UDK: 343.533::004(497.11)
Biblid 1451-3188, 14 (2015)
Год XIII, бр. 51, стр. 92–103
Изворни научни рад

Јоко ДРАГОЈЛОВИЋ, Msr.[1]
Далибор КРСТИНИЋ, Msr.[2]

ЕВРОПСКИ СТАНДАРДИ У БОРБИ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА И ЊИХОВА ИМПЛЕМЕНТАЦИЈА У ЗАКОНОДАВСТВУ РЕПУБЛИКЕ СРБИЈЕ

ABSTRACT

In recent years we have witnessed the IT revolution and along with it the internet revolution that is present in almost all areas of human activity. However, no matter how many advantages computers have brought, and what is their significance in contemporary life, they undoubtedly expose users to numerous risks such as invasion of privacy, the different types of fraud, to the destruction of intellectual property, identity theft, etc. So, all of this has created opportunities and the atmosphere for the emergence of new forms of crime, i.e. the occurrence of cyber crime. Considering there it is word about crime who does not know national boundaries, its prevention and combating against, have dedicated themselves to various international organizations. Consequently, the authors in this work will analyze the Convention on Cyber Crime, which currently represents the only international-recognized and continental widespread legal instrument in the fight against cyber crime, as well as its current implementation in the legislation of Republic of Serbia.

Key words: High-tech crime, the Convention on Cyber Crime, European standards, implementation.

[1] Правни факултет за привреду и правосуђе у Новом Саду, Универзитет Привредна академија у Новом Саду. Е-маил: jokodragojlovic@yahoo.com

[2] Правни факултет за привреду и правосуђе у Новом Саду, Универзитет Привредна академија у Новом Саду; email: krstinicdalibor@yahoo.com

I) УВОД

Данас се компјутери и компјутерска технологија могу злоупотребљавати на различите начине јер пружају могућност за вршење и планирање различитих кривичних дела. Велике могућности у свим сферама друштвеног живота које су се човеку указале развојем информационе технологије, несумњиво за собом су повукле и одређене ризике и опасности које се огледају у различитим видовима злоупотреба компјутера а самимим тим и компјутерских мрежа, пре свега интернета. С тим у вези, без обзира колико су рачунари донели предности и колики је њихов значај у савременом животу, они несумњиво излажу кориснике и бројним ризицима као што су нарушавање приватности, различитим врстама превара, деструкцији интелектуалних добара, крађи идентитета и слично. Дакле, све ово створило је могућности и атмосверу и за појаву нових облика криминалитета, тј. за појаву високотехнолошког криминалитета. Када је реч о дефинисању високотехнолошког криминалитета међу ауторима не постоји сагласност. Високотехнолошки криминалитет је готово немогуће дефинисати на јединствен и прецизан начин с обзиром да је реч о криминалитету код којег се нови појавни облици из дана у дан појављују, а већ постојећи додатно мењају и усавршавају. Међутим без амбиција да уђемо у дубљу анализу и дефинисање овог феномена, за потребе овог рада истаћи ћемо дефиницију која се налази у позитивноправним прописима наше државе. Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала[3], по први пут је и у домаћем законодавству дефинисан појам високотехнолошког криминала и то као: вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, док се под производима у електронском облику посебно подразумевају рачунарски програми и ауторска дела која се могу употребити у електронском облику.[4] Дакле, можемо разликовати кривична дела у којима се рачунари користе као средство извршења, објекат извршења као и кривична дела која се врше на основу незаконитог коришћења интернета. Високотехнолошки криминалитет обилује низом специфичности које се пре свега огледају у великој феноменолошкој разноврсности, специфичности учинилаца ових кривичних дела, брзини вршења кривичног дела, тежини последице и висини штете, великој тамној

[3] „Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала“, *Службени гласник РС*, бр. 61/05 и 104/09.

[4] „Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала“, *Службени гласник РС*, бр. 61/05 и 104/09, члан 2. став 1. и 2.

бројци, као и проширеном простору криминалног деловања који не захтева присуство извршиоца на месту извршења кривичног дела, а самим тим и транснационални карактер.[5] Имајући у виду напред изнете специфичности, јасно је да се ради о криминалитету који представља глобални безбедносни проблем чијем су се сузбијању посветиле и одређене међународне организације.

II) ЕВРОПСКИ СТАНДАРДИ У БОРБИ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА

Како је високотехнолошки криминалитет појава која не заобилази ни једну земљу света њеном спречавању и сузбијању су се супроставиле и одређене међународне организације. Први видови борбе против високотехнолошког криминалитета у Европи везују се за Конференцију Савета Европе о криминолошким аспектима привредног криминала. Поменута Конференција одржана је у Стразбуру 1976. године, на којој је представљено и неколико појавних облика високотехнолошког криминалитета. Након Конвенције о криминолошким аспектима привредног криминала из 1976. године, на којој је први пут указано на неколико различитих врста високотехнолошког криминалитета, Савет Европе је прве кораке у области регулације високотехнолошког криминала започео 1985. години, именовањем стручне комисије ради разматрања правних питања из ове сфере.[6] Након тога, 1989. године донета је Препорука о криминалним активностима повезаним са употребом рачунара (Савет Европе: Препорука бр. Р (89) 9) где је нагласак био на питањима материјалног кривичног права, а 1995. године донета је Препорука која је за предмет регулисања узела питања која се тичу процедуралних, односно процесних правила у вези са информатичким технологијама (Савет Европе: Препорука бр. Р (95) 13).

[5] Драган Јовашевић, Д., Тарик Хашимбеговић, *Кривичноправна заштита безбедности рачунарских података,* 2003, стр. 2, Интернет: http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-08.pdf (15. 01. 2015.); Јелена Матијашевић, *Кривичноправна регулатива рачунарског криминалитета*, Правни факултет за привреду и правосуђе у Новом Саду, Нови Сад, 2013; Ранко Јерковић, „Високотехнолошки криминал-актери и жртве“, *Ревија за безбедност, стручни часопис о корупцији и организованом криминалу*, Центар за безбедносне студије, Vol. 3, бр. 3/2009, Београд, 2009, стр. 28.

[6] Жељко Бјелајац, Јелена Матијашевић, Душко Димитријевић, „Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала“, *Међународна политика,* Vol. 63, бр. 1146, Институт за међународну политику и привреду, Београд, 2012, стр. 72.

Поред Савета Европе и остале међународне организације су донеле низ докумената који се односе на ову област,[7] али најважнији међународноправни документ из ове области свакако јесте Конвенција о *cyber* криминалу. У том смислу, Савет Европе је доношењем Конвенције о *cyber* криминалу (*Convention on Cybercrime, ETS 185*) од 23. новембра 2001. године[8] (у даљем тексту Конвенција) покушао да постави основе јединственог правног регулисања материјалног и процесног кривичног права из области високотехнолошког криминалитета. Конвенција је потписана у Будимпешти и представља међународноправни инструмент којим се по први пут регулишу проблеми везани за високотехнолошки криминалитет и савремене медије. Србија је Конвенцију потписала 2005. године а ратификовала 2009. године[9]. Овом Конвенцијом су прописане радње и мере, како материјално, тако и процесноправне природе, које су усмерене ка регулисању друштвено штетног понашања у овој области и које примењују савремене истражне методе приликом откривања и гоњења извршиоца кривичних дела, као што су претрага рачунарских мрежа и пресретање рачунарских података.[10] Конвенција има за циљ првенствено:

1. усклађивање домаћег кривичног материјалног права, елемената кривичних дела и повезаних одредби у подручју *cyber* криминалитета,
2. пружање домаћем кривичном процесном праву овлашћења која су потребна за истрагу и прогон таквих кривичних дела, као и других кривичних дела учињених помоћу рачунарског система и
3. постављање брзог и ефикасног режима међународне сарадње.[11]

Конвенција је састављена из четири поглавља: Прво поглавље обухвата терминологију тј. значење израза који се користе у Конвенцији. Па тако су дефинисани појмови као што су рачунарски систем, рачунарски подаци, аутоматска обрада података, пружалац услуга, подаци о саобраћају,

[7] Лидија Комлен – Николић, at. al. *Сузбијање високотехнолошког криминала,* Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010, стр. 32-69.

[8] *Convention on Cybercrime CETS No.: 185,* Интернет: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (16. 01. 2015.)

[9] Закон о потврђивању Конвенције о Високотехнолошком криминалу, *Службени гласник РС*, бр. 19/09.

[10] Бранко Стаменковић, at. al., *Високотехнолошки криминал-практични водич кроз савремено кривично право и примјере из праксе, OEBS мисија у Црној Гори, Подгорица,* 2014, стр. 21.

[11] Миодраг Симовић, *Конвенција о кибернетичком криминалу – настанак, садржај и имплементација,* Интернет: http://www.godisnjakpf.rs/wp-content/uploads/2012/02/simovic 12.pdf (16. 01. 2015.)

рачунарска мрежа и слично. У другом поглављу налазе се одредбе које се односе на кривично материјално право, процесно право и надлежност. Ово поглавље је састављено из три дела, дакле први део су одредбе материјалног права, други део чине одредбе процесног права и трећи део је састављен од одредби које се односе на надлежност. Важност и значај првог дела другог поглавља се огледа у неопходности хармонизације законодавних решења. У том смислу, Конвенција садржи четири групе дела:

1. дела против поверљивости, интегритета и доступности рачунарских података и система (од члан 2 до члана 6 Конвенције),
2. дела везана за рачунаре (члан 7 и 8 Конвенције),
3. дела везана за садржаје (9 Конвенције).
4. дела везана за коришћење ауторских и сродних права (члан 10. Конвенције)

На овај начим постављене су 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).[12] Ово је посебно важно из разлога што неопходност истог или баш сличног кажњавања овог вида криминалитета у различитим државама представља нужан услов за пружања међународноправне помоћи. Дакле, основни постулат пружања међународноправне помоћи у кривичним стварима је постојање кажњивости у кривичноправном смислу одређеног људског понашања, које мора бити прописано како материјалноправним одредбама кривичног законодавства земље молиље, тако и замољене земље. Сходно томе, недостатка хармонизације материјалноправних прописа у овој области, довео би до нежељеног исхода у виду немогућности предузимања радњи које су на располагању органима откривања и гоњења, а тиме и ефективног онемогућавања санкционисања такве врсте противправног понашања.[13] У другом делу другог поглавља налазе се одредбе које се односе на овлашћења која су на располагању органима који су задужени за откривање ових кривичних дела. Брзина и правовременост је главни предуслов за ефикасно откривање ових кривичних дела. Како, мере и процесна овлашћења морају бити прилагођена иновацијама које су рачунари

[12] Драган Јовашевић, (2014). „Рачунарски криминалитет у Србији и европски стандарди“, *Европско законодавство*, Вол. 13, бр, 47-48/2014, Институт за међународну политику и привреду, Београд, 2014., стр. 41.

[13] Бранко Стаменковић, at. al., *Високотехнолошки криминал-практични водич кроз савремено кривично право и примјере из праксе*, op. cit., стр. 28.

донели, стога је неопходно да органи на располагању имају овлашћења која се односе на хитно очување похрањених података, претраживање и одузимање рачунарских података, прикупљање компјутерских података у реалном времену, пресретање података који се налазе у садржају електронских комуникација и сл. У трећем поглављу се налазе одредбе које се односе на међународноправну помоћ. Дакле у овом делу су садржане одредбе о међународноправној помоћи и поступку изручења. Међународна сарадња пре свега обухвата сва кривична дела која се односе и обухватају рачунаре и рачунарске системе и мреже, као и податке који су генерисани од стране рачунара који су употребљени или на други начин искоришћени у току рачунарске комуникације, као и прикупљање доказа у електронској форми у вези извршења кривичних дела. Ово значи да, без обзира да ли је кривично дело извршено употребом рачунара, рачунарског система или се ради о уобичајеном вршењу кривичног дела које није извршено путем рачунара, али укључује електронске доказе, чланови Конвенције могу и требају бити примењени.[14] Када је реч о изручењу, до њега може доћи само у случају ако је у обе државе потписнице прописано кривично дело кажњиво са најмање годину дана затвора.[15] Четврто поглавље садржи завршне одредбе. У овом делу су прописане одредбе које регулишу начин приступања и могућност потписивања ове Конвенције, њено дејство и примену. Уз ову Конвенцију усвојен је и Допунски протокол који се односи на криминализацију аката расистичке и ксенофобичне природе која су учињена коришћењем рачунарске технологије (у даљем тексту Допунски протокол). Овај протокол представља на неки начин допуну Конвенције.

Сврха Допунског протокола је двострука:

1. усклађивање материјалног кривичног права у борби против расизма и ксенофобије на интернету која ће помоћи у борби против таквих кривичних дела на националном и међународном нивоу;
2. побољшање међународне сарадње у том подручју и размена корисних искустава, посебно у области изручења и међународноправне помоћи.[16]

Под расистичким или ксенофобичним материјалом подразумева било који писани материјал или слика или било који други акт којим се испољава

[14] Миодраг Симовић, Конвенција о кибернетичком криминалу – настанак, садржај и имплементација, op. cit., стр. 37.

[15] Драган Прља, Марио Рељановић, Звонимир Ивановић, *Интернет право,* Институт за упоредно право, Београд, 2012, стр. 142-143.

[16] Ibid, стр. 40.

или подстиче мржња, дискриминација или насиље против против било којег појединца или групе на основу расног, верског, националног или етичког основа.

III) ЗАКОНОДАВНИ ОКВИР У БОРБИ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА У РЕПУБЛИЦИ СРБИЈИ

Република Србија је 2005. године потписала Конвенцију и Додатни протокол, а 2009. године је оба ова документ и ратификовала, чиме су постали саставни део домаћег правног поретка. Стим у вези, настале су формално-правно обавезе које се односе на хармонизацију националног законодавства са одредбама ове Конвенције и Допунског протокола, а самим тим и стварања нормативноправних претпоставки за ефикасније сузбијање овог облика криминалитета. Као што смо и напоменули, како национални извори који се односе на ову област, морају бити у складу са поменутом Конвенцијом и Додатним протоколом, непосредно након њихове ратификације, приступило се хармонизацији истих. Ово се пре свега односи на Законо о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Кривични законик[17] и Законик о кривичном поступку.[18] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала неспорно представља најважнији правни документ у борби против овог вида криминалитета у Србији. Овај Закон примењује се ради, откривања, кривичног гоњења и суђења кривичних дела против безбедности рачунарских података одређених Кривичним закоником и – кривичних дела против интелектуалне својине, имовине, привреде и правног саобраћаја код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2.000 или настала материјална штета прелази износ од 1.000.000 динара, као и кривичних дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати

[17] „Кривични законик“, *Службени гласник РС*, бр. 85/05, 88/05 – испр., 107/05 – испр., 72/09 и 111/09 и 121/12, 104/2013.

[18] „Законик о кривичном поступку“, *Службени гласник РС*, бр. 72/11, 101/11, 121/12, 32/13, 45/13 и 55/14.

кривичним делима високотехнолошког криминала.[19] Како је реч о кривичним делима код којих је за успешно откривање, спречавање, и суђење неопходно поседовање одређених знања и вештина, нужна је била специјализација и оснивање посебних организационих јединица. У том смислу, за поступање по предметима кривичних дела високотехнолошког криминалитета надлежно је Посебно тужилаштво које се налази у оквиру Вишег јавног тужилаштва у Београду. За послове органа унутрашњих послова по предметима у вези са овим кривичним делима надлежна је Служба за борбу против високотехнолошког криминалитета која се налази у оквиру министарства унутрашњих послова. За поступање по предметима за кривична дела високотехнолошког криминалитета када је реч о судској надлежности за територији Србије, у првом степену надлежн је Виши суд у Београду, а у другом степену Апелациони суда у Београду. У Вишем суду у Београду за поступање по предметима кривичних дела високотехнолошког криминалитета организује се Одељење за борбу против високотехнолошког криминала. Када је реч о Кривичном законику (у даљем тексту КЗ) истаћи ћемо кривична дела везана за област високотехнолошког криминалитета, а која су притом, обухваћена и Конвенцијом. Када је реч о кривичним делима прописаним у КЗ-у, најпре ћемо истаћи главу XXVII где су прописана кривична дела против безбедности рачунарских података: оштећење рачунарских податак из члана 298 КЗ-а, рачунарска саботажа из члана 299 КЗ-а, прављење и уношење рачунарских вируса из члана 300 КЗ-а, рачунарска превара из члана 301 КЗ-а, неовлашћени приступ заштићеном рачунару, рачунарској мрежи или електронској обради података из члана 302 КЗ-а, спречавање и ограничавање приступа јавној рачунарској мрежи из члана 303 КЗ-а, неовлашћено коришћење рачунара или рачунарске мреже из члана 304 КЗ-а и прибављање, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података из члана 304а КЗ-а. Важно је напоменути и кривична дела против интелектуалне својине из главе XX, и то: повреду моралних права аутора и интерпретатора из члана 198 КЗ-а, неовлашћено искоришћавање ауторског дела или предмета сродног права из члана 199 КЗ-а, неовлашћено уклањање или мењање електронских информација о ауторским и сродним правима из члана 200 КЗ-а, повреда проналазачког права из члана 201 КЗ-а и неовлашћено коришћење туђег дизајна из члана 202 КЗ-а. Напоменућемо и кривична дела из главе XVIII где се налазе кривична дела против полних слобода и то: приказивање

[19] „Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала“, *Службени гласник РС*, бр. 61/05 и 104/09, члан 3.

порнографског материјала и искоришћавање деце за порнографију из члан 185 КЗ-а и искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу члан 185б КЗ-а, као и кривична дела против привреде из главе XXII, и то кривично дело фалсификовање и злоупотреба платних картица из члана 225 КЗ-а, која се такође могу сматрати кривичним делима индикаторима високотехнолошког криминалитета. Такође, у великом броју случајева у пракси се јављају кривична дела везана за такозвани говор мржње и то путем злоупотребе интернета и сродних друштвених мрежа, и то кривично дело изазивање националне, расне и верске мржње и нетрпељивости из члана 317 КЗ-а, као и кривично дело расне и друге дискриминација из члана 387 КЗ-а, које су такође из домена такозваног говора мржње и врло често пристичу из злоупотребе Интернета.[20] Законик о кривичном поступку (у даљем тексту ЗКП) представља *lex generalis* када је реч о кривичноправној процедури. Посматрано са аспекта кривичних дела високотехнолошког криминалитета, најважније одредбе из овог законика јесу одредбе које се односе на привремено одузимање предмета (овде се подразумевају уређаји за аутоматску обраду података као и уређаји на којима се чувају електронски записи) из члан 147 ЗКП-а, претресање стана (овде се подразумева претресање уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи) из члан 152 ЗКП-а. Када је реч о посебним доказним радњама, важно је напоменути да се оне не могу предузети за кривична дела високотехнолошког криминалитета. Наиме, законодавац је настојао да задовољи захтеве за супсидијарношћу и сразмерношћу њихове примене, дајући предност људским правима. Ово питање је и у ранијим законским решењима изазивало много пажње и подељених ставова. Међутим, законодавац је у односу на ранија законска решења ипак посебну доказну радњу, тајни надзор комуникације, поред кривичних дела за која се примењују и остале посебне доказне радње[21] прописао и за следећа кривична дела: неовлашћено коришћење ауторског дела или предмета сродног права из члана 199 КЗ-а, оштећење рачунарског подака и програма из члана 298 став 3 КЗ-а, рачунарска саботажа из члана 299 КЗ-а, рачунарска превара из члана 301 став 3 КЗ-а и неовлашћен приступ

[20] Жељко Никач, Никола Аритоновић, *Сузбијање високотехнолошког криминала у Србији – Легислативни и оперативни аспекти,* у: Слободан Р. Петровић, уредник, „Злоупотреба информационих технологија и заштита", Удружење судских вештака за информационе технологије, Београд, 2014, електронски извор.

[21] Видети члан 162. „Законика о кривичном поступку", *Службени гласник РС*, бр. 72/11, 101/11, 121/12, 32/13, 45/13 и 55/14.

заштићеном рачунару, рачунарској мрежи или електронској обради података из члана 302 КЗ-а. Ово је и разумљиво јер је код ових кривичних дела *modus operandi* коришћење телекомуникационих мрежа и уређаја. Стога, мишљења смо да би ову посебну доказну радњу било неопходно проширити и на сва кривична дела која спадају или представљају индикаторе високотехнолошког криминалитета. Имајући у виду напред изнето, намеће се закључак да су нормативна решења из ове области у Србији у великој мери усклађена са Конвенцијом, међутим уколико, упоредимо оперативне капацитете ЗКП-а са једним од законодавних решења кривичног законодавства Републике Француске, којим се омогућава претрес циљног рачунара преко интернета, уз претходно добијену наредбу истражног судије, лако можемо схватити у колико мери заостајемо за савременим законодавством.[22]

IV) ИЗВОРИ

„Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала“, *Сл. гласник* РС, бр. 61/05 и 104/09.

„Закон о потврђивању Конвенције о Високотехнолошком криминалу“, *Сл. гласник* РС, бр. 19/09.

„Законик о кривичном поступку“, *Сл. гласник* РС, бр. 72/11, 101/11, 121/12, 32/13, 45/13 и 55/14.

„Кривични законик“, *Сл. гласник* РС, бр. 85/05, 88/05 – испр., 107/05 – испр., 72/09 и 111/09 и 121/12, 104/2013.

Convention on Cybercrime CETS No.: 185, Интернет: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (16. 01. 2015.)

Бјелајац Жељко, Матијашевић Јелена, Димитријевић Душко, „Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала“, *Међународна политика*, Вол. 63, бр. 1146, Институт за међународну политику и привреду, Београд, 2012.

Јерковић Ранко, „Високотехнолошки криминал - актери и жртве“, *Ревија за безбедност, стручни часопис о корупцији и организованом криминалу*, Центар за безбедносне студије, Вол. 3, бр. 3/2009, Београд, 2009.

Јовашевић Драган, „Рачунарски криминалитет у Србији и европски стандарди“, *Европско законодавство*, Вол. 13, бр, 47-48/2014, Институт за међународну политику и привреду, Београд, 2014.

[22] Лидија Комлен – Николић, at. al., *Сузбијање високотехнолошког криминала*, op. cit. стр. 273.

Јовашевић, Драган, Хашимбеговић, Тарик, Кривичноправна заштита безбедности рачунарских података, Интернет: http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-08.pdf (15. 01. 2015.)

Комлен – Николић Лидија, at. al. *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010.

Матијашевић Јелена, *Кривичноправна регулатива рачунарског криминалитета*, Правни факултет за привреду и правосуђе у Новом Саду, Нови Сад, 2013.

Никач Желько, Аритоновић Никола, *Сузбијање високотехнолошког криминала у Србији – легислативни и оперативни аспекти*, у: Слободан Р. Петровић уредник, „Злоупотреба информационих технологија и заштита", Удружење судских вештака за информационе технологије, Београд, 2014, електронски извор.

Прља Драган, Рељановић Марио, Ивановић Звонимир, *Интернет право*, Институт за упоредно право, Београд, 2012.

Симовић, М., Конвенција о кибернетичком криминалу – настанак, садржај и имплементација, Интернет: http://www.godisnjakpf.rs/wp-content/uploads/2012/02/simovic12.pdf (16. 01. 2015.)

Стаменковић, Бранко, at. al. (2014). *Високотехнолошки криминал-практични водич кроз савремено кривично право и примјере из праксе*, OEBS мисија у Црној Гори, Подгорица, 2014.

IV) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Последњих година сведоци смо информатичке револуција а заједно са њом и интернет револуције која је присутна у готово свим областима људске делатности. Међутим, без обзира колико су рачунари донели предности и колики је њихов значај у савременом животу, они несумњиво излажу кориснике бројним ризицима као што су нарушавање приватности, различитим врстама превара, деструкцији интелектуалних добара, крађи идентитета и слично. Дакле, све ово створило је могућности и атмосверу и за појаву нових облика криминалитета, тј. за појаву високотехнолошког криминалитета. Сходно томе, високотехнолошки криминалитет представља можда један од највећих безбедносних изазова двадесет првог века, како развијених тако и мање развијених држава. Ефикасна превенција, откривање и покретање поступака против извршилаца кривичних дела додатно је отежана његовим транснационалним карактером. Услед тога проблеми око надлежности и неусклађености кривичног законодавства долази у пуној мери

до изражаја. Стога, неопходно је стално радити на хармонизацији законских решења из ове области и на интезивирању међународноправне помоћи. Као што смо и видели, нормативна решења у Србији из ове области, представљају добру основу за вођење успешне борбе против овог вида криминалитета. Такође, постојећа нормативна решења су у значајној мери усклађена са европским стандардима, тј. са Конвенцијом и Допунским протоколом. Међутим, када је реч о овој врсти криминалитета неопходно је константно радити на преиспитивању и ревидирању законских решења, јер се високотехнолошки криминалитет јако брзо развија а нови појавни облици се из дана у дан појављују. Србија је ратификовањем Конвенције и Допунског протокола и инкорпорирањем њених одредби у национално законодавство показала јасну вољу и спремност у борби против високотехнолошког криминала, међутим за ефикасну борбу против овог вида криминалитета нису довољна само нормативна решења, поготово ако она не прате стварање услова за ефикасном борбом. Када кажемо стварање услова пре свега мислимо на адекватан персонални кадар са једне стране, као и одговарајуће техничке услове са друге стране.