Ненад КОВАЧЕВИЋ[*]
Министарство одбране
Проф. др Младен МИЛОШЕВИЋ[**]
Факултет безбедности, Универзитета у Београду

ДОИ: 10.5937/bezbednost2201093K
УДК: 004.63:343.452(497.11)
Прегледни научни рад
Примљен: 1. 1. 2022. године
Датум прихватања: 1. 4. 2022. године

Заштита тајних података у дигиталној форми – безбедносни и кривичноправни аспекти

Апстракт: *Заштита тајних података један је од приоритетних задатака субјеката националне безбедности, јер се њиховим очувањем спречава настанак штете по важне јавне интересе. Посебан безбедносни изазов настаје с појавом тренда да се руковање подацима значајним делом премешта у сајбер простор, што, иако доноси велике практичне предности, рађа и разноврсне ризике по њихову безбедност. Заштита тајних података је предмет посебног закона, који је, са пратећом подзаконском регулативом, детаљно регулише. Овај рад је посвећен анализи стварног стања у области заштите дигиталних тајних података у погледу примене кључних законских решења, као и разматрању улоге и значаја кривичног права, односно квалитета и међусобне усаглашености важећих кривичноправних норми. Ради утврђивања имплементационих проблема аутори су укратко представили нормативни оквир и спровели интервју са експертом, чиме су настојали да осветле практични безбедносни аспект феномена заштите тајних података у дигиталној форми. Анализом одредби Кривичног законика и казнених одредби Закона о тајности података, аутори уочавају системску неусаглашеност релевантних законских одредби и предлажу решења de lege ferenda.*

Кључне речи: *тајни податак, кривичноправна и безбедносна заштита, подаци у дигиталном облику.*

[*] nenad.kovacevic7@yahoo.com
[**] milosevic@fb.bg.ac.rs

Увод

Закон о тајности података[1] (ЗТП) први је закон који на јединствен и систематичан начин уређује материју заштите тајних података. Пре његовог доношења, предметна област је била уређена по ресорном моделу, односно одредбама појединих закона и подзаконским актима у одговарајућим секторима (Министарство одбране, Министарство унутрашњих послова, Безбедносно-информативна агенција и др.). Заштита података у дигиталном облику је предмет и Закона о информационој безбедности[2] (ЗИБ). Стога, анализа безбедносног аспекта заштите тајних података подразумева првенствено анализу стварних резултата имплементације ова два закона.

Кривичноправни аспект заштите тајних података анализиран је кроз проучавање релевантних одредби главног и споредног кривичног законодавства. У том циљу, анализиран је Кривични законик[3], компаративно са одговарајућим казненим одредбама ЗТП-а.

Имајући у виду да се ток имплементације може оцењивати искључиво квалитативним методама, спроведен је интервју са експертом који је задужен за послове заштите података у дигиталном облику, органу јавне власти.

Спровођење истраживања реализовано је применом полустандардизованог интервјуа. Реч је о типу научног разговора којим се, на најефикаснији начин, могу остварити отвореност и флексибилност као кључне карактеристике квалитативног истраживачког приступа. Интервју је формално и садржајно разрађен, тако да је говор испитаника вођен унапред припремљеним питањима (Ђурић, 2016). Основни истраживачки циљ спроведеног интервјуа било је прикупљање података који нису у довољној мери доступни широј јавности, а значајно доприносе расветљавању предмета истраживања.

Правни оквир – кратак приказ

Доношењем Закона о тајности података и пратећих подзаконских аката успостављен је нормативни оквир за рад са тајним подацима, укључујући и оне који се обрађују у ИКТ системима.

1 Закон о тајности података (Службени гласник Републике Србије, бр. 104/09).

2 Закон о информационој безбедности (Службени гласник Републике Србије, бр. 6/16, 94/17, 77/19).

3 Кривични законик (Службени гласник Републике Србије, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19).

Поред ЗТП-а, од највећег значаја за уређење заштите тајних података у ИКТ системима јесу: ЗИБ, Уредба о посебним мерама заштите тајних података у ИКТ системима, Уредба о посебним мерама надзора над поступањем са тајним подацима, Уредба о посебним мерама физичко-техничке заштите тајних података, Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, као и Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године.[4] Поменути прописи имају и међународни значај због обавезе државе да усагласи законодавство са препорукама Европске уније[5] (Матић, 2014).

Практични проблеми у примени прописа о заштити тајних података у дигиталном облику

Због значаја и улоге превенције и заштите од безбедносних ризика у ИКТ системима у раду са подацима, као и због чињенице да са овом облашћу шира јавност није упозната у довољној мери, обављен је интервју са експертом који има вишегодишње искуство на пословима који обухватају активности у вези са активним учешћем у изради нацрта прописа у области информационе безбедности и изради прописа који се односе на њу.

На питање које се односи на *степен правне уређености* информационе безбедности у Републици Србији, саговорник одговара да је наведена област уређена на релативно високом нивоу, што по-

4 Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима (Службени гласник РС, бр. 53/11); Уредба о посебним мерама надзора над поступањем са тајним подацима (Службени гласник РС, бр. 90/11) ; Уредба о посебним мерама физичко-техничке заштите тајних података (Службени гласник РС, бр. 097/11); Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја (Службени гласник РС, бр. 94/16); Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године (Службени гласник РС, бр. 53/17).

5 Република Србија је, поред Босне и Херцеговине, последња земља у Европи која је донела Закон о информационој безбедности. Поменути закон је усклађен са Директивом Парламента и Савета у вези са мерама за осигурање високог нивоа мрежне и информационе безбедности у ЕУ (НИС директива). Измене и допуне закона уследиле су 2017. и 2019. године, а биле су, између осталог, извршене и због потпуног усклађивања са НИС директивом. У циљу ближег уређења појединих одредби ЗИБ-а донета су и одређена подзаконска акта (шест уредби и један правилник). Иначе, у контексту заштите тајних података допринос ЗИБ-а, између осталог, односи се на ближе уређење области криптобезбедности и заштите од компромитујућег електромагнетног зрачења (Маркагић, 2018; VanEck, 1985).

тврђују и званични подаци[6] Међународне уније за телекомуникације, као и подаци[7] са естонског сајта Националних индекса сајбер безбедности (О сајбер безбедности: Путник, 2009).

Закон о информационој безбедности углавном је усклађен са НИС директивом ЕУ, а посвећеност хармонизацији правног оквира са ЕУ, сматра он, потврђена је новелирањем ЗИБ-а 2019. године.

Ипак, истиче да прописима није довољно уређена област критичне информационе инфраструктуре (КИИ). Закон о критичној инфраструктури донет је 2018. године, али пропратни прописи којима се ближе уређује ова област још увек нису донети. Као посебан проблем истиче непостојање јединствене методологије за идентификовање критичне инфраструктуре.

На питање у *вези са степеном имплементације закона и других прописа* који уређују ову област, саговорник износи да се она нарочито реализује у делу који се односи на превенцију и реаговање на инциденте. У складу са законом, поред постојећег центра за превенцију безбедносних ризика у ИКТ системима (ЦЕРТ) у Академској мрежи Србије, основан је одређен број нових ЦЕРТ-ова (послови Националног ЦЕРТ-а су у надлежности Регулаторне агенције за електронске комуникације и поштанске услуге – РАТЕЛ). Узимајући у обзир достигнуте нивое капацитета ЦЕРТ-ова, МУП ЦЕРТ и Национални ЦЕРТ су, према испитанику, изнад осталих. Испитаник наглашава да су поменути ЦЕРТ-ови, између осталих[8], препознати у међународној стручној заједници (на сервису *Trusted Introducer*[9]*, глобалном форуму тимова за реаговање на инциденте и безбедност ФИРСТ, као и у Агенцији ЕУ за сајбер безбедност ЕНИСА). Испитаник сматра да су сви ЦЕРТ-ови у Србији оперативни, нарочито у делу који се односи на реаговање у случају идентификовања инцидента. За важан корак сматра оснивање Тела за координацију послова информационе безбедности*[10]*.*

6 На сајту ИТУ, према подацима за 2018, Србија је рангирана на 34. месту у Европи, односно 58. месту у свету.

7 На сајту НЦСИ Србија је рангирана на 17. месту.

8 На сајту ЕНИСА излистани су и следећи ЦЕРТ-ови из Србије: *AMRES-CSIRT*, *CERT MUP*, *MUP CERT*, *SHARE CERT*, *SRB-CERT* и *UNICOM CERT*.

9 Сервис *Trusted Introducer* основала је 2000. године Европска заједница ЦЕРТ како би се задовољиле заједничке потребе и изградила инфраструктура услуга која пружа виталну подршку свим тимовима за безбедност и реаговање на инциденте.

10 Ово тело основано је Одлуком о образовању Тела за координацију послова информационе безбедности (Службени гласник РС, бр. 24/16, 53/17, 79/17, 112/17, 93/18).

На питање у вези са уоченим проблемима у примени прописа саговорник је истакао да су проблеми превасходно кадровске и техничко-технолошке природе, и условљени финансијским фактором. Србија (као и многе друге земље) још увек нема решење за спречавање одласка кадрова специјализованих за послове информационе безбедности из државних органа. Разлог види у немогућности државних органа да буду конкурентни послодавци на тржишту рада у односу на приватни сектор. Са техничко-технолошког аспекта, проблеми се односе на набавку наменске опреме и алата (софтверских решења). Испитаник указује на проблеме који произлазе из терминолошке и појмовне неусаглашености ЗИБ-а и ЗТП-а, као и непоштовања законом прописаних рокова за доношење подзаконске регулативе. Он наглашава и да прописима није дефинисано надлежно тело за сертификацију ИКТ система, што онемогућава руковање страним тајним подацима у тим системима.

На питање у вези са *оствареном сарадњом у циљу побољшања информационе безбедности*, саговорник сматра да постоји врло добра сарадња на националном (интерресорна) и међународном плану. Сарадња на међународном плану постоји на свим нивоима и постепено се развија. Регионална сарадња је релативно добра и углавном се своди на размењивање информација релевантних за информациону безбедност (непосредни контакти ЦЕРТ-ова). Успостављена је сарадња са међународном мрежом центара за превенцију безбедносних ризика у ИКТ системима. Међународна сарадња се испољава и кроз донације, с циљем подизања капацитета информационе безбедности у Србији.

Испитаник истиче сарадњу са Интерполом и Организаијом за европску безбедност и сарадњу (ОЕБС). У контексту те сарадње посебно наглашава допринос Србије у вези са спонзорством над имплементацијом мера ОЕБС-а за изградњу поверења број 9[11]. Србија је активан учесник у неформалној радној групи ОЕБС-а за сајбер безбедност, а учествује и у другим активностима ОЕБС-а.[12]

На питање које се односи на *предлоге и визије по питању превазилажења постојећих проблема и подизање капацитета*, саговор-

11 Све мере ОЕБС за изградњу поверења могу се наћи у Одлуци Сталног савета ОЕБС бр. 1202.

12 На основу Одлуке бр. 1202 – мере ОЕБС-а за изградњу поверења за смањење ризика од конфликата који произилазе из употребе информационих и комуникационих технологија.

ник је истакао да је приоритет изградња потпуног и усаглашеног правног оквира. Са организационог аспекта сматра да би се интеграцијом Националног ЦЕРТ-а и ЦЕРТ-а републичких органа у један ЦЕРТ обезбедила већа ефикасности у примени мера информационе безбедности. Поред наведеног сматра да би било веома значајно дати шира овлашћења Телу за координацију послова информационе безбедности, у контексту правовременог и адекватног реаговања на идентификоване инциденте у ИКТ системима. Постојеће капацитете ЦЕРТ-ова могуће је побољшати и бољом сарадњом јавног и приватног сектора, академске заједнице и невладиних организација. Важан допринос подизању капацитета ЦЕРТ-ова, према његовом мишљењу, представљала би израда конкретних процедура за поступање у различитим ситуацијама појаве инцидента, као и периодично увежбавање запослених у спровођењу тих процедура.

Кривичноправна заштита тајних података

Члан 98 ЗТП-а прописује који облици противправног понашања према тајним подацима представљају кривично дело. Основни облик кривичног дела (које, иначе, нема законски назив) чини онај ко, без овлашћења, „непозваном лицу саопшти, преда или учини доступним податке или документа који су му поверени или до којих је на други начин дошао или прибавља податке или документа, а који представљају тајне податке са ознаком тајности ‘интерно’ или ‘поверљиво’, одређене према овом закону“ (члан 98, став 1 ЗТП). Прописана казна је затвор у трајању од три месеца до три године. Радња је алтернативно постављена и може се остварити на три начина: 1. када овлашћено лице (свако лице које је у законитом поседу податка или документа у ком се податак налази) учини доступним податке и документе непозваном лицу; 2. уколико непозвано лице (које је на незаконит начин дошло у посед тајне) исту пренесе трећем, такође неовлашћеном лицу; 3. када непозвано лице незаконито прибавља податке или документе који садрже тајни податак (Miloševi ć, 2021).

Вреди поменути да је у правно-техничком смислу одредба могла да буде прецизније формулисана (додавањем речи „незаконито“ или „противправно“ испред речи „прибавља документе...“).

Први квалификовани облик предвиђен је у члану 98 став 2 ЗТП-а. Квалификаторна околност је степен тајности документа или податка

који је противправно откривен. Реч је о степену „строго поверљиво“, а предвиђена је казна од шест месеци до пет година затвора. Други тежи облик, за који је запрећена казна затвора у трајању од једне до десет година, постојаће уколико је непозваном лицу неовлашћено откривен податак који је степенован као државна тајна.

Трећи тежи облик је стипулисан у облику алтернативне радње извршења, с тим што се односи на сва три претходна облика, уз посебне запрећене казне. Квалификаторне околности код овог облика су: користољубље, намера „објављивања или коришћења тајних података у иностранству“ и вршење дела за време ратног или ванредног стања. Довољно је да постоји једна од три наведене квалификаторне околности. Уколико би учинилац остварио две или све три квалификаторне околности, то би се могло узети у обзир приликом одмеравања казне (Стојановић, 2018; Вуковић, 2020).

Уколико је испуњена барем једна од наведених околности, „учинилац ће се казнити за дело из става 1. овог члана затвором од шест месеци до пет година, за дело из става 2. затвором од једне до осам година, а за дело из става 3. затвором од пет до петнаест година“ (члан 98, став 4 ЗТП-а).

Став 5 члана 98 санкционише нехатно одавање тајног податка. За нехатно извршење дела из става 1 прописана је казна затвора до две године, а из става 2 од три месеца до три године, док је за дело из става 3 учињено из нехата прописана казна од шест месеци до пет година затвора.

Озбиљан проблем у правно-догматском и практичном смислу стварају системске неусаглашености одговарајућих одредби КЗ-а и овог члана ЗТП-а. КЗ садржи следеће инкриминације: одавање државне тајне (члан 316), одавање службене тајне (члан 369) и одавање војне тајне (члан 415).

Члан 316 КЗ-а предвиђа: „Ко неовлашћено непозваном лицу саопшти, преда или учини доступним податке или документе који су му поверени или до којих је на други начин дошао, а који представљају државну тајну, казниће се затвором од једне до десет година“. Ово дело се разликује од сродне инкриминације шпијунаже по томе што није присутан елемент иностраности (Стојановић, 2018; Ђорђевић, 2014; Делић, 2021).

Став 2 члана 316 КЗ-а предвиђа привилеговани облик, који је присутан ако учинилац другом лицу саопшти податке (или документа) „до којих је противправно дошао, а за које је знао да пред-

стављају државну тајну“. Прописана је казна од шест месеци до пет година затвора. Други лакши облик (члан 316, став 4) постоји ако је државна тајна одана из нехата (прописана казна од шест месеци до пет година).

Тежи облик је прописан у ставу 3 овог члана. Квалификаторне околности представљају време (уколико је оно учињено током ратног стања) или последица (ако је дошло до угрожавање безбедности, економске или војне моћи земље). Запрећена казна је затвор у трајању од три до петнаест година.

Овде је, међутим, приметна и једна озбиљна законска неусаглашеност. Члан 321 КЗ-а, који прописује најтеже облике кривичних дела против уставног уређења и безбедности државе, у ставу 3 одређује да ће се, између осталих, кривична дела из чл. 314–319, казнити са најмање десет година затвора или доживотним затвором ако су учињена током ратног или ванредног стања или оружаног сукоба. Дакле, ако је одавање државне тајне учињено за време ратног стања, није јасно која је запрећена казна, јер законодавац очигледном омашком прописује два различита распона (од три до петнаест година затвора ако се суди по члану 316 став 3, или најмање десет година затвора односно доживотни затвор уколико се суди по члану 321 став 3) (Милошевић, 2010).

Због начела законитости, као и правила *in dubio pro reo*, свакако би требало применити одредбу члана 316 став 3. Ипак, заиста је неопходна законодавна интервенција како би се ова неусаглашеност отклонила. То посебно стоји ако имамо у виду да бисмо језичким и екстензивним тумачењем важећих решења морали да закључимо да је казна из члана 321 став 3 предвиђена у случају да је државна тајна одана за време ванредног стања или другог оружаног сукоба (осим рата). Према томе, запрећена је строжа казна за одавање државне тајне у време ванредног стања или оружаног сукоба него у време рата.

У члану 316 став 5 КЗ даје и дефиницију појма државне тајне. Законодавац уводи формални и материјални критеријум (Стојановић, Перић, 2011: 269; Делић, 2020). У формалном смислу државна тајна је податак или документ који је законом или другим општим актом односно појединачним актом надлежног органа донетим у складу са законом прогласио државном тајном. Материјални елемент подразумева да би одавање таквог податка или документа довело или могло да доведе до наступања штетних последица по безбедност или

економску и војну моћ земље. Став 6 додатно ограничава појам државне тајне увођењем негативног одређења – државном тајном се не сматрају „подаци или документи који су управљени на тешке повреде основних права човека, или на угрожавање уставног уређења и безбедности Србије, као и подаци или документи који за циљ имају прикривање учињеног кривичног дела за које се по закону може изрећи затвор од пет година или тежа казна“ (члан 316, став 6 КЗ).

Поменута збрка настала због „судара“ члана 321 став 3 и члана 316 став 3 КЗ-а постала је још већа након доношења ЗТП-а. Као што смо установили, члан 98 став 4 прописује казну од пет до петнаест година затвора уколико је одавање податка степенованог као државна тајна учињено под неком од наведених квалификаторних околности.

Једна од околности је управо извршење дела током ратног или ванредног стања. Можемо закључити да су за одавање државне тајне за време ратног стања истовремено на снази чак три различита распона казне, док су за исто дело учињено током ванредног стања прописана два различита распона. Сматрамо да је овакво стање законодавства неприхватљиво и да га треба отклонити што пре (иако траје већ 12 година).

Вреди поменути још један недостатак законског одређења кривичног дела из члана 316 КЗ-а. Ова инкриминација, као што и њен законски назив сведочи, првенствено је намењена санкционисању радњи одавања државне тајне. Последица оваквог приступа законодавца јесте да радње неовлашћеног прибављања тајне не спадају у опсег примене члана 316. Став 2 инкриминише ситуацију у којој лице противправно дође до државне тајне, али само под условом да је пренесе трећем непозваном лицу. Није јасно зашто законодавац пропушта да инкриминише и противправно прибављање степенованог документа од стране непозваног лица, без обзира да ли је тајна даље пренета.

Затим, поставља се питање да ли су у КЗ-у оправдано задржана кривична дела одавање службене тајне (чл. 369) и одавање војне тајне (чл. 415). Те категорије тајних података укинуте су доношењем ЗТП-а (видети члан 109), али сигурно није извршено (или у јавности није познато) преиспитивање ознака свих докумената и података који су проглашени за војну или службену тајну по прописима који су важили до ступања на снагу ЗТП-а, иако је члан 105 став 2 овог прописа експлицитно одредио да је то потребно учинити у року од две године од ступања закона на снагу.

Ипак, члан 105 став 1 ЗТП-а јасно одређује да документи и подаци означени по одредбама раније важећих прописа задржавају врсту и степен тајности које су имали (члан 105, став 1 ЗТП-а). Интенција законодавца да се преиспитају све раније утврђене ознаке тајности тешко је могла бити спроведена у пракси због претпостављеног обима и бројности означених података и докумената.

Имајући у виду одредбу члана 105 став 1 ЗТП-а, јасно је да одредбе КЗ-а којима се инкриминишу одавање војне и службене тајне морају остати на снази докле год су присутни документи и подаци који су означени као наведене врсте тајних података, те и оне представљају предмет нашег рада.

Одавање службене тајне спада у кривична дела која може учинити само одређена категорија учинилаца (Стојановић 2014; Вуковић, 2020). Реч је о службеним лицима, које законодавац одређује у члану 112 став КЗ-а. Став 6 члана 369 експлицитно предвиђа да учинилац овог дела може бити и службено лице ком је то својство престало, што је логично имајући у виду природу овог кривичног дела.

Кривично дело из члана 369 постоји када се службена тајна учини доступном непозваном лицу, путем саопштавања, предаје или на сличан начин. Основни облик постоји и када се подаци прикупљају у намери да се предају непозваном лицу. Ту се ради о припремној радњи уздигнутој на ранг радње извршења (Вуковић, 2020). Запрећена је казна од шест месеци до пет година затвора.

Тежи облик, за који је прописана казна од једне до осам година затвора, биће остварен ако је испуњена нека од следећих квалификаторних околности: дело је учињено из користољубља; подаци су били степеновани као нарочито поверљиви; подаци су били неовлашћено одани ради коришћења у иностранству. Куриозитет је да је запрећена казна за кривично дело одавања пословне тајне строжа у односу на казну за дело из члана 369 (Милошевић, 2021). Став 3 предвиђа казну до три године затвора за нехатно одавање службене тајне. Ставови 4 и 5 дефинишу службену тајну и објашњавају који се подаци не могу сматрати службеном тајном.

Одавање војне тајне је инкриминисано чланом 415 КЗ-а. Основни облик се практично не разликује од инкриминације службене тајне, јер су сви елементи осим врсте и степена тајности идентични. Исто се односи и на тежи облик у поређењу са чланом 369 став 2, као и на упоредо посматране привилеговане облике ова два кривична дела.

Кривична дела одавање војне и службене тајне, као ни инкриминација из члана 316 КЗ-а, не пружају адекватну кривичноправну заштиту од неовлашћеног прибављања тајне. Ту стоји примедба коју смо изнели у вези са чланом 316. Ипак, овде треба изнети и додатну критику. Код одавања државне тајне инкриминисано је и незаконито коришћење тајне (став 2). Код одавања војне и службене тајне, законодавац је испустио да регулише истоветне ситуације.

Осим наведеног, намеће се и питање специфичности одавања тајних података у дигиталном облику. Кривичноправна заштита од високотехнолошког криминала регулисана је одредбама КЗ-а, али су надлежности за спречавање, откривање, разјашњавање и суђење за дела сајбер криминалитета прописане посебним процесним прописом – Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала.[13] Дакле, учешће специјализованих служби за откривање дела сајбер криминала зависи од испуњености услова прописаних Законом о ВТК.

Међутим, већ језичка анализа члана 3 овог закона показује да кривично дело из члана 98 ЗТП-а не потпада под законско одређење појма високотехнолошког криминала. Законодавац допушта да специјализована одељења надлежних органа поступају у случајевима извршења тачно наведених група кривичних дела, уколико су кумулативно испуњени критеријуми из члана 2 Закона о ВТК. Али, инкриминација из члана 98 ЗТП-а не помиње се у члану 3 Закона о ВТК.

Закључак

Нормативни оквир заштите тајних података, укључујући и оне у дигиталном формату, може се начелно оценити као савремен и компатибилан са системима других држава. Ипак, анализа квалитативних података из експертског интервјуа указује и да је потребно: свеобухватније и усаглашеније нормативно уређење области; прецизније или другачије дефинисање надлежности релевантних појединих органа и тела, као и јачање јавно-приватне сарадње; уједначавање методологије за идентификовање КИИ; садржајније и ефикасније обуке запослених у погледу поступања са подацима; стимулисање стручног кадра и подизање нивоа безбедносне културе.

13 *Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала* (Службени гласник Републике Србије), бр. 61/05, 104/09 (Закон о ВТК).

Разматрање кривичноправног аспекта заштите тајних података указало је на низ неусаглашености и неуједначености, као и на недостатак системског приступа законодавца приликом доношења или новелирања међусобно блиских и повезаних закона. Законодавна интервенција је неопходна уколико желимо да успоставимо солидан и непротивречан кривичноправни оквир заштите тајних података.

Коначно, држимо да су потребне измене важећих прописа у предметној области, али и интензиван рад на развоју безбедносне културе, како би се код одговорних лица за примену закона развила свест о заштити тајних података као задатку од ког у значајној мери зависи очување виталних интереса Републике Србије.

Литература

1. *CSIRTs by Country - Interactive Map*. (2021). The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Serbia. доступан 14. 02. 2021.
2. *DECISION No. 1202 OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES*. (2016). Organization for Security and Co-operation in Europe, https://www.osce.org/files/f/documents/d/a/227281.pdf. доступан 10. 02. 2021.
3. Ђурић С. (2016), „*Интервјуисање експерата: специфичности и принципи примене*“, Годишњак Факултета безбедности 2016: 11-28.
4. Global Cybersecurity Index 2018. (2019). Geneva: International Telecommunication Union, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. доступан 10. 02. 2021.
5. *Кривични законик Републике Србије*, Службени гласник Републике Србије, бр. 85/05, 88/05 , 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19.
6. Мандић, Г., Путник, Н., Милошевић, М. (2017). *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти*. Београд: Универзитет у Београду-Факултет безбедности.

7. Маркагић, М. (2018), „Компромитујућа електромагнетна зрачења – изазови, претње и заштита“, *Војнотехнички гласник* 2018, вол. 66, бр. 1, стр. 143-153.
8. Матић, Г., (2014). *Практични аспекти примене закона о тајности података из 2009. године*. У Зборник радова „Примена закона о тајности података, 10 најзначајнијих препрека“, Мисија ОЕБС у Србији и Канцеларија Савета за националну безбедност и заштиту тајних података, Београд , стр. 11-24,
9. Милошевић М. (2010). *Кривична дела против уставног уређења и безбедности Републике Србије-историјски и позитивноправни приказ*, у: Цветковић, В. (уредник), Ризик, моћ и заштита-увођење у науке безбедности, Службени гласник и Универзитет у Београду-Факултет безбедности, Београд, стр. 414-452.
10. Milošević, M. (2021). *The Role of Criminal Law in Trade Secret Protection*. „Archibald Reiss Days“, 11th Thematic Conference Proceedings of International Significance, Belgrade, 9-10 November 2021. University of Criminal Investigation and Police Studies, pp. 53-63.
11. National Cyber Security Index. (2019). Tallinn: National Cyber Security Index, https://ncsi.ega.ee/ncsi-index. доступан 14. 02. 2021.
12. *Одлука о образовању Тела за координацију послова информационе безбедности*, Службени гласник Републике Србије, бр. 24/16, 53/17, 79/17, 112/17, 93/18.
13. Путник, Н. (2009). *Сајбер простор и безбедносни изазови*. Универзитет у Београду - Факултет безбедности.
14. Стојановић, З. (2018). *Коментар Кривичног законика*. Београд: Службени гласник.
15. *Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године*, Службени гласник Републике Србије, број 53/17.
16. *Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима,* Службени гласник Републике Србије, број 53/11.
17. *Уредба о посебним мерама физичко-техничке заштите тајних података*, Службени гласник Републике Србије, број 097/11.
18. *Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја*, Службени гласник Републике Србије, број 94/16.

19. Van Eck, W. (1985), *„Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?“*, Computers & Security Volume 4, Issue 4, December 1985, Pages 269-286.
20. Вуковић, И. (2021). *Кривично право – општи део*. Београд: Правни факултет Универзитета у Београду.
21. *Закон о информационој безбедности,* Службени гласник Републике Србије, бр. 6/16, 94/17 и 77/19.
22. *Закон о критичној инфраструктури,* Службени гласник Републике Србије, број 87/18.
23. *Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала*, Службени гласник Републике Србије, бр. 61/05, 104/09.
24. *Закон о тајности података,* Службени гласник Републике Србије, број 104/09.

Protection of Classified Information in Digital Form - Security and Criminal Aspects

***Abstract**: The protection of classified information is one of the priority tasks of the subjects of national security, because their preservation prevents the occurrence of damage to important public interests. A particular security challenge arises with the fact that numerous data are being moved to cyberspace, which, although it brings great practical advantages, gives rise to various risks to their security. The protection of classified information is the subject of a special law, which, with the accompanying bylaws, regulates it in detail. This paper is dedicated to the analysis of the actual situation in the field of protection of digital classified information in terms of the application of key legal solutions, as well as to considering the role and importance of criminal law, i.e. the quality of applicable criminal law norms. To determine the implementation problems, the authors briefly presented the normative framework and conducted an interview with an expert, seeking to shed light on the practical security aspect of the phenomenon of protection of classified information in digital form. By analyzing the provisions of the Criminal Code and the penal provisions of the Law on Data Secrecy, the authors note the systemic inconsistency of the relevant legal provisions and propose solutions de lege ferenda.*

***Keywords:** classified information, criminal law and security protection, digital data.*