавним информацијама (Dandelot 2018).

У нацистичкој Немачкој, тајност је била кључни инструмент репресије, посебно кроз рад Гестапоа, задуженог за елиминацију противника и надзор над становништвом (Browder, 1996). Режим је користио шифроване комуникације, тајне архиве и пропаганду за централизовање информација и сузбијање отпора. Током рата, грађени су тајни бункери и тунели за прикривање војних операција (German Culture 2025). У фашистичкој Италији је *OVRA* (тајна полиција Мусолинија формирана 1927. године) спроводила политичку репресију, док су тајни дипломатски канали и шифре подржавали међународне циљеве, укључујући инвазије на Етиопију

и Албанију (Britannica, 2025; Wikipedia, 2025). Јапан је у периодима Меиџи (*Meiji*) и Шова (*Shōwa*) користио цензуру и тајност за учвршћивање милитаризма (Andrew 2014), а током Другог светског рата Јединица 731 спроводила је тајни програм биолошког ратовања над заробљеницима (Tsuneishi 2006).

Култура тајности у Русији пре Октобарске револуције била је чврсто укорењена у царским институцијама. Од Московске Русије до краја XIX века, тајност је служила за централизовано управљање и ограничавање приступа кључним подацима (McCauley 2025, 112). У XIX веку, тајна полиција *Охрана* постаје главни инструмент сузбијања револуционарних покрета, користећи инфилтрацију и цензуру за одржање политичке стабилности (Emmons 2017, 118). Тајност се одражавала и у економским и дипломатским политикама, ограничавајући јавну дебату и успоравајући модернизацију у поређењу са Западом (World Atlas 2025, 3). Револуција 1917. године означила је прелаз ка новом моделу – од царске тајности ка идеолошкој контроли информација, заснованој на пропаганди и цензури (Timofejev i Piljak 2017).

Култура тајности у Сједињеним Америчким Државама има релативно кратку, али интензивну историју, која је постала институционализована током XX века. Иако су рани облици тајности постојали у дипломатским и војним структурама, модерни систем класификације података успостављен је тек 1951. године, када је председник Хари Труман издао извршну наредбу којом су дефинисане категорије *Top Secret, Secret,* и *Confidential* (Lebovitz 2016, 2). Током Хладног рата, тајност је постала кључни елемент националне безбедности, посебно у области нуклеарних истраживања. Америчка влада је развила сложене механизме за контролу информација, укључујући Закон о слободном приступу информацијама (*Freedom of Information Act*) који је усвојен 1966. године, како би се омогућио јавни надзор над државним документима. Ипак, паралелно са тим, тајност је наставила да се шири кроз програме попут *Restricted Data*, који су регулисали приступ информацијама о нуклеарном оружју (Wellerstein 2021, 78). У савременом добу, култура тајности у САД је додатно ојачана кроз механизме дигиталног надзора и масовног прикупљања података. Док влада оправдава ове мере потребом за националном безбедношћу, критичари истичу да прекомерна тајност омогућава концентрацију моћи и смањује јавну одговорност (Connelly 2023, 458).

Социјалистичке државе су често користиле тајност као инструмент политичке контроле, посебно у периоду Хладног рата. Совјетски Савез је био један од најтајновитијих режима у историји, са системом строге контроле информација, цензуре и надзора. Совјетска држава је користила четири стуба тајности: државни монопол над производњом и комуникацијама, свеобухватну цензуру, партијску дисциплину и Комитет државне безбедности (*Комитет государственной безопасности – КГБ*) као инструмент надзора (Harrison 2023, 45). Након пада Берлинског зида 1989. године, државе попут Пољске, Чешке, Мађарске и балтичких земаља започеле су процес демократизације, али су механизми тајности остали присутни у различитим облицима. У многим случајевима, бивше комунистичке службе безбедности наставиле су да играју значајну улогу у политичком животу, што је довело до дебата о декласификацији архивских докумената и транспарентности (Berend 2023, 112).

Тајност је била темељ репресивне моћи диктаторских режима Латинске Америке XX века, попут оних Пиночеа, Трухиља и Виделе. Тајне службе су спроводиле цензуру, надзор и елиминацију противника (Galván 2013, 89). У Чилеу је Управа националне обавештајне службе (Dirección de Inteligencia Nacional – *DINA)* била кључни инструмент репресије, док је у Аргентини Секретаријат државне обавештајне службе (*Secretaría de Inteligencia del Estado – SIDE*) водила кампању масовних „нестанака" (Minster 2025, 44). Сличне праксе постојале су и у афричким ауторитарним режимима — у Заиру је тајност служила за централизацију моћи, у Либији за свеобухватни надзор, а у Уганди под Идијем Амином за елиминацију опозиције (Decalo 1985, 209; Ekwo 2013, 112).

Култура тајности у ратовању има дубоке историјске корене, од античких стратегија прикривања војних планова до савремених облика информационе безбедности. У древној Спарти, метод *scytale* омогућавао је шифровану комуникацију између војних заповедника, док су римске легије користиле сложене сигналне системе за пренос поверљивих наредби (Balmer 2016, 45). Средњовековне војске су примењивале тактике дезинформације како би обмануле противнике, а током Наполеонових ратова, француска војска је развила напредне методе шифровања за заштиту оперативних планова (Imperial War Museums 2024, 12). Са развојем модерног ратовања, тајност је постала кључни фактор у војним операцијама.

Током Првог и Другог светског рата, употреба шифрованих комуникација, попут немачке *Енигме*, значајно је утицала на исход сукоба. У савременом добу, војне стратегије укључују напредне системе сајбер безбедности и алгоритамске методе прикривања података, што омогућава контролу информација на глобалном нивоу (Total Military Insight 2024, 8).

Култура тајности у Србији темељи се на дубоко укорењеним историјским структурама – од средњовековног феудалног система и црквених институција до модерне државности. Владарске породице, попут Немањића, користиле су тајну дипломатију, а манастири чували поверљиве информације политичке и војне природе (Ćirković 1995). Током Првог српског устанка, шифроване поруке и тајни канали били су кључни за војну координацију и избегавање османске контраобавештајне активности (SrpskiKod 2025, 3). Иако је устанак окончан 1813, поставио је темеље новим безбедносним структурама. Тајни дипломатски односи с Русијом имали су значајну стратешку улогу (Royal Family of Serbia 2025, 10). Услед Другог устанка, тајност се институционализује кроз дипломатију и прве обавештајне службе (Stojančević 2004). У Краљевини Југославији, тајне службе постају инструмент политичке контроле (Петрановић 1988), а током Другог светског рата, партизански покрет развија комплексне мреже шифри и курира ради координације отпора (Dević 2021).

У социјалистичкој Југославији култура тајности била је дубоко интегрисана у политички, економски и културни систем. Комунистичка партија и безбедносне службе, по узору на совјетски модел, контролисале су друштвене токове и надгледале грађане и дисиденте. Након распада Југославије, тајност је преживела у новим државама, али је постојано трансформисана кроз демократске промене, законе о приступу информацијама и реформу служби безбедности (History State Gov. 2025, 7).

КУЛТУРА ТАЈНОСТИ У ИНСТИТУЦИОНАЛНОМ КОНТЕКСТУ

Савремена култура тајности често превазилази своју првобитну безбедносну функцију, постајући средство заштите политичких, економских и личних интереса (Zuboff 2019, 189). Тајност се све чешће користи за избегавање јавне одговорности

и онемогућавање институционалног надзора (Schneier 2015, 78). У многим државама постаје инструмент очувања моћи – у САД, на пример, Закон о поступању са тајним подацима (*Classified Information Procedures Act – CIPA*) омогућава ограничење приступа доказима у поступцима који укључују националну безбедност (US Department of Justice 2008, 45). Ово често доводи до тога да се кључне информације не могу користити у судским процесима, што има последице по транспарентност и правду (Wikipedia 2025).

Култура тајности данас често надмашује првобитне безбедносне сврхе и прелази у механизам заштите политичких, економских и личних интереса (Zuboff 2019, 189). Уместо искључиво обезбеђења критичних информација, тајност се неретко користи за избегавање јавне одговорности и спречавање институционалног надзора (Schneier 2015, 78).

Култура тајности у Уједињеним нацијама развијала се као саставни део дипломатске праксе, нарочито у контексту међународних преговора и мировних мисија. Иако су принципи транспарентности формално заступљени, бројни механизми – попут поверљивих извештаја Савета безбедности и интерних комуникација – ограничавају јавни приступ информацијама (Duquet and Wouters 2015, 10). Тајност у процесима одлучивања често искључује јавност из увида у кључне безбедносне и политичке процесе. Ова пракса изазива критике, посебно у вези са одсуством јавне доступности података о злоупотребама у мировним мисијама, што доводи у питање одговорност институција (Wiseman 2015, 320). Иако УН трпи притиске ка већој транспарентности, дипломатске норме и безбедносни интереси и даље доминирају управљањем информацијама унутар организације.

У Европској унији институционална тајност се интензивно примењује, нарочито у оквиру трговинских преговора. Детаљи економских политика често нису доступни ни посланицима, што отежава демократски надзор над одлукама које утичу на милионе грађана (Changoe 2024, 12). Европска комисија примењује специјалне процедуре за руковање поверљивим информацијама, што додатно ограничава јавни увид у кључне политичке и економске документе (Regulation (EC) No 1049/2001). Тајни подаци у ЕУ регулисани су Одлуком Савета 2013/488 (Council Decision 2013/488/EU 2013) која дефинише четири нивоа тајности: *TRÈS SECRET UE/EU TOP SECRET* (*Државна тајна ЕУ*), *SECRET UE/EU SECRET*

(*Строго поверљиво ЕУ)*, *CONFIDENTIEL UE/EU CONFIDENTIAL (Поверљиво ЕУ)* и *RESTREINT UE/EU RESTRICTED (Итерно ЕУ)*, у зависности од потенцијалне штете по интересе Уније. За управљање овим подацима задужени су специјализовани органи, међу којима је и Европски центар за обавештајне информације и ситуације (EU INTCEN), који делује као цивилна обавештајна служба под ингеренцијом Високог представника ЕУ за спољну политику и безбедност. Поред тога, Европска комисија и Савет ЕУ развили су унутрашње протоколе који покривају индустријску, физичку и информациону безбедност, како би се осигурала заштита поверљивих података од неовлашћеног приступа.

Култура тајности у НАТО-у развијала се као основа безбедносне стратегије, с циљем заштите осетљивих информација и оперативних планова од оснивања Алијансе 1949. године. Доктрина заштите тајних података уводи класификације попут *NATO Secret*, *NATO Confidential* и *NATO Restricted,* уз строге процедуре руковања тајним подацима (Van Ham 2001, 395). Документ о политици безбедности НАТО-а (*NATO Security Policy C-M(2002)49*) поставља стандарде за заштиту класификованих информација, укључујући безбедносне провере особља и заједничке мере чланица за спречавање неовлашћеног приступа (NATO 2002, 49). Тајност унутар Алијансе је често предмет критике, нарочито у светлу потребе за демократским надзором и јавном одговорношћу. Иако НАТО оправдава рестрикције потребом за оперативном безбедношћу, критичари упозоравају на ризик од прекомерне затворености и отежаног надзора војних интервенција (Žotkevičiūtė-Banevičienė 2022, 90). Сајбер безбедност и дигитална обавештајна анализа додатно усложњавају однос између транспарентности и безбедности у савременом окружењу.

Пословна тајна је суштински део корпоративне културе тајности, механизма којим компаније настоје да заштите своје конкурентске предности и ограниче приступ кључним информацијама. Док је основна сврха пословне тајне заштита иновација, тржишних стратегија и финансијских података, она истовремено може служити као средство ограничења транспарентности и избегавања регулаторног надзора (Zuboff 2019, 189). У оквиру културе корпоративне тајности, пословна тајна обухвата различите стратегије заштите информација. Један од најучесталијих облика пословне тајне је патентна стратегија,

где компаније држе истраживања у тајности, како би спречиле конкуренцију у развоју сличних производа (Foss-Solbrekk 2021, 247).

Недоступност алгоритама представља форму корпоративне тајности којом технолошке компаније ограничавају јавни надзор над аутоматизованим одлукама, утичући на друштво и тржиште (Lexology 2021, 30). Иако правни оквири попут ЕУ Директиве 2016/943 (Directive (EU) 2016/943) и америчког Закона о заштити пословне тајне (*The Defend Trade Secrets Act*) (Clarke, Higgs and Garavan 2024), злоупотреба те заштите може довести до монопола, смањења конкуренције и ерозије демократске контроле. Регулатори попут Федералне комисије за трговину (*FTC*) и Европске комисије (European Commission) све чешће захтевају алгоритамску транспарентност као одговор на ову затвореност (Tran 2025). Тајност у корпоративном сектору тако постаје етички и правно изазован простор, у којем је нужно разграничити иновацију од прикривања штетног утицаја.

Култура тајности у Србији функционише као институционални механизам заштите осетљивих информација у секторима попут безбедности, привреде, финансија и јавне управе. Правни оквир регулише приступ и употребу поверљивих података, уз механизме који подстичу транспарентност. Основни закон који дефинише тајне податке јесте Закон о тајности података (Zakon o tajnosti podataka 2009), који се односи на информације од значаја за националну безбедност, јавни поредак и спољне послове. Допунски нормативни оквири укључују Закон о одбрани (Zakon o odbrani 2018), Закон о информационој безбедности (Zakon o informacionoj bezbednosti 2019) и Закон о критичној инфраструктури (Zakon o kritičnoj infrastrukturi 2018). Поред државних тајни, српско законодавство препознаје и друге облике штићених података, међу којима је пословна тајна, регулисана Законом о заштити пословне тајне (Zakon o zaštiti poslovne tajne 2021) и Закон о привредним друштвима (Zakon o privrednim društvima 2025).

Банкарска тајна је дефинисана Законом о банкама (Zakon o bankama 2025) који прописује ограничења у приступу подацима о клијентима. Пореска тајна је регулисана Законом о пореском поступку и пореској администрацији (Zakon o poreskom postupku i poreskoj administraciji 2020) који ограничава приступ пореским подацима. Професионална тајна обухвата поверљиве информације

у медицинском, адвокатском и другим професионалним секторима, регулисане посебним етичким кодексима и прописима. Њена примена осигурава заштиту личних и корпоративних интереса, уз истовремено поштовање етичких стандарда.

Кривично-правна заштита тајних података у Србији заснована је на члану 98 Закона о тајности података, који предвиђа санкције за неовлашћено откривање, употребу или приступ поверљивим информацијама. Одговорност може бити кривична или прекршајна, у зависности од тежине повреде. Кривични законик (Krivični zakonik RS 2024) додатно уређује дела као што су одавање службене, војне, пословне и банкарске тајне, предвиђајући казне од новчаних санкција до затвора и забране вршења функције, у складу са последицама по безбедност или економске интересе државе.

КУЛТУРА ТАЈНОСТИ У НОВОМ ДИГИТАЛНОМ ДОБУ И САЈБЕР БЕЗБЕДНОСТ

Култура тајности добија нову димензију услед развоја дигиталних технологија. Док су традиционални механизми почивали на физичкој заштити докумената и ограничењима приступа, савремена тајност све више зависи од сајбер безбедносних алата. Институције и компаније управљају осетљивим подацима уз помоћ шифровања, дигиталне аутентификације и контролисаног приступа, али се истовремено јављају ризици злоупотребе безбедносних мера ради прикривања информација од јавног значаја (Schneier 2015, 78; Singer and Friedman 2014, 152). Европска унија је Директивом *NIS2* (Directive (EU) 2022/2555, 2022) поставила стандарде за заштиту критичних инфраструктура, обавезујући државе чланице на примену стриктних мера сајбер безбедности. Међутим, изазов остаје — како обезбедити дигиталну тајност без нарушавања транспарентности и демократског надзора.

Иако је сајбер безбедност кључна за заштиту осетљивих података, у пракси се понекад користи као изговор за ускраћивање информација од јавног значаја. Институције неретко одбијају да објаве резултате безбедносних провера, позивајући се на „сајбер протоколе", упркос законској обавези транспарентности (Greenwald 2014, 89). У Европској унији, Акт о сајбер безбедности (Regulation EU 2019/881, 2019) успоставља систем сертификације безбедносних производа и услуга, док Уредба (ЕУ) 2025/37

(Regulation (EU) 2025/37, 2025) уводи мере управљања ризицима у дигиталном окружењу. Ови инструменти имају за циљ да подстакну транспарентност и спрече злоупотребу сајбер безбедности у сврху прикривања информација.

Сајбер безбедност је постала кључни аспект управљања осетљивим информацијама, али истовремено може бити злоупотребљена за масовни надзор грађана. Док су безбедносни механизми неопходни за заштиту критичних инфраструктура, постоје примери у којима су владе користиле дигиталне алате за праћење комуникација без знања јавности. Програм *PRISM,* који је открио Едвард Сноуден 2013. године, показао је како америчка влада користи дигиталне алате за прикупљање комуникација милиона људи без њиховог знања. Тај програм је омогућио Националној безбедносној агенцији (*NSA*) да добија податке од великих технолошких компанија, укључујући *Google, Facebook* и *Microsoft,* на основу судских налога издатих у оквиру Закона о надзору страних обавештајних служби *(FISA*) (Hawkins 2025, 16).

Један од најпознатијих примера злоупотребе сајбер безбедности је случај шпијунског софтвера *Pegasus*, у којем су бројне владе користиле шпијунски софтвер за праћење новинара, адвоката и опозиционих политичара. Софтвер *Pegasus*, који је развила израелска компанија *NSO Group,* омогућава тајни приступ мобилним уређајима без знања корисника, укључујући читање порука, приступ камери и микрофону, као и праћење локације (Council of Europe 2023, 9).

Напад *WannaCry* из 2017. године открио је дубоку рањивост критичних инфраструктурних система на глобалном нивоу. Рансомвер је онемогућио приступ подацима на преко 300.000 рачунара широм света, погађајући болнице, владине институције и приватни сектор (Europol 2017, 5). Користио је алат *EternalBlue* развијен од стране *NSA*, који је процурео у јавност преко хакерске групе *Shadow Brokers,* чиме је омогућено брзо ширење кроз протокол *SMB* (Greenberg 2019, 134). Последице су биле озбиљне: британска Национална здравствена служба *(NHS)* је претрпела колапс у пружању здравствених услуга, а глобалне финансијске штете су се мериле у милијардама долара (CSO Online 2024, 45). Иако је *Microsoft* издао безбедносне закрпе, многе организације нису ажурирале своје системе, омогућивши ширење напада. Европол и

друге агенције покренуле су истраге са циљем спречавања сличних инцидената у будућности (Europol 2017, 5).

Велики сајбер напади, попут хаковање компаније *SolarWinds* 2020. године, показали су како се рањивости у безбедносним системима могу искористити за масовно прикупљање података. У овом нападу, хакери су компромитовали софтвер који користе владе и корпорације широм света, омогућавајући приступ осетљивим информацијама. Напад је изведен преко злонамерног ажурирања платформе *SolarWinds Orion*, што је омогућило хакерима да добију приступ мрежама америчких владиних агенција и великих технолошких компанија (MITRE ATT&CK 2024, 45).

Цурења података и деловање узбуњивача откривају рањивост дигиталне тајности и њен потенцијал за злоупотребу. Хаковање сервера *Yahoo* 2013. године, са 3 милијарде компромитованих налога, показује да ни технолошки гиганти нису заштићени од сајбер-претњи (Zuboff 2019, 312). Последице укључују нарушавање приватности, финансијске губитке и правну одговорност, што подстиче унапређење безбедносних мера. Узбуњивачи попут Едварда Сноудена и случај *Pegasus* указују на злоупотребе надзорних алата од стране држава (Greenwald 2014, 89; Council of Europe 2023, 9). Иако узрокују потресе, оваква открића покрећу јавну расправу о транспарентности, приватности и одговорности.

Услед развоја дигиталних технологија расте значај транспарентности у сајбер безбедности. Иако се тајност често користи ради заштите критичних система, постоји ризик злоупотребе и слабог јавног надзора. Директива NIS2 и Акт о сајбер безбедности ЕУ постављају оквире за управљање ризицима, али бројни изазови остају (Regulation 2019/881 2019; Westerlund et al. 2021, 7). Примери попут *PRISM*-а, *Pegasus*-а, као и напада *WannaCry* и *SolarWinds* показују рањивост дигиталне тајности и њен потенцијал за манипулацију (Zuboff 2019, 312; Greenwald 2014, 89). Злоупотреба безбедносних мера ради прикривања информација додатно угрожава транспарентност и одговорност институција.

Будућност сајбер безбедности зависи од способности да се заштите подаци уз очување демократских вредности и јавне контроле. Иако безбедносни механизми служе за одбрану од претњи (Luknar and Jovanović 2024), неопходно је спречити да постану средство прикривања информација од јавног значаја.

Баланс између безбедности и транспарентности остаје кључни изазов дигиталног доба.

ГРАНИЦА ИЗМЕЂУ ЗАШТИТЕ И ЗЛОУПОТРЕБЕ ТАЈНОСТИ

Управљање информацијама захтева равнотежу између легитимне заштите, попут приватности и безбедности, и јавног интереса. Тајност је оправдана када штити критичне системе, али њена институционализација може ограничити демократски надзор. Када механизми тајности онемогућавају јавну контролу, они постају средство концентрације моћи без одговорности (Schneier 2015, 78; Zuboff 2019, 312).

Примери добре праксе у балансирању тајности и транспарентности обухватају механизме временски ограничене класификације, као што је аутоматска декласификација докумената од јавног значаја. Независне ревизије тајне грађе и закони о заштити узбуњивача доприносе спречавању злоупотреба и јачању одговорности. Законодавни инструменти попут права на приступ информацијама омогућавају увид у институционално одлучивање и онемогућавају да тајност постане средство прикривања незаконитости (Greenwald 2014, 89).

У појединим државама, транспарентност је унапређена кроз активну декласификацију докумената. У САД, Закон о слободном приступу информација из 1966. године омогућава приступ владиним документима и представља основу за јавни надзор, што је резултирало откривањем бројних злоупотреба власти (Harvard Law Review 2008, 45; FOIA.gov 2024). Насупрот томе, у Русији се тајност често користи као механизам прикривања корупције, уз недоступност државних уговора и финансијских извештаја под изговором националне безбедности. Истраживања указују да ова пракса ограничава јавни надзор и подстиче политичку непрозирност, односно доприноси политичкој нетранспарентности (Transparency International 2023, 75; RAND 2024).

Тајност у корпоративном сектору штити пословне интересе, али може да ограничи транспарентност и јавни надзор. Компаније често чувају резултате истраживања у тајности до званичне патентне регистрације, што, иако штити иновације, може успорити технолошки напредак (Busuioc, Curtin and Almada 2023).

Недоступност алгоритама, посебно код вештачке интелигенције, додатно отежава јавну контролу над аутоматизованим одлукама и отвара етичке и правне изазове у вези са приватношћу и дискриминацијом (Lexology 2021, 30).

Закон о слободном приступу информацијама од јавног значаја (Zakon o slobodnom pristupu informacijama od javnog značaja 2004.) представља кључни правни оквир транспарентности у Србији. Он обавезује институције да објављују податке и омогућава грађанима увид у рад јавне управе. Међутим, примена је често ограничена административним препрекама, селективним тумачењем и позивањем на изузетке попут националне безбедности (Media Observatory 2017). Пораст броја жалби због ускраћивања информација указује на потребу за јачањем механизама надзора и примене закона (Global Freedom of Expression 2013).

ЗАКЉУЧНА РАЗМАТРАЊА

Култура тајности је историјски служила као средство политичке моћи од оријенталних деспотија до савремених дигиталних система. У старим империјама попут Египта, Персије и Кине, она је омогућавала централизовано управљање и апсолутну контролу (Wittfogel 1957, 112), док је у Европи постала саставни део дипломатских и војних стратегија. Тоталитарни режими XX века, попут Совјетског Савеза и нацистичке Немачке, усавршили су механизме надзора и цензуре (Barros 2019, 78). У дигитално доба, тајност се трансформише кроз алгоритамски надзор, масовно прикупљање података и сајбер безбедност као нове облике контроле јавног дискурса (Birchall 2016, 45). Док су традиционални модели почивали на физичком ограничавању приступа, модерни користе технологију као средство дигиталне контроле. Ово отвара нова правна, етичка и безбедносна питања: иако је заштита података важна ради безбедности и приватности, прекомерна тајност може угрозити демократију, транспарентност и јавни надзор.

Сајбер безбедност, иако темељ заштите података, често поставља питање граница између потребне тајности и јавног интереса. Регулативе попут NIS2 и Акта о сајбер-безбедности ЕУ усмеравају се ка техничкој отпорности, али не гарантују транспарентност у пракси. Примери узбуњивача, као што је Едвард Сноуден и афере попут *Panama Papers* откривају да дигиталне

структуре могу постати алати прикривања, а не само заштите. Суочавање са овим парадоксом захтева интеграцију демократског надзора у технолошке оквире управљања безбедношћу (Greenwald 2014, 89; Zuboff 2019, 312).

Савремено друштво мора обезбедити одрживу равнотежу између заштите података и транспарентности, нарочито у области сајбер безбедности. Иако технолошка средства повећавају степен заштите, све чешће се користе за ограничење јавног приступа информацијама (Zuboff 2019, 312). Да би се спречила злоупотреба тајности, неопходни су правни механизми који омогућавају јавну контролу, попут декласификације, ревизија тајних докумената и заштите узбуњивача. Такве мере осигуравају да тајност остане у функцији јавног интереса и демократских вредности (Greenwald 2014, 89).

Све већа примена вештачке интелигенције у управљању информацијама отвара нова етичка питања (Luknar and Jovanović, 2023) посебно у контексту аутоматске класификације података. Алгоритми могу самостално означити податке као поверљиве, без људске интервенције, што доводи до ризика неконтролисане тајности и концентрације моћи (Cronin 2020, 58). Недовољна транспарентност алгоритамских процеса ограничава јавни приступ информацијама од значаја. Иако дигитална ера нуди алате за ефикаснију заштиту података, неопходно је успоставити границу између оправдане безбедности и злоупотребе тајности. Будући изазов остаје развој механизама који омогућавају транспарентност алгоритама уз очување безбедносних интереса (Schneier 2015, 245).

Будућност управљања тајношћу зависи од способности друштва да одржи равнотежу између безбедности и транспарентности. Како се технологија развија, механизми јавног надзора и одговорног управљања информацијама постају не само важни, већ и неопходни за очување демократских вредности.

РЕФЕРЕНЦЕ

Andress, David. 2006. *The Terror: The Merciless War for Freedom in Revolutionary France.* New York: Farrar, Straus and Giroux.

Andrew Gordon, 2014. *A Modern History of Japan: From Tokugawa Times to the Present*. Oxford: Oxford University Press.

Balmer, Brian 2016. *Secrecy and Science.* London: Routledge.

Barros, Robert. 2019. *Secrecy and Authoritarian Regimes*. Cambridge: Cambridge University Press.

Bauer, Nicole. 2023a. *Keeping you in the Dark: The Bastille Archives and Police Secrecy in Eighteenth-century France*. Cambridge: Cambridge University Press.

Bauer, Nicole. 2023b. "Secrecy in the Late Ancien Regime." *The French History Podcast*. 10 June 2023. https://www.thefrenchhistorypodcast.com/secrecy-in-the-late-ancien-regime-with-dr-nicole-bauer/.

BBC. 2018. "Edward Snowden surveillance powers ruled unlawful." 13 September 2018. https://www.bbc.com/news/uk-45510662.

Berend, Ivan. 2023. *From the Soviet Bloc to the European Union.* Cambridge: Cambridge University Press.

Birchall, Claire. 2016. *"*Managing Secrecy in the Digital Age*"*. *International Journal of Communication* 10: 152–163.

Bok, Sissela. 1989. *Secrets: On the Ethics of Concealment and Revelation.* New York: Vintage Books.

Brittanica 2025. "The Fascist Era in Italy." Accessed 12 June 2025. https://www.britannica.com/place/Italy/The-end-of-constitutional-rule.

Browder, George C. 1996. *Hitler's Enforcers: The Gestapo and the SS Security Service in the Nazi Revolution*. New York: Oxford University Press.

Busuioc, Madalina, Deirdre Curtin, and Marco Almada. 2023. "Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act." *European Law Open* 1 (2023): 63–80. doi: 10.1017/elo.2022.36.

Changoe, Audrey 2024. "EU-Mercosur Deal Concluded in Secrecy: A Tragic Blow to the Planet and Democracy." *Climate Action Network Europe.* 6 December 2024. https://caneurope.org/eu-mercosur-deal-concluded-in-secrecy-a-tragic-blow-to-the-planet-and-democracy/.

Ćirković, Sima. 1995. *Srbi u srednjem veku.* Beograd*:* IDEA

Clarke, Nicholas, Malcolm Higgs, and Thomas Garavan. 2024. "Legitimating Organizational Secrecy." *Journal of Business Ethics* 197 (1): 19–38. doi: 10.1007/s10551-024-05763-3.

Connelly, Matthew. 2023. *Past, Present and Future of Government Secrecy*. New York: Pantheon.

Council of Europe. 2023. "Pegasus Spyware Called into Question by PACE." *Council of Europe*. Last modified 16 October 2023. https://www.coe.int/en/web/freedom-expression/-/pegasus-spyware-called-into-question-by-pace.

Council of the European Union. 2013. Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU). *Official Journal of the European Union*, L 274, 15 October 2013, 1–50. https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng/.

Cronin, John. 2020. *Artificial Intelligence and Data Governance: Ethical Challenges in Automated Decision-Making.* Oxford: Oxford University Press.

CSO Online. 2024. "UK sets out new cyber resilience plan to protect NHS from cyberattacks." https://www.csoonline.com/article/574821/uk-sets-out-new-cyber-resilience-plan-to-protect-nhs-from-cyberattacks.html.

Dandelot, Marc. 2018. "*Évolution* et enjeux du droit d'accès aux documents administratifs depuis la loi du 7 octobre 2016 pour une République numérique." *Revue française d'administration publique* 165 (2018): 127–133.

Decalo, Samuel. 1985. "African Personal Dictatorships." *The Journal of Modern African Studies* 23 (2): 209–237. doi:10.1017/S0022278X0000015X.

Dević Nemanja. 2021. *Za Partiju i Tita: partizanski pokret u Srbiji 1941–1944.* Beograd: Službeni glasnik.

Duquet, Sanderijn, and Jan Wouters. 2015. "*Diplomacy, Secrecy and the Law*." *Working Paper No. 151*. Leuven: Leuven Centre for Global Governance Studies.

Ekwo, Uchenna. 2013. "Culture of Secrecy and Opaque Leadership in Africa." *Center for Media and Peace Initiatives*. https://www.mycmpi.org/culture-of-secrecy-and-opaque-leadership-in-africa/.

Emmons, Terence. 2017. *History and Politics in Russia before the Revolution*. Leiden: Brill.

European Parliament and Council. 2016. Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance). Official Journal of the European Union, L 157, 15 June 2016, 1–18 https://eurlex.europa.eu/eli/dir/2016/943/oj/eng/

European Parliament and Council. 2022. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European

Union, L 333, 27 December 2022, pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng/.

Europol. 2017. *Cybercrime Trends and Ransomware Attacks: The Case of WannaCry*. The Hague: Europol Press.

FOIA.gov. 2024. "Freedom of Information Act Portal." *U.S. Department of Justice*. https://www.foia.gov/.

Foss-Solbrekk. 2021. "Three Routes to Protecting AI Systems Under IP Law 247." *Journal of Intellectual Property Law & Practice* 16 (3): 247–258. doi:10.1093/jiplp/jpab033.

Galván, Javier. 2013. *Latin American Dictators of the 20th Century.* Jefferson: McFarland and Company.

German Culture. n.d. "The Underground Cities of Germany: Bunkers, Tunnels, and Hidden Secrets." Accessed 25 June 2025. https://germanculture.com.ua/history/the-underground-cities-of-germany-bunkers-tunnels-and-hidden-secrets/.

Global Freedom of Expression. 2013. "Global Freedom of Expression Report 2013." *Columbia University*. https://globalfreedomofexpression.columbia.edu/.

Greenberg, Andy 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Metropolitan Books.

Habberstad, Luke. 2023. *Leaking Rulers and Confidential Officials: Secrecy and Status of Early Chinese Political Culture.* Cambridge: Cambridge University Press.

Harrison, Mark. 2023. *Secret Leviathan: Secrecy and State Capacity under Soviet Communism*. Stanford: Stanford University Press.

Harvard Law Review. 2008. *Freedom of Information and Government Accountability*. Cambridge: Harvard Law Review Association.

Hawkins, Kate. 2025. "What Is the PRISM Program? NSA, Edward Snowden and Government Surveillance in 2025." *Cloudwards*. Last modified 16 May 2025. https://www.cloudwards.net/prism-snowden-and-government-surveillance/.

Haynes, Alan. 2011. *The Elizabethan Secret Services*. Stroud: The History Press.

History State Gov. 2025. "Breakup of Yugoslavia." *U.S. Office of the Historian*. https://history.state.gov/milestones/1989–1992/breakup-yugoslavia.

Imperial War Museums. 2024. "The Secret War." https://www.iwm.org.uk/history/secret-war-what-you-need-to-know.

International Consortium of Investigative Journalists (ICIJ). 2016. "ICIJ releases offshore Panama Papers Data." https://www.icij.org/inside-icij/2016/05/icij-releases-panama-papers-offshore-company-data/.

International Consortium of Investigative Journalists (ICIJ). 2023. "Where are the key Panama Papers figures 7 years later." https://www.icij.org/investigations/panama-papers/where-are-they-now-2023/.

Krivični zakonik, „Službeni glasnik RS". br. 85/05; 88/05, 107/05; 72/09, 111/09; 121/12; 104/13, 108/14, 94/16, 35/19 i 94/2024.

Lebovic, Sam. 2016. "The Surprisingly Short History of American Secrecy." *Perspectives On History*. https://www.historians.org/perspectives-article/the-surprisingly-short-history-of-american-secrecy-september-2016/.

Lexology. 2021. "Algorithmas and Trade Secrets: How to Meet Transparency Obligations." https://www.lexology.com/pro/content/algorithms-and-trade-secrets-how-meet-transparency-obligations.

Luknar, Ivana, and Filip Jovanović. 2023. "An Ethics for Emerging Technologies." In *Conference on Advances in Science and Technology COAST 2023*. May 31–June 3.

Luknar, Ivana, and Filip Jovanović. 2024. "Various types of cyber threats." *Srpska politička misao* 83 (1): 161–177. doi: 10.5937/spm83-46059.

MacMullen, Ramsay. 1988. *Corruption and the Decline of Rome.* New Haven and London: Yale University Press.

Matthews, John.1989. *The Roman Empire of Ammianus,* Michigan: Michigan Classical Press.

McCauley, Martin. 2025. *Russia from 1801 to 1917*. London: Routledge.

Media Observatory. 2017. "Serbia: the hard fight for information." 17 February 2017. https://mediaobservatory.net/radar/serbia-hard-fight-information.

Minster, Christopher. 2025. "Latin American Dictators – Leaders in Complete Control." *ThoughtCo*. Last modified 1 May 2025. https://www.thoughtco.com/latin-american-dictators-2136482.

MITRE ATT&CK®. 2024. "SolarWinds Compromise, Campaign C0024." Last modified 3 September 2024. https://attack.mitre.org/campaigns/C0024/.

Moran, Christopher. 2014. *Classified: Secrecy and the Modern State*. Cambridge: Cambridge University Press.

NATO. 2002. *Security Within the North Atlantic Treaty Organization*. C-M(2002)49.

RAND. 2024. "2024 RAND Annual Report." Accessed 29 January 2025. https://www.rand.org/pubs/corporate_pubs/CPA1065-5.html.

Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents. Official Journal of the European Communities, L 145, May 31, 2001. https://eur-lex.europa.eu/eli/reg/2001/1049/oj.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) *OJ L 151, 7.6.2019, 15–69.*

Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (Text with EEA relevance). 2025. *Official Journal of the European Union*, L 15, 15 January 2025. https://eur-lex.europa.eu/eli/reg/2025/37/oj/eng.

Reporters Without Borders. 2021. "Pegasus Project: Worldwide Investigation." Paris: RSF.

Royal Family of Serbia. n.d. "History of Serbia from 1815 to 1868." https://royalfamily.org/about-serbia/history-of-serbia-from-1815-to-1868.

Schneier, Bruce. 2015. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.

Serbia Info. 2025. "History of Serbia: Medieval Serbia. 2025. History of Serbia: Medieval Serbia (7th–14th century)." *Archive of Serbia*. Accessed 25 June 2025. https://www.arhiva.serbia.gov.rs/enc/history/medieval.html.

Singer, Peter, and Allan Friedman. 2014. *Cyber Security and Cyber War: What everyone needs to know.* Oxford: Oxford University Press.

Smith, Michael. 2010. *The Secrets of Bletchley Park: The Codebreakers Who Changed the World*. London: Biteback Publishing.

SrpskiKod. 2025. "The First Serbian Uprising." *Serbia Historical Archive*. https://www.srpskikod.org/sr/.

Stevens, Kathryn. 2013. "Secrets in the Library: Protected Knowledge and Professional Identity in Late Babylonian Uruk." *Iraq* 75: 211–253. doi: 10.1017/S0021088900000474/.

Stojančević, Vladimir. 2004. *Obaveštajna služba u Karađorđevoj i Miloševoj Srbiji.* Beograd: Novinsko-izdavački centar Vojska.

Thompson, John B. 2000. *Political Scandal: Power and Visibility in the Media Age*. Cambridge: Polity Press.

Timofejev, Aleksej i Milan Piljak. 2017. *Ruska revolucija 1917. u očima Kraljevine Srbije.* Višegrad: Andrićev institut.

Total Military Insight. 2024. "The Role of Secrecy in Military Operations." Accessed 7 June 2025. https://totalmilitaryinsight.com/.

Tran, Bao. 2025. "Are Algorithms Protectable Under Patent or Trade Secret Law?" *Patentpc*. 14 June 2025. https://patentpc.com/blog/algorithms-protectable-under-patent-or-trade-secret-law/.

Transparency International. 2023. "Global Corruption Report: Government Accountability and Secrecy."

Tsuneishi, Keiichi. 2005. "Unit 731 and the Japanese Imperial Army's Biological Warfare Program." *The Asia-Pacific Journal: Japan Focus*. https://apjjf.org/tsuneishi-keiichi/2194/article.

U.S. Department of Justice. 2008. "Synopsis of Classified Information Procedures Act." https://www.justice.gov/archives/jm/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa.

United States Congress. 2016. "Defend Trade Secrets Act of 2016, Public Law 114–153, codified at 18 U.S.C. § 1836 et seq." https://www.congress.gov/bill/114th-congress/senate-bill/1890/.

Van Ham, Peter. 2001. "Security and Culture in NATO." *Security Dialogue* 32 (4): 409–426. doi: 10.1177/0967010601032004005.

Wellerstein, Alex. 2021. *Restricted Data: The History of Nuclear Secrecy in the United States*. Chicago: University of Chicago Press.

Westerlund, Mika, Diane A. Isabelle, and Seppo Leminen. 2021. "The Acceptance of Digital Surveillance in an Age of Big Data." *Technology Innovation Management Review* 11 (3): 16–27. doi: 10.22215/timreview/1427.

Wikipedia contributors. 2025. "Classified Information Procedures Act." *Wikipedia*. Last modified June 2025. https://en.wikipedia.org/wiki/Classified_Information_Procedures_Act.

Wiseman, Geoffrey. 2015. "Diplomatic Practices at the United Nations." *Cooperation and Conflict* 50 (3): 316–333. doi: 10.1177/0010836715574916.

Wittfogel, Karl. 1957. *Oriental Despotism: A Comparative Study of Total Power*. New Haven: Yale University Press.

WorldAtlas. 2025. "What Was Russia Like Before the Russian Revolution?" Last modified 2025. https://www.worldatlas.com/history/what-was-russia-like-before-the-russian-revolution.html.

Zakon o bankama, „Službeni glasnik RS”, br. 107/2005, 91/2010, 14/2015 i 19/2025.

Zakon o informacionoj bezbednosti, „Službeni glasnik RS”, br. 6/16, 94/17, 77/19.

Zakon o kritičnoj infrastrukturi, „Službeni glasnik RS”, br. 87/18.

Zakon o odbrani, „Službeni glasnik RS”, br. 116/07, 88/09, 104/09; 10/15; 36/18.

Zakon o poreskom postupku i poreskoj administraciji, „Službeni glasnik RS”, br. br. 80/2002, 84/2002 - ispr., 23/2003 - ispr., 70/2003, 55/2004, 61/2005, 85/2005 - dr. zakon, 62/2006 - dr. zakon, 63/2006 - ispr. dr. zakona, 61/2007, 20/2009, 72/2009 - dr. zakon, 53/2010, 101/2011, 2/2012 - ispr., 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 - autentično tumačenje, 112/2015, 15/2016, 108/2016, 30/2018, 95/2018, 86/2019, 144/2020, 96/2021, 138/2022 i 94/2024.

Zakon o privrednim društvima, „Službeni glasnik RS”, br. 36/11, 99/11, 83/14, 5/15, 44/18, 95/18, 91/19, 109/21, 19/25.

Zakon o tajnosti podataka, „Službeni glasnik RS”, br. 104/09.

Zakon o zaštiti poslovne tajne, „Službeni glasnik RS”, br. 53/21.

Žotkevičiūtė-Banevičienė, Agnietė. 2022. “The Cultural Element in NATO Military Doctrines: Important, but a Declarative Issue?” *Politologija* 108 (4): 85–115. doi:10.15388/Polit.2022.108.3.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Goran D. Matić*

Office of the National Security Council and Classified Information Protection

THE CULTURE OF SECRECY IN THE DIGITAL AGE: BETWEEN NECESSITY, ABUSE AND CYBERSECURITY

Resume

The secrecy culture represents an institutionalised information management model that has evolved from ancient civilisations to modern digital societies. Historically, secrecy was justified by security and political interests, but often transformed into a mechanism for power concentration and restriction of democratic oversight. In the Roman Empire, information was stored in formal archives (tabularia), while the Chinese dynasties Qin and Han developed complex bureaucratic mechanisms for managing confidential data. Modern secrecy models, such as the D-Notice system in the United Kingdom, continue to institutionalise control over information. Digital transformation has expanded the concept of secrecy through algorithms and mass surveillance, enabling new mechanisms for concealing and manipulating data. Examples such as the misuse of Pegasus spyware or the widespread classification of public contracts show that technology facilitates information management and enables more subtle forms of secrecy. At the same time, whistleblowers like Edward Snowden highlight the vulnerability of digital privacy, while legal instruments such as the U.S. Freedom of Information Act and declassification initiatives promote transparency. This paper analyses the historical development of the culture of secrecy, its transformation in the digital age, and contemporary challenges in balancing legitimate security protection with the need for transparency. Special attention is given to public oversight mechanisms, including freedom of information laws, declassification processes, and the role of whistleblowers in preserving transparency as a foundation of democratic society.

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

Keywords: politics, security, secrecy culture, cybersecurity, digital society, public interest, data protection, transparency.

* Овај рад је примљен 14. октобра 2025. године, а прихваћен на састанку Редакције 5. децембра 2025. године.