Institut za uporedno pravo

Српска академија наука и уметности
Аудиовизуелни архив и дигитални центар
САНУ

Приредио / Edited by: **Драган Прља**

ПРАВНИ АСПЕКТИ ДИГИТАЛИЗАЦИЈЕ КУЛТУРНЕ БАШТИНЕ

THE LEGAL ASPECTS OF DIGITISATION OF CULTURAL HERITAGE

ПРАВНИ АСПЕКТИ ДИГИТАЛИЗАЦИЈЕ КУЛТУРНЕ БАШТИНЕ

THE LEGAL ASPECTS OF DIGITISATION OF CULTURAL HERITAGE

ПРАВНИ АСПЕКТИ
ДИГИТАЛИЗАЦИЈЕ
КУЛТУРНЕ БАШТИНЕ

THE LEGAL ASPECTS
OF DIGITISATION
OF CULTURAL HERITAGE

Изавачи
Институт за упоредно право, Београд
Српска академија наука и уметности
Аудиовизуелни архив и
дигитални центар САНУ

Published by
Institute of Comparative Law, Belgrade
Serbian Academy of Sciences and Arts
Audiovisual Archive and Center for
Digitization of SASA

За издаваче
Владимир Чоловић
Радослав Зеленовић

For the Publishers
Vladimir Čolović
Radoslav Zelenović

Рецензенти
Проф. др Стеван Лилић
Проф. Иоана Васиу
Проф. др Митар Лутовац

Reviewed by
Prof. dr Stevan Lilić
Prof. Ioana Vasiu Ph. D.
Prof. dr Mitar Lutovac

Лектура и коректура
Невенка Жалац

Proofreading
Nevenka Žalac

Тираж
500

Copies
500

ISBN 978-86-80186-24-5 (ИУП)
ISBN 978-86-7025-745-0 (САНУ)

ISBN 978-86-80186-24-5 (ICL)
ISBN 978-86-7025-745-0 (SASA)

Припрема и штампа
Досије студио, Београд

Prepress and Printing
Dosije studio, Belgrade

ПРАВНИ АСПЕКТИ ДИГИТАЛИЗАЦИЈЕ КУЛТУРНЕ БАШТИНЕ

THE LEGAL ASPECTS OF DIGITISATION OF CULTURAL HERITAGE

Приредио / Edited by
Драган Прља

Београд, 2017

Издавање ове књиге и одржавање научног скупа финансијски су помогли
Српска академија наука и уметности
Аудиовизуелни архив и дигитални центар САНУ
Министарство просвете, науке и технолошког развоја Републике Србије

САДРЖАЈ

ПРЕДГОВОР

Дигиталне технологије и интернет омогућили су потпуно нови ниво заштите културне баштине, као и нове облике доступности дигитализоване културне баштине у сврху забаве, образовања, истраживања и обављања разних послова у домену културе. Нове могућности, наравно, обилују и новим изазовима којима морамо да изађемо у сусрет. Ти изазови су техничке природе, организационе природе, научне природе, па и правне природе. Правно уређивање области дигитализације културне баштине у складу са савременим трендовима од изузетног је значаја за успех процеса дигитализације културне баштине. Нажалост правни аспекти дигитализације културне баштине већ су годинама запостављени, а процес дигитализације траје скоро двадесетак година. Недостатак правне литературе из области дигитализације културне баштине настојали смо да ублажимо објављивањем овог зборника радова са научне конференције одржане 19. октобра 2017. г. у Београду под називом „Правни аспекти дигитализације културне баштине".

У овој књизи представљено је четрнаест рецензираних оригиналних научних радова који обухватају питања нормативног регулисања надлежности за дигитализацију културне баштине у Србији, земљама у региону и земљама Европске уније, питања међународних правних стандарда за дигитализацију културне баштине, питања судских случајева везаних за дигитализацију културне баштине и њену доступност у сајбер простору, питања заштите безбедности дигитализованих података, питања ауторских права и интелектуалне својине везаних за дигитализацију културне баштине, питања управљања колективним правима, питања проблема одговорности у процесу аутентификације уметничких дела, питања значаја израде база података о украденим културним добрима, као и нека друга правна питања везана за дигитализацију културне баштине. У књизи су представљени и неки примери из праксе, као што је то пример дигиталног репозиторија Универзитета у Београду – Phaidra.

Почетни корак у обједињавању знања из области правних аспеката дигитализације културне баштине је направљен, а надамо се да ће се истраживање у овој области наставити, да ће се резултати тих истраживања објављивати, и да ће у будућности дигитализацију културне баштине пратити адекаватно уређена многобројна правна питања.

Београд, 2017. Приређивач

Проф. др *Драган Јовашевић*[*]

ЗАШТИТА БЕЗБЕДНОСТИ ДИГИТАЛНИХ БАЗА ПОДАТАКА О КУЛТУРНОЈ БАШТИНИ СРБИЈЕ

Апстракт

На бази усвојених међународних докумената универзалног и регионалног карактера највећи број држава, па тако и Република Србија, у свом националном законодавству познају више рачунарских (компјутерских) кривичних дела којима се штите различите дигиталне базе података, па тако и дигиталне базе података о културном наслеђу. За учиниоце ових специфичних кривичних дела прописана је кривична одговорност и кажњивост физичких и правних лица. Поред специфичних рачунарских кривичних дела, у савременим условима и бројна стара класична кривична дела (крађа, превара, фалсификовање) добијају нову димензију са већим степеном тежине и опасности када се врше употребом рачунара или рачунарских система. Будући да се ради о криминалитету где најчешће нема временске и просторне повезаности учиниоца и његове радње извршења и проузроковане последице, односно оштећеног лица, то савремена законодавства познају и посебне доказне радње у поступку откривања и доказивања ових кривичних дела. Управо о појму и карактеристикама рачунарског криминалитета који се врши на штету дигиталних база података о културној баштини Републике Србије говори овај рад.

Кључне речи: дигитална база, културна баштина, закон, кривично дело, кривична санкција, Србија

1. УВОД

Усвајањем Закона о изменама и допунама Кривичног закона Републике Србије[1] априла 2003. године на бази међународних стандарда универзалног или регионалног карактера у систем кривичног права Републике Србије је по први пут уведено више рачунарских (компјутерских) кривичних дела, те одређена правила о кривичној одговорности и кажњавању учинилаца ових дела[2]. Наиме, у новоуведеној глави 16А. Кривичног закона предвиђена су кривична дела против безбедности рачунарских података. Тиме се и наша држава прикључила низу држава које се на различите начине (у првом реду системом превентивних и репресивних мера) покуша-

* Редовни професор, Правни факултет Универзитета у Нишу, e-mail: jovas@prafak.ni.ac.rs.

1 *Сл. гласник Републике Србије*, бр. 39/2003.

2 Д. Јовашевић, Коментар Кривичног закона Републике Србије са судском праксом, Београд, 2003, 351–361.

вају ефикасно, законито и квалитетно супротставити различитим облицима и видовима злоупотребе рачунара у циљу остварења противправне имовинске користи за себе или друго физичко или правно лице, односно у циљу наношења (имовинске) штете другом лицу или ради повреде права другог лица.

Конституисањем Републике Србије као самосталне и међународно признате државе септембра 2005. године донет је Кривични законик Републике Србије[3] (КЗ). У глави двадесет седмој под називом: „Кривична дела против безбедности рачунарских података" Кривични законик прописује рачунарска кривична дела. Овај законик је почео да се примењује од 1. јануара 2006. године.

2. ЕВРОПСКИ СТАНДАРДИ ЗАШТИТЕ РАЧУНАРСКИХ СИСТЕМА И КУЛТУРНОГ НАСЛЕЂА

Савет Европе је доношењем Конвенције о кибернетичком (сајбер) криминалу (Convention on Cybercrime, ETS 185) од 23. новембра 2001. године[4] покушао да постави основе јединственог европског система материјалног и процесног кривичног права у области неопходне сарадње држава чланица у сузбијању различитих облика и видова рачунарског (кибернетичког) криминала. При томе је сама Конвенција (чл. 2–13) прописала пет кривичних дела ове врсте која су управљена против тајности, целовитости и доступности рачунарских података и система. Овим су постављене основе за поједина национална законодавства да прецизније одреде обележја и карактеристике појединих рачунарских кривичних дела, њихове основне, лакше или теже облике, те да пропишу кривичне санкције за њихове учиниоце (физичка или правна лица).

Уз ову конвенцију је усвојен и Допунски протокол о криминализирању аката расистичке и ксенофобичне природе која су учињена посредством рачунарских система. И овај протокол у чл. 3–7. прописује такође кривичну одговорност и кажњивост за злоупотребу рачунара у вршењу кривичних дела из расистичких и ксенофобичних побуда (мотива)[5].

Имајући у виду утврђене обавезе за државе чланице Савета Европе, било је логично очекивати да ће и у домаћем кривичном законодавству уследити, прво, на законодавном плану, па потом и у пракси ефикасна, квалитетна и законита борба са рачунарским криминалитетом и њиховим извршиоцима. Прихватајући наведену конвенцију, изменама и допунама Кривичног закона Републике Србије из априла 2003. године у наш правни систем уведено је више рачунарских кривичних дела у глави 16а. под називом: „Кривична дела против безбедности рачунарских података"[6].

---

3 *Сл. гласник Републике Србије*, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016.

4 B. Pavišić, Kazneno pravo Vijeća Evrope, Zagreb, 2006, 261–265.

5 Д. Јовашевић, Међународно кривично право, Ниш, 2011, 116–124.

6 Д. Јовашевић, Коментар Кривичног закона Републике Србије са судском праксом, Београд, 2003, 351–361.

У основи Конвенције о кибернетичком криминалу као обавезујућем међународном документу[7] који је донет од стране најзначајније и најмасовније европске регионалне организације налази се више претходно донетих препорука као што су[8]: 1) Препорука број Р (85) 10 о практичној примени Европске конвенције о узајамној помоћи у кривичним предметима у погледу пружања међународне кривичноправне помоћи при пресретању комуникација, 2) Препорука број Р (88) 2 о пиратству на пољу ауторских и сродних права, 3) Препрорука број Р (87) 15 која прописује употребу личних података у области делатности полиције, 4) Препорука број Р (95) 4 о заштити личних података на подручју телекомуникационих услуга са посебним освртом на улогу телефоније, 5) Препорука број Р (89) 9 о рачунарском криминалу која даје смернице националним органима у погледу дефинисања појединих рачунарских кривичних дела и 6) Препорука број Р (95) 13 о проблемима кривично процесног права који су везани за информатичку технологију.

Конвенција о кибернетичком криминалу[9] предвиђа низ правних средстава, мера и поступака који су нужни ради одвраћања лица од радњи које су усмерене против тајности, целовитости и доступности рачунарских система, мрежа и рачунарских података, као и за одвраћање од њихове злоупотребе у било ком виду. На тај начин се олакашава откривање, истраживање и кривични прогон тих дела и њихових учинилаца на домаћем и међународном нивоу и осигурава ефикасна и брза међународна сарадња. У члану 1. Конвенција[10] је дефинисала основне појмове рачунарског (кибернетичког, сајбер) криминалитета као што су: рачунарски систем, рачунарски податак, давалац услуга или подаци о промету. Овим је дато упутство националном законодавцу да у овом духу третира ове заштићене вредности као објекте кривичноправне заштите.

У другом поглављу под називом: „Казнено материјално право" у више одредби су дати појам и карактеристике појединих кривичних дела које треба инкриминисати у националним правним системима држава чланица Савета Европе. То су следећа кривична дела: 1) кривична дела против тајности, целовитости и доступности рачунарских података и система (чл. 2–6): незаконити приступ, незаконито пресретање, ометање података, ометање система и злоупотреба уређаја, 2) рачунарска кривична дела (чл. 7–8): рачунарско фалсификовање и рачунарска превара, 3) кривична дела у вези са садржајем (члан 9) – кривична дела везана за дечју порнографију и 4) кривична дела повреде ауторских и сродних права (члан 10). Оно што је од посебног значаја јесу одредбе Конвенције које изричито захтевају од држава чланица да се казни и за покушај ових кривичних дела, као и за облике саучесништва[11] у виду подстрекавања и помагања, као и да се поред одго-

7 D. Jovašević, V. Ikanović, Međunarodno krivično pravo, Banja Luka, 2015, 116–118.

8 B. Petrović, D. Jovašević, Međunarodno krivično pravo, Sarajevo, 2010, 87–92.

9 D. Jovašević, V. Ikanović, Međunarodno krivično pravo, Banja Luka, 2015, 78–82.

10 S. Emm Kareklas, Priručnik za krivično pravo Evropske unije, Beograd, 2009, 94–97.

11 Д. Јовашевић, Кривично право, Општи део, Београд, 2016, 178–185.

ворности физичких лица, за ова дела предвиди и кривична одговорност правних лица[12].

Све наведене стандарде ново кривично законодавство Србије је у потпуности имплементирало у свој правни систем обезбеђујући врсту и меру казне за поједина кривична дела, као и формирајући посебне органе у оквиру полиције, јавног тужилаштва и Вишег суда у Београду посебне организационе јединице за борбу против високотехнолошког криминала где спадају наведена кривична дела.

На сличан начин у оквиру држава чланица Савета Европе успостављају се јединствени правни основи за свеобухватну и ефикасну заштиту и очување културног наслеђа[13]. У том циљу донета је и Оквирна конвенција Савета Европе о вредности културног наслеђа за друштво која је усвојена у Фару 27. октобра 2005. године[14]. На тај начин је створена јединствена основа да се употпуни постојећи систем регистрације, очувања, унапређења и заштите културног наслеђа успостављен са више различитих међународних докумената ове европске регионалне организације као што су: 1) Европска културна конвенција из 1954. године, 2) Конвенција о заштити архитектонског наслеђа Европе из 1985. године, 3) Европска конвенција о заштити археолошког наслеђа из 1992. године и 4) Европска конвенција о пределу из 2000. године[15].

У том контексту је посебно истакнута потреба да се сваки појединац укључи у стални процес дефинисања и управљања културним наслеђем у коме долази до пуног изражаја остварење принципа политике културног наслеђа и иницијатива у образовању које сматрају да је сво културно наслеђе једнако, унапређујући тако дијалог међу културама и религијама. Тиме се стварају основе за успостављање „паневропског" оквира за сарадњу у динамичном процесу стварне примене принципа обезбеђења и заштите културног наслеђа као тековине развоја људске цивилизације, а у чијој се основи налази Европска културна конвенција из 1954. године.

Оквирна конвенција Савета Европе о вредности културног наслеђа за друштво је донета како би се остварили постављени циљеви[16] који су одређени као постигнути ниво сагласности држава чланица ове регионалне европске организације о следећим питањима као што су: 1) признавање да је право на културно наслеђе неодвојиво од права на учешће у културном животу, као што је утврђено у Универзалној декларацији ОУН о људским правима (из 1948. године), 2) признавање појединачне и колективне одговорности према културном наслеђу као заједничкој баштини целокупног људског рода, 3) наглашавање да је крајњи циљ очување културног

12 M. Simović, D. Jovašević, V.Simović, Privredno kazneno pravo, Banja Luka, 2016, 89–97.

13 J. Holthoff, Kulturraum Europa, Baden-Baden, 2006, 67–79.

14 *Сл. їласник Рейублике Србије – Међународни уїовори*, бр. 1/2010.

15 Б. Стојковић, Културна политика европске интеграције, Београд, 1995, 45–49.

16 M. de Angelo, P. Vesperini, Cultural Policies in Europe: A Comparative Approach, Council of Europe, 1998, 65–68.

наслеђа и његова одржива намена за људски развој и квалитет живота и 4) предузимање неопходних корака за примену одредаба ове конвенције у погледу: а) улоге културног наслеђа у изградњи мирољубивог и демократског друштва, као и процеса одрживог развоја и унапређења културне разноликости и б) веће синергије надлежности између свих заинтересованих јавних, институционалних и приватних актера.

Заједничко културно наслеђе Европе које спаја њену прошлост, садашњост и будућност састоји се из две врсте елемената. То су: 1) сви облици културног наслеђа у Европи који чине заједнички извор сећања, разумевања, идентитета, кохезије, стваралаштва и 2) идеали, принципи и вредности који су проистекли из искустава стечених кроз напредак и сукобе из прошлости, који негују развој мирољубивог и стабилног друштва, заснованог на поштовању људских права, демократије и владавини права. Овако дефинисано културно наслеђе, заправо, означава скуп ресурса наслеђених из прошлости, које људи идентификују, независно од власништва над њима, као одраз и израз непрекидно еволуирајућих вредности, уверења, знања и традиција. Оно обухвата све видове животне средине настале интеракцијом човека и простора током времена. У односу на тако одређено културно наслеђе које има посебан значај за друштво у целини, државе у оквиру Савета Европе су преузеле одређена права и обавезе.

Тај корпус њихових права и обавеза може се свести на обавезу државе потписнице ове европске конвенције да признају да: 1) сви људи, појединачно или колективно, имају право да уживају добробит културног наслеђа и доприносе његовом богаћењу, 2) сви, појединачно или колективно, имају обавезу да поштују културно наслеђе других на исти начин као и сопствено наслеђе, а самим тим и заједничко наслеђе Европе и 3) остваривање права на културно наслеђе може да подлеже само оним ограничењима која су нужна у демократском друштву ради заштите јавног интереса, права и слобода других[17]. У том смислу европске државе су се обавезале да у свом националном политичком, правном и друштвеном систему предузму следеће мере и радње као што су: 1) да признају јавни интерес везан за елементе културног наслеђа у складу са њиховим значајем за друштво, 2) да унапређују вредност културног наслеђа његовом идентификацијом, проучавањем, тумачењем, заштитом, очувањем и представљањем и 3) да обезбеде у специфичном контексту сваке поједине државе постојање законских одредаба које се односе на процедуре остваривања права на културно наслеђе[18].

На исти начин су државе, међу којима и Република Србија после ратификације ове европске конвенције, преузеле и следеће обавезе: 1) да негују привредну и друштвену климу која подстиче учешће у активностима везаним за културно наслеђе, 2) да унапређују заштиту културног наслеђа као централног фактора у међусобно повезаним циљевима одрживог развоја, културне разноликости и савременог стваралаштва који се међусобно надопуњују, 3) да препознају вредност културног наслеђа које се налази на

17 A. Semperini, Мултикултурализам, Београд, 1999, 17–19.

18 Council of Europe, Handbook of cultural affairs in Europe, Baden Baden, 2000, 45–53.

територији под њиховом надлежношћу, без обзира на његово порекло и 4) да формулишу интегрисане стратегије ради олакшања примене одредаба ове конвенције.

3. КРИВИЧНОПРАВНА ЗАШТИТА РАЧУНАРСКИХ ПОДАТАКА

Због постојања различитих облика и видова испољавања злоупотребе рачунара у свакодневним животним ситуацијама Кривични законик Републике Србије прописује више рачунарских кривичних дела или како их он назива „кривичних дела против безбедности рачунарских података“[19]. Но, сва та поједина дела поред бројних различитости, имају и низ специфичних карактеристика које су им заједничке[20]. Рачунар, у сваком случају, представља једну од најзначајнијих и најреволуционарнијих тековина развоја техничко-технолошке цивилизације. Но, поред бројних предности које собом носи и огромне користи за човечанство, рачунар је брзо постао и средство за разне злоупотребе несавесних појединаца, група, па и читавих организација. Тако настаје рачунарски криминалитет као посебан и специфичан облик савременог криминалитета по структури, особеностима, облицима испољавања, карактеристикама учиниоца, начину и средствима извршења итд.

Овај вид криминалитета, за разлику од других, још увек не представља заокружену феноменолошку категорију, те га је немогуће дефинисати јединственим и прецизним појмовним одређењем. Рачунарски криминалитет је само општа форма кроз коју се испољавају различити облици криминалне делатности уз помоћ или посредством рачунара. Наиме, то је криминалитет који је управљен против безбедности рачунарских (информатичких, компјутерских) система у целини или његових појединих делова на различите начине и различитим средствима у намери да се себи или другом физичком или правном лицу прибави противправна имовинска корист или другоме нанесе каква, најчешће, имовинска штета.

3.1. Објекат рачунарских кривичних дела

Објект заштите код рачунарских кривичних дела јесте безбедност рачунарских (компјутерских) података и система, односно рачунарске мреже[21]. Иако је данас уобичајено да се ова кривична дела обухватају појмом „компјутерски“ криминалитет[22], наш је законодавац за њих ипак употребио термин „рачунарски“ криминалитет. Но, поред овог назива за кривична дела

19 Д. Јовашевић, Кривично право, Посебни део, Београд, 2017, 214–221.

20 С. Петровић, Компјутерски криминалитет, Безбедност, Београд, бр. 1, 1994, 32–40.

21 Д. Јовашевић, Обележја компјутерског криминалитета, Правни информатор, Београд, бр. 3, 1998, 56–62.

22 Овај појам користи Кривични законик Републике Македоније после доношења Закона о изменама и допунама Кривичног законика (*Сл. весник на Рейублика Македонија*, бр. 37/96, 80/99, 4/2002, 43/2003 и 19/2004).

систематизована на овом месту, наше законодавство употребљава и појам „високотехнолошки“ криминал[23]. Под овим се појмом подразумева вршење кривичних дела код којих се као објекат или као средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, рачунарски системи, као и њихови производи у материјалном или електронском облику.

При томе је сам законодавац у члану 112. Кривичног законика одредио појам и карактеристике објекта напада код ових кривичних дела. То су[24]: 1) рачунарски податак, 2) рачунарска мрежа, 3) рачунарски програм, 4) рачунарски вирус, 5) рачунар и 6) рачунарски систем. Тако је рачунарски податак свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију (члан 112. став 17. КЗ). Рачунарска мрежа представља скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке (члан 112. став 18. КЗ). Као рачунарски програм сматра се уређени скуп наредби који служи за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара (члан 112. став 19. КЗ). Рачунарски вирус је рачунарски програм или други скуп наредби који је унет у рачунар или рачунарску мрежу, који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података (члан 112. став 20. КЗ). Рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке (члан 112. став 33. КЗ). И коначно, рачунарски систем је сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма врши аутоматску обраду података (члан 112. став 34. КЗ).

3.2. Појам рачунарских кривичних дела

Компјутер (рачунар) представља једну од најзначајнијих и најреволуционарнијих тековина техничко-технолошког развоја на крају 20. века. Но, поред предности које рачунар носи са собом и огромне користи за човечанство, он је убрзо постао и средство злоупотребе несавесних појединаца или група. Тако настаје рачунарски криминалитет као посебан и специфичан облик савременог криминалитета. Захваљујући огромној моћи рачунара у меморисању и брзој обради великог броја података, аутоматизовани информациони системи постају све бројнији и незамењиви пратилац целокупног људског и друштвеног живота физичких и правних лица[25].

---

23 Појам, карактеристике, органи кривичног гоњења и поступак за кривична дела високотехнолошког криминала уређени су одредбама Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала (*Сл. гласник Републике Србије*, бр. 61/2005).

24 Д. Јовашевић, Кривично право, Посебни део, Београд, 2017, 189–192.

25 З. Ђокић, С. Живановић, Компјутерски криминал као обележје прогресивног криминалитета, Зборник радова, Казнено законодавство – прогресивна или регресивна решења, Београд, 2005, 305–318.

Различите форме примене рачунара у свим областима живота, привреде и других друштвених делатности нису остале незапажене од стране несавесних и злонамерних појединаца или група који не бирајући средства и начине покушавају да прибаве за себе или другог противправну имовинску корист или да другоме нанесу какву, најчешће, штету. Тако рачунар постаје средство, оруђе за извршење различитих кривичних дела. За различите облике и видове злоупотребе рачунара у теорији се употребљавају и различити називи као што су: злоупотреба рачунара (цомпутер абусе), деликти уз помоћ рачунара (цриме бу цомпутер), компјутерска превара (цомпутер фрауд), информатички криминалитет, рачунарски криминалитет, сајбер криминалитет, техно криминалитет итд[26].

У правној теорији[27] могу се уочити различита одређења појма рачунарског криминалитета. Тако Дон Паркер одређује рачунарски (компјутерски) криминалитет као злоупотребу компјутера у смислу сваког догађаја који је у вези са употребом компјутерске технологије у коме жртва трпи или би могла да трпи губитак, а учинилац делује у намери да себи прибави или би могао да прибави корист[28]. Август Бекуи дефинише компјутерски (рачунарски) криминалитет као вршење кривичних дела код којих се рачунар појављује као оруђе или објект заштите, односно као употребу компјутера при вршењу преваре, утаје или злоупотребе чији је циљ присвајање новца, услуге или вршење политичке или пословне манипулације, укључујући и радње уперене против самог рачунара[29]. Бого Брвар под рачунарским криминалитетом сматра вршење кривичних дела код којих се компјутер појављује као средство (оруђе), предмет или објект напада за чије је вршење или покушај неопходно извесно знање из рачунарства или информатике[30].

Тако се може закључити да се под појмом рачунарског криминалитета[31] подразумева свеукупност различитих облика, видова и форми испољавања противправних понашања управљених против безбедности рачунарских, информационих и компјутерских система у целини или њихових појединих делова на различите начине и различитим средствима у намери да се себи или другом прибави корист (имовинске или неимовинске природе) или да се другоме нанесе штета[32].

---

26 Д. Јовашевић, Лексикон кривичног права, Београд, 2011, 639.

27 D. Jovašević, V. Ikanović, Krivično pravo Republike Srpske, Posebni deo, Banja Luka, 2012. godine, str. 178–187.

28 D. Parker, Computer abuse, Springfild, 1973, 70.

29 A. Bequai, Computer crime, Lexington, 1978, 4.

30 B. Brvar, Pojavne oblike zlorabe računlnika, Revija za kriminalistiko in kriminologijo, Ljubljana, br. 2, 1982, 29.

31 Д. Јовашевић, Кривичноправна заштита безбедности рачунарских података, Правни информатор, Београд, бр. 6, 2003, 53–58.

32 Н. Китаровић, Компјутерски криминалитет, Билтен судске праске Врховног суда Србије, Београд, бр. 2–3, 1998, 52–56.

Из овако одређеног појма рачунарског криминалитета произилазе његове основне карактеристике[33]: 1) објект заштите је безбедност рачунарских података или информационог система у целини или његовог појединог дела (сегмента), 2) посебан, специфичан карактер и природа противправних делатности појединаца, 3) посебна знања и специјализација на страни учиниоца ових кривичних дела која искључује могућност да се свако, било које лице нађе у овој улози, 4) посебан начин и средство предузимања радње извршења – уз помоћ или употребом (злоупотребом) рачунара и 5) намера учиниоца као субјективни елеменат у време предузимања радње која се огледа у намери прибављања за себе или другог користи или наношења штете другом физичком или правном лицу.

Рачунарски криминалитет карактерише велика динамика и изузетна шароликост појавних облика, форми и видова испољавања. То је и разумљиво јер се ради о новој технологији са великим могућностима примене у широкој сфери људске, друштвене и привредне делатности, те су и могућности злоупотребе рачунара сваки дан све веће. Поред нових појавних облика раније, већ познатих кривичних дела која под утицајем злоупотребе компјутера мењају традиционални, класични начин и модус испољавања (крађа, превара, фалсификовање), јављају се и нови облици противправног и кажњивог понашања који не познају границе између држава (прављење рачунарског вируса).

Штетне последице рачунарских кривичних дела су велике и испољавају се у наступању имовинске штете за физичка или правна лица (понекад и за целу државу), у губитку пословног угледа, губитку поверења у сигурност и истинитост рачунарског пословања и уопште рачунарских података, опасности од злоупотребе по слободе и права човека и грађана на разне начине, одавање личне, пословне и других видова тајни и сл.

3.3. Остали елементи рачунарских кривичних дела

У теорији кривичног права у област рачунарског криминалитета сврставају се различити облици противправног, недозвољеног понашања као што су: 1) рачунарска превара, 2) финансијске крађе, преваре, утаје и злоупотребе, 3) крађа добара, 4) фалсификовање података и докумената, 5) вандализам, 6) саботажа, 7) хакерисање, 8) рачунарска шпијунажа и 9) крађа времена.

Велике практичне могућности које пружа савремена високо софистицирана рачунарска и информатичка технологија са собом носе и опасност од ширења и масовне употребе електронског прислушкивања, крађе пословних и других тајни, као и различитих облика интелектуалне својине, затим озбиљног нарушавања приватности и угрожавања људских слобода и права, као и личног интегритета, а у последње време је присутна и ре-

33 B. Petrović, D. Jovašević, A. Ferhatović, Krivično pravo 2, Sarajevo, 2016, 211–214.

ална опасност од таласа различитих облика терористичког деловања (тзв. „техно“ или „сајбер“ тероризам).

Извршиоци рачунарских кривичних дела[34] представљају специфичну категорију лица. Ради се, углавном, о неделиквентним и социјално прилагодљивим, ненасилним личностима. Они за вршење кривичних дела путем рачунара морају да поседују одређена специјална, стручна и практична знања и вештине у домену информатичке и рачунарске технике и технологије. Поред тога, ради се о лицима којима су оваква техничка средства (рачунари) доступна у физичком смислу.

Ова се кривична дела врше прикривено, често без видљиве просторне и временски блиске повезаности између учиниоца дела и оштећеног (пасивног субјекта). У пракси постоји већа или мања временска разлика између предузете радње извршења кривичног дела и тренутка наступања његове последице. Ова се дела тешко откривају, а још теже доказују, дуго времена остају практично неоткривена, све док оштећени не претрпи штету у домену информатичких и рачунарских података или система. Ради се о криминалитету који брзо и лако мења форме и облике испољавања, границе међу државама, као и врсту оштећеног. У погледу кривице, ова се дела врше искључиво са умишљајем.

4. ПОЈЕДИНА РАЧУНАРСКА КРИВИЧНА ДЕЛА

Кривични законик Републике Србије у глави двадесет седмој под називом: „Кривична дела против безбедности рачунарских података“ предвиђа следећа рачунарска кривична дела: 1) оштећење рачунарских података и програма, 2) рачунарска саботажа, 3) прављење и уношење рачунарских вируса, 4) рачунарска превара, 5) неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, 6) спречавање и ограничавање приступа јавној рачунарској мрежи, 7) неовлашћено коришћење рачунара или рачунарске мреже и 8) прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података.

4.1. Оштећење рачунарских података и програма

Дело из члана 298. КЗ се састоји у неовлашћеном брисању, измени, оштећењу, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма[35]. Објект заштите је безбедност рачунарских података или рачунарских програма, а објект напада је рачунарски податак или програм. Рачунарски податак је свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду

34 B. Petrović, D. Jovašević, A. Ferhatović, Krivično pravo 2, Sarajevo, 2016, 211–214.

35 Д. Јовашевић, Коментар Кривичног закона Републике Србије са судском праксом, Београд, 2003, 353–354.

у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију. Рачунарски програм је уређени скуп наредби који служи за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара.

Радња извршења је алтернативно одређена и састоји се у предузимању следећих делатности: 1) брисању, 2) измени, 3) оштећењу, 4) прикривању и 5) чињењу неупотребљивим рачунарског податка или програма. За постојање овог дела је битно да се радња предузима неовлашћено, дакле од стране неовлашћеног лица, на начин и у поступку који нису дозвољени и на закону засновани. Брисање је уклањање рачунарских података у целини или делимично или рачунарског програма. Измена је делимична промена постојећих података или уношење нових података на начин, од стране лица и у поступку који није предвиђен одговарајућим прописима или по одговарајућој процедури. Оштећење је привремено, делимично или краткотрајно онеспособљење коришћења рачунарског податка или програма изазивањем кварова или кидањем појединих делова, веза или склопова, тако да се рачунарски податак или програм не могу користити за одређено време за сврху за коју су намењени. Прикривање је премештање податка или програма са места на коме је био похрањен или садржан и склањање на друго, најчешће непознато место. Чињење неупотребљивим на други начин је свако друго онеспособљење за краће или дуже време или онемогућавање у већој или мањој мери коришћења рачунарског податка или програма. Последица дела је повреда заштићеног добра – рачунарског податка или програма који припада физичком или правном лицу у смислу његове употребљивости, корисности уопште или за одређено време, на одређеном месту или за одређену намену. Извршилац дела може да буде свако лице, а у погледу кривице потребан је умишљај.

За ово дело је прописана новчана казна или казна затвора до једне године. Суд учиниоцу дела обавезно изриче меру безбедности одузимања уређаја и средстава ако су испуњена два услова: 1) да се ради о средствима и уређајима којима је кривично дело учињено и 2) да су средства и уређаји у својини учиниоца дела.

Ово дело има два тежа облика. Први тежи облик дела постоји ако је предузетом радњом извршења основног дела проузрокована штета у износу преко 450.000 динара. Висина причињене имовинске штете у време извршења дела у законом утврђеном износу представља квалификаторну околност. За ово дело је прописана казна затвора од три месеца до три године. Други тежи облик дела за који је прописана казна затвора од три месеца до пет година постоји ако је предузетом радњом основног дела проузрокована имовинска штета у износу преко 1.500.000 динара.

4.2. Рачунарска саботажа

Рачунарско дело из члана 299. КЗ чини лице које унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар

или други уређај за електронску обраду и пренос података у намери да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државни орган, јавну службу, установу, предузеће или друге субјекте[36]. Објект заштите је двојако одређен као: 1) рачунарски податак или програм и 2) рачунар и други уређај за електронску обраду и пренос података. Битно је да ови уређаји и средства припадају, односно да су од значаја за државни орган, јавну службу, установу, предузеће или другог субјекта.

Радња извршења је алтернативно одређена као: 1) унос, 2) уништење, 3) брисање, 4) измена, 5) оштећење, 6) прикривање и 7) чињење неупотребљивим на други начин рачунарског податка или програма, односно уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података. Унос је уписивање или похрањивање новог до тада непостојећег податка или измена већ постојећег рачунарског или другог податка у рачунарском програму. Уништење је потпуно и трајно разарање супстанце или облика одређеног предмета тако да више уопште не може да се користи за сврху, намену за коју је раније коришћен. Брисање је уклањање најчешће механичким или другим путем у целини или делимично рачунарског податка или програма. Измена је делимично мењање постојећих података у смислу њихове садржине, места где се налазе или њихове природе или уношење других неистинитих података у рачунарски систем. Оштећење је привремено, делимично или краткотрајно онеспособљење рачунарског податка, програма, рачунара или другог уређаја за сврху за коју су иначе намењени. Прикривање је склањање податка или предмета са места на коме се до тада налазио и које је свима било познато и премештање на друго најчешће скривено место тако да се са њиховом садржином не могу упознати друга лица уопште или за одређено време. Чињење неупотребљивим рачунарског податка или програма представља сваку делатност којом се у већој или мањој мери утиче на употребљивост рачунарских података или програма.

Зависно од објекта напада према коме је управљена радња извршења овог кривичног дела, разликују се два његова облика. То су: 1) уништење или оштећење рачунарског податка или програма и 2) уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података. Оно што је битно за постојање оба облика дела јесте: а) да се радња извршења предузима у односу на објекте који припадају државном органу, јавној служби, установи, предузећу или другом субјекту (правном лицу са посебним овлашћењима). Дакле, својство оштећеног представља елеменат бића овог кривичног дела и б) да на страни учиниоца у време предузимања радње постоји одређена намера – намера да се онемогући (у потпуности и трајно) или знатно омете (отежа) поступак електронске обраде и преноса података. Није од значаја да ли је ова намера у конкретном случају и остварена. Последица дела је повреда рачунарског податка, програма, рачунара

36 Д. Јовашевић, Кривично право, Посебни део, Београд, 2017, 216–218.

или уређаја за аутоматски пренос или обраду података у смислу њихове употребљивости и корисности.

Извршилац дела може да буде свако лице, а у погледу кривице потребан је директни умишљај који карактерише наведена намера. За ово дело је прописана казна затвора од шест месеци до пет година.

4.3. Прављење и уношење рачунарских вируса

Дело из члана 300. КЗ састоји се у прављењу рачунарског вируса у намери његовог уношења или његовом уношењу у туђи рачунар или рачунарску мрежу[37]. Објект заштите је безбедност рачунара и рачунарске мреже од вируса различите врсте и природе, а објект напада је рачунарски вирус. То је рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података.

Радња извршења састоји се у: 1) прављењу – стварању рачунарског вируса који је подобан, довољан, који је у могућности да проузрокује одређене промене, оштећења у коришћењу или употребљивости рачунара или рачунарске мреже у целини или делимично. За постојање ове радње извршења потребно је да учинилац поступа са намером (као субјективним елементом) да тако створени рачунарски вирус унесе у туђи рачунар или рачунарску мрежу. Намера мора да постоји на страни учиниоца у време предузимања радње без обзира да ли је у конкретном случају она и остварена и 2) уношењу рачунарског вируса, непосредно или посредно, у туђи рачунар или рачунарску мрежу, без обзира ко је овај вирус направио.

Извршилац дела може да буде свако лице, а у пракси су то лица која поседују посебна, специјална знања из области рачунарства и информатике. У погледу кривице потребан је директни умишљај који карактерише наведена намера.

За ово дело је прописана новчана казна или казна затвора до шест месеци. Уређаји и средства којима је учињено дело обавезно се одузимају применом мере безбедности одузимања предмета.

Тежи облик дела за који је прописана новчана казна или казна затвора до две године постоји ако је овако створени вирус унет у туђи рачунар или рачунарску мрежу чиме је проузрокована штета. За постојање дела је битно да је учинилац свестан, да зна у време предузимања радње – рада на рачунару, да на такав начин управо уноси рачунарски вирус у туђи рачунар или рачунарску мрежу. Штета која је на овај начин проузрокована, може бити имовинског или неимовинског карактера. Битно је да овако проузорокована штета представља резултат предузете радње основног дела и да у односу на њу учинилац поступа са нехатом.

---

37 Д. Јовашевић, Коментар Кривичног закона Републике Србије са судском праксом, Београд, 2003, 355–356.

4.4. Рачунарска ūревара

„Рачунарска превара“ из члана 301. КЗ састоји се у уношењу нетачног податка, пропуштању уношења тачног податка или на други начин прикривању или лажном приказивању податка чиме се утиче на резултат електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује имовинска штета другом лицу[38]. Објект заштите је безбедност рачунарских система од уношења нетачних, неистинитих података и поверење у ове системе.

Радња извршења састоји се из две алтернативно предвиђене делатности. То су: 1) прикривање и 2) лажно приказивање рачунарског податка. Прикривање је неуношење неког податка од стране лица које је обавезно да исти унесе у рачунар или рачунарску межу. Може се радити о било каквом податку. Лажно приказивање рачунарског податка постоји када се у рачунарској мрежи приказује, објављује, уноси или користи неистинити податак (било да је у потпуности или делимично неистинит). Обе делатности морају бити предузете у односу на податак који је по свом значају, природи, карактеру, времену уношења или употребе такав да је подобан да утиче на резултат (ток и поступак) електронске обраде и преноса података у рачунарском систему.

Било која од ових делатности у смислу кривичног дела мора бити предузета на Законом одређени начин: 1) уношењем нетачног (неистинитог) податка у целини или делимично, 2) пропуштањем да се унесе, неуношењем, неуписивањем каквог важног податка (значи не било каквог податка, већ само оног који је у конкретном случају важан) или 3) на други начин. Све делатности у смислу радње извршења овог кривичног дела морају бити предузете у одређеној намери – намери да учинилац за себе или другог прибави противправну имовинску корист. Та намера мора да постоји на страни учиниоца у време предузимања радње, али она у конкретном случају не мора бити и остварена. Последица дела је повреда која се огледа у проузроковању имовинске штете за другог. Може се радити о штети у било ком износу која је у узрочно-последичној вези са предузетом радњом извршења без обзира да ли је оштећени власник или корисник рачунарске мреже.

Извршилац дела може да буде свако лице, а у погледу кривице је потребан директни умишљај који квалификује наведена намера. За ово дело је прописана новчана казна или казна затвора до три године.

Лакши облик дела постоји када је учинилац предузео радњу извршења – прикривање или лажно приказивање података у рачунару или рачунарској мрежи на законом предвиђени начин са намером да се другоме нанесе штета, дакле, да се друго физичко или правно лице оштети. Малициозна намера учиниоца да се другоме нанесе имовинска или неимовинска штета представља привилегујућу околност за коју је Закон прописао новчану казну или казну затвора до шест месеци.

38 D. Jovašević, V. Ikanović, Krivično pravo Republike Srpske, Posebni deo, Banja Luka, 2012, 189–192.

Ово дело има два тежа облика. Први тежи облик дела за који је прописана казна затвора од једне до осам година постоји ако је услед предузете радње извршења основног дела прибављена имовинска корист (за учиниоца или друго лице) у износу преко 450.000 динара. Висина прибављене имовинске користи представља квалификаторну околност. Она се мора налазити у узрочно-последичној вези са предузетом радњом извршења. Други тежи облик дела постоји ако је предузетом радњом извршења учинилац за себе или другог прибавио противправну имовинску корист у износу преко 1.500.000 динара. За ово дело је прописана казна затвора од две до десет година.

4.5. Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података

Ново дело из члана 304а. КЗ састоји се у производњи, продаји, набављању ради употребе, увозу, дистрибуцији или стављању на располагање на други начин: а) уређаја и рачунарских програма који су пројектовани или првенствено намењени у сврхе извршења неког од кривичних дела против безбедности рачунарских података и б) рачунарске шифре или сличног податка путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буду употребљени за извршење наведених кривичних дела или у поседовању неког од наведених средстава у намери њихове употребе за извршење наведених кривичних дела. Овом инкриминацијом је прописана кажњивост за припремне радње као самостално кривично дело. Објект заштите је безбедност рачунарских система и података. Као објект напада могу се јавити: 1) рачунарски уређај, 2) рачунарски програм, 3) рачунарска шифра и 4) рачунарски подаци путем којих се може приступити рачунарском систему.

С обзиром на радњу извршења дело има два облика испољавања. Први облик дела се предузима са више алтернативно предвиђених радњи извршења. То су: 1) производња – стварање, прављење до тада непостојећег предмета или преправљање, прерада постојећег предмета, 2) продаја – замена предмета за домаћи или инострани новац, 3) набављање ради употребе – долажење у посед предмета на било који начин, са накнадом или без накнаде, на дозвољени или недозвољени начин. Битно је да се радња предузима у намери даље употребе оваквих предмета, 4) увоз – уношење или примање из иностранства у земљу предмета, непосредно или посредно, било којим начином или средством, 5) дистрибуција – омогућавање другим лицима да дођу у посед предмета и 6) стављање на располагање – чињење доступним предмета индивидуално неодређеном броју лица на било који начин.

Други облик дела се састоји у поседовању предмета. То је непосредна или посредна државина, фактичка власт учиниоца над предметом. За постојање дела је битно да се радња извршења предузима у односу: 1) на

одређене предмете: а) рачунарски уређај, б) рачунарски програм, в) рачунарску шифру и г) рачунарски податак путем кога се може приступити рачунарском систему у целини или неком његовом делу и 2) у одређеној намери, циљу – ради извршења неког од кривичних дела против безбедности рачунарских података, без обзира да ли је неко од ових кривичних дела уопште извршено или покушано.

Извршилац дела може да буде свако лице, а у погледу кривице потребан је умишљај. За први облик дела је прописана казна затвора од шест месеци до три године, а за други облик дела новчана казна или казна затвора до једне године. Уз казну суд обавезно изриче и меру безбедности одузимања предмета.

5. ЗАКЉУЧАК

Рачунарски криминалитет, било класични, било организовани полако, али сигурно заузима своје место у обиму, динамици и структури савременог криминалитета уопште, а посебно као облик угрожавања културног наслеђа свих врста и облика испољавања. Уочавајући опасности од злоупотребе рачунара и савремене технологије која је повезана са рачунарским системима међународна заједница је реаговала доношењем одређених међунароних докумената. Стандарди садржани у њима су тако постали основа за јединствену акцију појединих држава и на националном плану у циљу спречавања и сузбијања рачунарског криминалитета свих врста, облика и видова испољавања, па тако и оних облика којима се повређује или угрожава културно наслеђе.

На бази међународних стандарда које је прихватила и Република Србија, још 2003. године је у домаћем кривичном законодавству уведено више рачунарских кривичних дела са различитим облицима и видовима испољавања и системом кривичних санкција за њихове учиниоце. Потом је формитран систем државних органа специјализованих за откривање и доказивање кривичних дела ове врсте као што су тужилац за високотехнолошки криминал и одељење Вишег суда у Београду за високотехнолошки криминал уз истовремено формирање и специјализованих органа у МУП-у.

Prof. *Dragan Jovašević*, L.L.D.
Full Professor, Law Faculty University of Niš

SECURITY PROTECTION OF THE DIGITAL DATABASES OF CULTURAL HERITAGE OF THE REPUBLIC OF SERBIA

Summary

On the basis of ratified international documents of universal and regional character, the majority of countries, and so the Republic of Serbia also, in its national legislation, recognizes several computer related criminal acts which serve to protect different types

of digital databases, and so it protects digital databases of cultural heritage. For the perpetrators of these specific crimes there is a prescription of criminal responsibility and culpability of physical and juridical persons. Besides specific computer related crimes, in modern times many other old classical crimes (theft, fraud, forgery) take on a new dimension with a greater degree of severity and danger when they are committed using computers or computer systems. Because it mostly involves criminality which does not involve geographic and temporal correlation of the perpetrator and his act of perpetration and the caused consequence, i.e. injured person, modern legislation recognizes also special evidence collection procedures in the process of discovering and proving these crimes. This paper deals with the idea and the characteristics of computer crime which is done to the detriment of the digital databases of cultural heritage of the Republic of Serbia.

Keywords: digital database, cultural heritage, law, criminal offence, criminal sanction, Serbia