UDK: 343.98:004.006
Biblid 1451-3188, 13 (2014)
Год XIII, бр. 47–48, стр. 40–56
Изворни научни рад

Проф. др Драган ЈОВАШЕВИЋ[1]

РАЧУНАРСКИ КРИМИНАЛИТЕТ У СРБИЈИ И ЕВРОПСКИ СТАНДАРДИ

ABSTRACT

The new criminal law of the Republic of Serbia, which was adopted in 2005, prescribes criminal liability and punishability for a number of criminal acts against the security of computer data. The perpetrator performs these computer criminal acts by the abuse of computers, this causing property or non-property damage to other natural or legal persons. These incriminations basically include European standards defined by the Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime as well as a number of other European documents. The paper analyses the basic characteristics of cyber crimes in Serbia and to what extent they are harmonised with the European standards.

Key words: Computer abuse, European standards, crime, responsibility, sanction.

I) УВОД

Савет Европе је доношењем Конвенције о кибернетичком (сајбер) криминалу (Convention on Cybercrime, ETS 185) од 23. новембра 2001. године,[2] 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,

[1] Редовни професор, Правни факултет Универзитета у Нишу, Ниш, e-mail: jovas@prafak.ni.ac.rs.

[2] Berislav Pavišić, *Kazneno pravo Vijeća Evrope*, Tehnička knjiga, Zagreb, 2006, str. 261-265.

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 пропише кривичне санкције за њихове учиниоце (физичка или правна лица). Уз ову Конвенцију усвојен је 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). Имајући у виду утврђене обавезе за државе чланице Савета Европе, било је логично очекивати да ће и у домаћем кривичном законодавству (тада Државној заједници Србија и Црна Гора) 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 кривичноправни систем уведено је више рачунарских кривичних дела у глави 16а. под називом: „Кривична дела против безбедности рачунарских података".[3] Идентична кривична дела уведена су и у Кривичном законику Црне Горе 2003. године у глави 28. под истим називом.[4]

II) ЕВРОПСКИ СТАНДАРДИ ЗАШТИТЕ РАЧУНАРСКИХ СИСТЕМА

У основи Конвенције о кибернетичком криминалу, као обавезујућем међународном документу који је донет од стране најзначајније и најмасовније европске регионалне организације, налази се више претходно донетих препорука као што су:

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] Драган Јовашевић, *Коментар Кривичног закона Републике Србије са судском праксом*, Номос, Београд, 2003, стр. 351-361.

[4] Љубиша Лазаревић, Бранко Вучковић, Весна Вучковић, *Коментар Кривичног законика Црне Горе*, Обод, Цетиње, 2004, стр. 816-824.

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 процесог права који су везани за информатичку технологију.

Конвенција о кибернетичком криминалу 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 олакашава се 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[5] 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 дати су 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): незаконти 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 у виду подстрекавања и помагања, као и да се поред одговорности физичких лица, за ова дела предвиди и кривична

[5] Stephanos Emm Kareklas, *Priručnik za krivično pravo Evropske unije*, Institut za uporedno pravo i Mladi pravnici, Beograd, 2009, str. 94-97.

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

III) ОПШТЕ КАРАКТЕРИСТИКЕ КРИВИЧНОПРАВНЕ ЗАШТИТЕ РАЧУНАРСКИХ ПОДАТАКА

Објект заштите ових кривичних дела јесте безбедност рачунарских (компјутерских) података и система, односно рачунарске мреже.[6] Иако је данас уобичајено да се ова кривична дела обухватају појмом компјутерски криминалитет, наш законодавац за њих је ипак употребио термин рачунарски криминалитет. Но, поред овог назива за кривична дела систематизована на овом месту, наше законодавство употребљава и појам високотехнолошки криминал.[7] Под овим појмом подразумева се 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.[8]

При томе је Кривични законик (КЗ)[9] из 2005. године у члану 112. одредио појам и карактеристике: рачунарског податка, рачунарске мреже, рачунарског програма, рачунарског вируса, рачунара и рачунарског система у смислу објекта напада код ових кривичних дела. Рачунарски податак је 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 (став 17). Рачунарска мрежа представља скуп међусобно

[6] Bofo Brvar, „Pojavne oblike zlorabe računalnika", *Revija za kriminalistiko in kriminologijo*, Ljubljana, broj 2/1982, str. 27-32; Vlado Vodinelić, „Metodika otkrivanja, razjašnjenja i dokazivanja računarskog kriminaliteta", *Priručnik,* Zagreb, broj 4/1990, str. 330-337.

[7] 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 (Службени гласник Републике Србије број 61/2005).

[8] Драган Јовашевић, „Кривичноправна заштита безбедности рачунарских података", *Правни информатор*, Београд, број 6/2003, стр. 53-58.

[9] Службени гласник Републике Србије број 85/2005.

повезаних рачунара, односно рачунарских система који комуницирају размењујући податке (став 18). Рачунарски програм је уређени скуп наредби који служи за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара (став 19). 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 (став 20). Рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке (став 33). 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 (став 34).

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. 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 штету.[10] Тако рачунар постаје средство, оруђе за извршење кривичних дела. За различите облике и видове злоупотребе рачунара у теорији се употребљавају различити називи: злоупотреба рачунара, деликти уз помоћ рачунара, информатички криминалитет, рачунарски криминалитет, сајбер криминалитет, техно криминалитет, итд. Под појмом рачунарског криминалитета подразумева се 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

[10] Слободан Петровић, „Компјутерски криминалитет", *Безбедност*, Београд, број 1/1994, стр. 32-40.

другоме нанесе штета. Из овако одређеног појма рачунарског криминалитета произилазе његове карактеристике: 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.[11] Рачунарски криминалитет[12] 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 ранијих појавних облика, већ познатих кривичних дела која под утицајем злоупотребе компјутера мењају традиционални, класични начин и модус испољавања, јављају се и нови облици противправног понашања који не познају границе између држава. 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 слободе и права човека и грађана на разне начине, одавање личне, пословне и других видова тајни и сл. Извршиоци ових кривичних дела 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 технолошка средства доступна у физичком смислу. Ова се кривична дела врше прикривено, често без видљиве просторне и временски блиске повезаности

[11] Зоран Ђокић и Саша Живановић, „Компјутерски криминал као обележје прогресивног криминалитета", Зборник радова, *Казнено законодавство – прогресивна или регресивна решења*, Београд, 2005, стр. 305-318.

[12] Никола Китаровић, „Компјутерски криминалитет", *Билтен судске праксе Врховног суда Србије*, Београд, број 2-3/1998, стр. 52-56.

између учиниоца дела и оштећеног (пасивног субјекта). У пракси постоји већа или мања временска разлика између предузете радње извршења и тренутка наступања 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.

IV) ПОЈЕДИНА РАЧУНАРСКА КРИВИЧНА ДЕЛА

Нови Кривични законик Републике Србије, са применом од 1. јануара 2006. године, преузео је у великој мери низ утврђених европских стандарда који предвиђа наведена европска конвенција како би у потпуности створио основе за ефикасну, квалитетну, закониту и благовремену кривичноправну заштиту рачунарских података, система и других заштићених вредности. У односу на првобитна решења, септембра 2009. године додато је ново кривично дело прописано у члану 304а.КЗ. Тако данас систем кривичних дела против безбедности рачунарских података чине следећа кривична дела:[13]

1. Оштећење рачунарских података и програма (члан 298. КЗ),
2. Рачунарска саботажа (члан 299. КЗ),
3. Прављење и уношење рачунарских вируса (члан 300. КЗ),
4. Рачунарска превара (члан 301. КЗ),
5. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302. КЗ),
6. Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303. КЗ),
7. Неовлашћено коришћење рачунара или рачунарске мреже (члан 304. КЗ) и
8. Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а. КЗ).

[13] Војислав Ђурђић и Драган Јовашевић, *Кривично право, Посебни део,* Номос, Београд, 2010, стр. 215-217.

1) Оштећење рачунарских података и програма

Кривично дело из члана 298. састоји се у неовлашћеном брисању, измени, оштећењу, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма.[14] 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 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.[15] За постојање овог дела битно је 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

[14] Зоран Ђокић и Саша Живановић, „Компјутерски криминал као обележје прогресивног криминалитета'', Зборник радова, *Казнено законодавство – прогресивна или регресивна решења*, Београд, 2005, стр. 305-318.

[15] Љубиша Лазаревић, Бранко Вучковић, Весна Вучковић, *Коментар Кривичног законика Црне Горе,* оп. цит., стр. 816-817.

погледу кривице потребан је умишљај. За ово дело прописана је 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 прописана је казна затвора од три месеца до три године. Други тежи облик дела за који је прописана казна затвора од три месеци до пет година постоји ако је предузетом радњом основног дела проузрокована имовинска штета у износу преко 1.500.000 динара.

2) Рачунарска саботажа

Ово 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.[16] 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.[17] 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,

[16] Никола Китаровић, „Компјутерски криминалитет", *Билтен судске праске Врховног суда Србије*, Београд, број 2-3/1998, стр. 52-56.

[17] Драган Јовашевић, *Коментар Кривичног закона Републике Србије са судском праксом,* оп. цит., стр. 354-355.

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 и 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 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 је дело прописана казна затвора од шест месеци до пет година.

3) Прављење и уношење рачунарских вируса

Специфично кривично дело из члана 300. КЗ састоји се у прављењу рачунарског вируса у намери његовог уношења или његовом уношењу у туђи рачунар или рачунарску мрежу.[18] Објект заштите је безбедност

[18] Драган Јовашевић, *Коментар Кривичног закона Републике Србије са судском праксом,* ибид, стр. 355-356.

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.[19] 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 прописана је 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 битно је да је учинилац свестан, да зна да у време предузимања радње – рада на рачунару 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.

4) Рачунарска превара

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

[19] Драган Јовашевић, „Кривичноправна заштита безбедности рачунарских података", *Правни информатор*, Београд, број 6/2003, стр. 53-58.

електронске обраде и преноса података у намери да се себи или другом прибави противправна имовинска корист и тиме проузрокује имовинска штета другом лицу.[20] 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.[21] 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 бити свако лице, а у погледу кривице потребан је директни умишљај који квалификује наведена намера. За ово дело прописана је новчана казна или казна затвора до три године. Лакши облик дела постоји када је учинилац предузео радњу извршења – прикривање или лажно приказивање податка 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.

[20] Ksenija Turković et al., *Komentar Kaznenog zakona*, Narodne novine, Zagreb, 2013, стр. 345-346.

[21] Драган Јовашевић, „Обележја компјутерског криминалитета", *Правни информатор*, Београд, број 3/1998, стр. 56-62.

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. 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 је дело прописана казна затвора од две до десет година.

5) Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података

Следеће рачунарско дело из члана 302. КЗ састоји се у неовлашћеном укључивању у рачунар или рачунарску мрежу, или у неовлашћеном приступу електронској обради података кршењем мера заштите.[22] Објект заштите је безбедност рачунара или рачунарске мреже, односно система електронске обраде података који су заштићени посебним техничким и другим мерама заштите. Радња извршења је неовлашћено укључивање у рачунар или рачунарску мрежу или приступ електронској обради података.[23] То је улазак, продирање, приступ у заштићени систем рачунарских података, у систем електронске обраде или преноса података, као и у рачунарску мрежу у целини или њен поједини део. Битно је да се ради о рачунару, рачунарском систему или систему електронске обраде података који су заштићени посебним мерама заштите. Стога се радња извршења предузима на одређени законом предвиђени начин: 1) неовлашћено и 2) кршењем мера заштите (поступањем противно свим прописаним мерама или само појединим мерама, и то чињењем или нечињењем). Извршилац дела може бити свако лице које поседује одређена знања из области заштите рачунара или рачунарских система. У погледу кривице потребан је умишљај. За ово је дело прописана новчана казна или казна затвора до шест месеци.

[22] Драган Јовашевић, *Коментар Кривичног закона Републике Србије са судском праксом,* оп. цит., стр. 359-360.

[23] Ksenija Turković et al., *Komentar Kaznenog zakona*, op. cit., str. 341-342.

Дело има два тежа облика. Први тежи облик дела постоји у случају снимања или употребе рачунарског податка који је добијен неовлашћеним укључивањем у туђи рачунар или рачунарску мрежу, или туђи систем електронске обраде података под условом да је то учињено кршењем мера заштите. За ово дело прописана је новчана казна или казна затвора до две године. Без значаја је у ком циљу или у којој намери је употребљен на овај начин прибављен (снимљен) рачунарски податак. Други тежи облик дела, за који је прописана казна затвора до три године, постоји ако је неовлашћеним укључивањем, кршењем мера заштите прибављен рачунарски податак (један или више њих) који је потом употребљен, услед чега је дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже, или су наступиле друге тешке последице за друго (физичко или правно) лице. Теже последице могу бити имовинске или неимовинске природе, али морају бити у узрочно-последичној вези са употребом податка до кога се дошло неовлашћеним укључивањем или приступом. За постојање овог тежег дела битно је да је дошло до наступања теже последице повреде у виду застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или да су наступиле друге тешке последице. Које су то тешке последице представља фактичко питање које судско веће решава у конкретном случају.

6) Спречавање и ограничавање приступа јавној рачунарској мрежи

Кривично дело из члана 303. КЗ састоји се у неовлашћеном спречавању или ометању приступа јавној рачунарској мрежи.[24] Објект заштите је јавна рачунарска мрежа и слободан приступ истој од стране индивидуално неодређеног броја лица. Мотив ове инкриминације је спречавање монопола у коришћењу јавне рачунарске мреже. Радња извршења је спречавање или ометање слободног приступа јавној рачунаској мрежи.[25] Спречавање је онемогућавање у потпуности, трајно или за одређено краће време, приступа другом лицу јавној рачунарској мрежи. То може бити учињено физичким спречавањем, постављањем одређених услова или препрека, односно захтевањем испуњења одређених претпоставки. Ометање је делимично

[24] Драган Јовашевић, „Обележја компјутерског криминалитета", *Правни информатор*, Београд, број 3/1998, стр. 56-62.

[25] Никола Китаровић, „Компјутерски криминалитет", *Билтен судске праске Врховног суда Србије,* Београд, број 2-3/1998, стр. 52-56.

усложавање, отежавање, чињење недоступним или условљавање другом лицу да несметано, слободно, по свом нахођењу приступи или користи јавну рачунарску мрежу. Битно је да се ради о радњи извршења која је предузета неовлашћено (од неовлашћеног лица, мимо услова и претпоставки и ван поступка који су законом или другим прописима из ове области предвиђени) у односу на јавну рачунарску мрежу. Извршилац дела може бити свако лице, а у погледу кривице потребан је умишљај. За ово дело прописана је новчана казна или казна затвора до једне године. Тежи облик дела, за који је прописана казна затвора до три године, постоји ако је радњу извршења предузело службено лице у вршењу службе. Својство учиниоца дела и начин предузимања радње извршења – кршењем или злоупотребом службене дужности, представљају квалификаторне околности за које закон прописује строже кажњавање.

7) Неовлашћено коришћење рачунара или рачунарске мреже

Кривично дело из члана 304. КЗ састоји се у неовлашћеном коришћењу рачунарске услуге или рачунарске мреже у намери да се себи или другом лицу прибави противправна имовинска корист.[26] Објекат заштите је законитост и савесност у коришћењу рачунарских система – услуга или мреже од свих облика злоупотребе и несавесности. Радња извршења је неовлашћено коришћење, дакле употреба, искоришћавање података који су прибављени или похрањени у рачунару или рачунарској мрежи у користољубивој намери – намери да на овај начин учинилац за себе или друго физичко или правно лице прибави противправну (не било какву) корист. Ова намера мора да постоји на страни учиниоца у време предузимања радње извршења, али она не мора у конкретном случају да буде и остварена. Извршилац дела може бити свако лице, а у погледу кривице потребан је директни умишљај који карактерише наведена намера. За ово дело прописана је новчана казна или казна затвора до три месеца.

8) Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података

Ово је ново рачунарско кривично дело (члан 304а. КЗ) које је уведено новелом Кривичног законика из 2009. године. Заправо, овде се ради о

[26] Драган Јовашевић, *Коментар Кривичног закона Републике Србије са судском праксом,* оп. цит., стр. 360-361.

кажњивим припремним радњама за извршење неког од рачунарских кривичних дела. Само дело[27] састоји се у поседовању, прављењу, набављању, продаји или давању другоме на употребу рачунара, рачунарског система, рачунарског податка или програма за извршење неког од кривичних дела против безбедности рачунарских података. За ово дело прописана је казна затвора од шест месеци до три године, при чему се обавезно од учиниоца одузимају предмети извршења дела применом посебне мере безбедности одузимања премета. Објект заштите је и у овом случају безбедност рачунарских система и података, али која се обезбеђује на специфичан начин – пре непосредног предузимања радње кривичног дела. Радња извршења је вишеструко алтернативно одређена. Она се састоји у: поседовању, прављењу, набављању, продаји или давању другоме на употребу предмета. Поседовање је сама државинска власт извршиоца над предметима, непосредно или посредно што укључује његову могућност њиховог коришћења. Прављење је израда новог или преправљање, преинака постојећег предмета. Набављање је долажење у посед, у државину предмета. Продаја је замена предмета за домаћи или страни новац, а давање на употребу другоме је радња помагања којом се стварају услови да друго лице непосредно употреби ове предмете. Битно је да се радња извршења предузима: 1) у односу на законом тачно одређене предмете као што су: рачунар, рачунарски систем, рачнарски податак или програм и 2) у одређеној намери – за извршење неког од кривичних дела против безбедности рачунарских података.

V) ЗАКЉУЧАК

Прихватањем одредби низа релевантних европских докумената који су коначно инаугурисани усвајањем Конвенције о кибернетичком криминалу, у националним законодавствима држава чланица Савета Европе створена је правна основа за увођење посебне врсте „рачунарски, компјутерских" кривичних дела која имају за циљ да обезбеде ефикасно, квалитетно, законито, безбедно и уз поверење обављање различитих послова и услуга путем рачунара. Заправо, увођењем посебних кривичних дела обезбеђује се безбедност рачунарских система и података у националним и међународним размерама. Тако је и у Републици Србији, почев од 2003. године, у кривичноправни систем уведено више кривичних дела ове врсте при чему је законодавац поштујући утврђене европске стандарде

[27] Илија Симић и Александар Трешњев, *Кривични законик с краћим коментаром*, Инг про, Београд, 2010, стр. 213-214.

обезбедио кривичне санкције за поједине облике и видове испољавања прописаних рачунарских кривичних дела. Слична кривична дела су саставни део и новодонетог Кривичног законика из 2005. године. На тај начин, уз одговарајуће процесне претпоставке (формирање посебних органа за сузбијање високотехнолошког криминала у оквиру полиције, јавног тужилаштва и суда), створене су претпоставке за ефикасну борбу наше државе са овим савременим облицима и видовима криминалитета који не познаје границе између држава.

VI) ИЗВОРИ

- Brvar, B., „Pojavne oblike zlorabe računalnika'', Revija za kriminalistiko in kriminologijo, Ljubljana, broj 2/1982.
- Vodinelić, V., „Metodika otkrivanja, razjašnjenja i dokazivanja računarskog kriminaliteta'', *Priručnik,* Zagreb, broj 4/1990.
- Ђокић, З., Живановић, С., „Компјутерски криминал као обележје прогресивног криминалитета'', Зборник радова, *Казнено законодавство – прогресивна или регресивна решења*, Београд, 2005.
- Ђурђић, В., Јовашевић, Д., *Кривично право, Посебни део,* Номос, Београд, 2010.
- Јовашевић, Д., „Обележја компјутерског криминалитета'', *Правни информатор*, Београд, број 3/1998.
- Јовашевић, Д., *Коментар Кривичног закона Републике Србије са судском праксом*, Номос, Београд, 2003.
- Јовашевић, Д., „Кривичноправна заштита безбедности рачунарских података'', *Правни информатор*, Београд, број 6/2003.
- Kareklas, C.E., *Priručnik za krivično pravo Evropske unije*, Institut za uporedno pravo i Mladi pravnici, Beograd, 2009.
- Китаровић, Н., „Компјутерски криминалитет'', *Билтен судске праске Врховног суда Србије*, Београд, број 2-3/1998.
- Лазаревић, Љ., Вучковић, Б., Вучковић, В., *Коментар Кривичног законика Црне Горе*, Обод, Цетиње, 2004.
- Pavišić, B., *Kazneno pravo Vijeća Evrope,* Tehnička knjiga, Zagreb, 2006.
- Петровић, С., „Компјутерски криминалитет'', *Безбедност*, Београд, број 1/1994.
- Симић, И., Трешњев, А., *Кривични законик с краћим коментаром*, Инг про, Београд, 2010.
- Службени гласник Републике Србије број 61/2005.
- Службени гласник Републике Србије број 85/2005.
- Turković, K., et al., *Komentar Kaznenog zakona*, Narodne novine, Zagreb, 2013.