Проф. др Миомира Костић, редовни професор *UDK: 343.41:004.738.5*
Правни факултет Универзитета у Нишу
Вида Вилић, *студенткиња докторских студија, Правни факултет Ниш*

БОРБА ПРОТИВ ЗЛОУПОТРЕБЕ ПРАВА НА ПРИВАТНОСТ У СВЕТЛУ КОНВЕНЦИЈЕ САВЕТА ЕВРОПЕ О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ[1]

Апстракт*: Проналазак и развој компјутера представља резултат фасцинантног развоја људске мисли и проналазаштва. Са повећањем употребе рачунара, рачунарских мрежа, интернета и броја корисника, повећавају се и могућности за њихову злоупотребу. Смањење ризика од злоупотребе могуће је једино развијањем јединствених стандарда за коришћење рачунара, рачунарских мрежа и интернета, као и доношењем и применом одговарајућих правних стандарда којима се инкриминишу понашања везана за њихову злоупотребу. У вези са компјутерским злоупотребама поставило се питање заштите појединачног личног права - права на приватност. Компјутерској злоупотреби приватности нарочито су изложене одређене групе људи о којима је прикупљен већи број података, то су на пример они који се најчешће користе одређеним друштвеним услугама и чије је понашање девијантно или криминално. Међународна и национална правна регулатива којима се забрањује компјутерски криминалитет треба да буду веома флексибилни и да прате свакодневни развој компјутерске технологије и иновација. Само развијањем компатибилних стандарда и правних прописа овакве иновације могу да се развијају уз смањење ризика од њихове злоупотребе. Начин на који успемо да обликујемо правне стандарде и законе везане за ову врсту криминалитета имаће утицаја на животе милиона људи. Компјутери постају технолошки све моћнији, а човечанство све зависније од њихове примене, што отвара велико поље за њихову злоупотребу и за вршење кривичних дела.*

Кључне речи*: компјутерски криминалитет, злоупотреба, право на приватност, међународна и национална правна регулатива, Савет Европе.*

1 Council of Europe – Convention on Cybercrime, Budapest 23.11.2001., ETS No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, приступ 01.11.2012.године

Увод

Проналазак и развој компјутера представља резултат фасцинантног развоја људске мисли и проналазаштва. Са повећањем употребе рачунара, рачунарских мрежа, интернета и броја корисника, повећавају се и могућности за њихову злоупотребу.

Како би се у највећој могућој мери смањио ризик од злоупотребе, неопходно је уложити напоре у развијање јединствених стандарда за коришћење рачунара, рачунарских мрежа и интернета, као и у доношење одговарајућих међународних и националних правних стандарда који би инкриминисали понашања везана за њихову злоупотребу.

Савет Европе је 2001. године усвојио Конвенцију о високотехнолошком криминалу и Додатни протокол уз Конвенцију. Република Србија је 16.априла 2005. године у Хелсинкију потписала оба ова документа, а марта 2009.године Народна скупштина Републике Србије их је ратификовала. Ови документи су послужили као подлога за доношење одговарајућих националних правних прописа и стандарда и за формирање посебних државних органа специјализованих за борбу проив компјутерског криминалитета уопште. Али да ли су ипак неке теме остале правно нерегулисане и несанкционисане?

Могућност злоупотребе компјутера и компјутерских технологија у циљу кршења права на приватност

Компјутери и компјутерска технологија се могу злоупотребљавати на разне начине, криминалитет који се реализује коришћењем компјутера може имати облик било ког од традиционалних видова криминалитета, а подацима који се неовлашћено прибављају злупотребом информационих система може се на разне начине манипулисати.

Најчешћи појавни облици компјутерског криминалитета су: компјутерске крађе, компјутерске преваре, неовлашћено прибављање информација уз помоћ компјутера, неовлашћено прибављање или уништење информација садржаних у компјутеру, онемогућавање или отежавање приступа таквим информацијама (компјутерска саботажа), компјутерски тероризам.[2]

Приступ компјутерском систему било је могуће, у циљу борбе против свих видова компјутерског криминалитета, аутоматски контролисати коришћењем лозинки, давањем мањег или већег овлашћења корисницима и сл. Записивањем, односно бележењем свих улазака у систем и њиховом провером, било је могуће открити и санкционисати сваки или бар већину неовлашћених приступа.

Често се у оквиру компјутерског криминалитета у вези са друштвеним мрежама помиње **интернет насиље**. **Интернет насиље** (енгл. *"***cyber bullying"),**

2 Константиновић Вилић, С, Николић Ристановић В., Костић М.: Криминологија, Пеликан принт, Ниш, 2009., с.182,183.

се дефинише као свака комуникацијска активност рачунарском технологијом која се састоји у претњи, узнемиравању, омаловажавању, застрашивању или другом начину угрожавања и наношења штете појединцу[3].

Постоје различити облици ове врсте насиља:

- слање узнемиравајућих порука,
- крађа или неовлашћена промена лозинке или имена кориснику компјутера,
- објављивање приватних података или неистина о некоме,
- слање вируса и штетних програма (енгл.malware),
- слање увредљивих, порнографских или нежељених садржаја,
- лажно представљање и обмањивање жртве и сл.

Последице оваквих поступака извршилаца виртуелног интернет насиља понекад могу бити и озбиљније од последица ”реалног” насиља - жртва може сваки пут поново да прочита шта је насилник написао, коју је слику поставио, који су коментари написани. Жртва је јавно експонирана док насилник остаје анониман, што је један од разлога зашто се овакви извршиоци кривичних дела осећају моћни.

Глобалне друштвене мреже допринеле су даљем развијању компјутерског криминалитета, где се компјутерске мреже користе као циљ напада (нападају се сервиси, функције, садржаји који се налазе на мрежи), средство или алат (он лине продаја сексуалних услуга, људских органа, жена и деце за простуитуцију, производња и дистрибуција недозвољених штетних садржаја, као што су дечија порнографија, педофилија, верске секте, расистичке, нацистичке и сличне идеје), као и окружење у коме се напади реализују (коришћење мреже за прикривање криминалних радњи).[4]

Осим тога, у оквиру компјутерског криминалитета створен је нов, софистициран, неупадљив, технички образован профил извршиоца кривичног дела коме је тешко супротставити се због његове ”невидљивости” и ”неопипљивости”. Због изузетно великог броја корисника, доступности података, отворености у комуникацији али и недовољене законске регулисаности на националном и међународном плану, друштвене мреже представљају одлично скровиште за извршиоце ове врсте кривичних дела.

Друштвене мреже представљају погодно место за подстицање групне мржње, нападе на приватност, узнемиравање, праћење, вређање, несавестан приступ штетним садржајима, ширење насилних и увредљивих коментара, слање претећих и креирање тзв. ”фантомских” профила које садрже приче, цртежи, слике и шале на рачун жртве. Због отвореног приступа личним подацима корисника, често долази до велике злоупотребе коришћењем ових

3 http://kidshealth.org/parent/positive/talk/cyberbullying.html, приступ 10.9.2012.године

4 Константиновић Вилић, С, Николић Ристановић В., Костић М.: Криминологија, Пеликан принт, Ниш, 2009., с.184.

података. Нису ретки случајеви, да разни програмери или хакери, упадају у системе мрежа угрожавајући како кориснике тако и администраторе. Најчешће жртве су малолетници, па многи од сервиса имају заштиту за малолетнике која им донекле пружа сигурније коришћење сервиса.

Све су чешћи глобални напади на приватност, чији је циљ злоупотреба информација о појединцу. На основу тих информација, могуће је идентификовање појединца, његовог личног живота, групне припадности, свакодневног кретања и понашања - могућа је реконстукција живота и личности сваког субјекта података. Приватност на интернету укључује право на личне информације у вези са чувањем, употребом, обезбеђењем од трећих лица и приказивање личних информација преко интернета[5], као и идентификационе информације које се односе на посетиоца одређене интернет странице. Велики број експерата из области компјутерске безбедности и приватности верују да приватност не постоји: „Приватност је мртва – преболите то“ према мишљењу Стива Рамбама, приватног детектива у области интернет приватности[6].

Конвенција о високотехнолошком криминалу и њена имплементација у српско законодавство

Најсвеобухватнији покушај да се правно уобличи борба против високотехнолошког криминала на међународном нивоу свакако представља Конвенција Савета Европе о високотехнолошком криминалу из 2001. године. Конвенција је осмишљена у циљу спречавања дела која су усмерена против интегритета, поверљивости и доступности компјутерских система, мрежа и података, а самим тим и спречавања злоупотребе тих система, мрежа и података. Циљ је било и увођење казненог система мера ради ефикасније борбе против извршилаца ових кривичних дела, чиме би се на националном и међународном нивоу олакшало откривање, истрага и гоњење за извршена кривична дела и обезбедили услови за брзу и поуздану међународну сарадњу.

Она садржи, између осталог, материјалне и процесне кривичноправне одредбе, чијом би имплементацијом у национална законодавства држава потписница требало да се постигне висок степен хармонизације различитих законодавстава и да се убрза и квалитативно унапреди међународна сарадња на плану борбе против сајберкриминала.

Чињеница да су Конвенцију потписале и поједине земље које нису чланице Савета Европе, указује на то колики је значај овог правног акта и колика су очекивања да се направи крупан искорак у сузбијању ове врсте криминалитета.

---

5 http://sr.wikipedia.org/wiki/, приступ 8.8.2012.године

6 «Стив Рамбам - Приватност је мртва – преболите то», Google video, http://www.documentary24.com/privacy-is-dead-get-over-it--317/, приступ 8.8.2012.године

Конвенција садржи четири поглавља која се односе на значење и употребу основних термина, на мере које је потребно предузети на националном нивоу у оквиру процесног и материјалног законодавства, одредбе о стандардима међународне сарадње у оквиру узајамне помоћи у борби против компјутерског криминалитета и завршне одредбе потписавања и ступања на снагу (приступање, територијална примена, изјаве, резерве, решавање спорова, отказ, итд.).

Конвенција је препознала као кривична дела, уредила и санкционисала следећих девет облика високотехнолошког криминалитета које треба прилагодити националном нивоу и које су сврстане у 4 групе:

I) Кривична дела против поверљивости, интегритета и доступности компјутерских података и система:

- недозвољен приступ (члан 2),
- недозвољено пресретање података (члан 3),
- ометање података - мењање садржаја, брисање или оштећење (члан 4),
- ометања нормалног рада рачунара или рачунарског система (члан 5),
- злоупотреба уређаја - производња, продаја, дистрибуције или употреба уређаја пројектованих у сврху почињења неког од претходно наведених кривичних дела (члан 6);

II) Кривична дела у вези са компјутерима:

- фалсификовање које је у вези са компјутерима (члан 7),
- преваре које је у вези са компјутерима (члан 8);

III) Кривична дела у односу на садржај (члан 9) и

IV) Кривична дела која се односе на кршење ауторских и њима сличних права (члан 10).

Конвенција је написана технички неутралним језиком тако да се њене одредбе могу применити и на тренутно постојећу и на будућу технологију. Сви преступи, по Конвенцији, морају да буду учињени *намерно и умишљајно*, али су сами појмови "намере" и "умишљаја" остављени на тумачење националним законодавствима. Такође, сам преступ компјутеру или компјутерском систему мора бити учињен *бесправно,* тј. да по домаћем праву за њега не постоји оправдање.

Законодавство Републике Србије је у периоду од априла 2005. до марта 2009. године усвојило више прописа којима је извршено усклађивање одредби Конвенције у наш правни систем. Најважнији донети прописи који су прилагођени одредбама Конвенције су: Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[7], Кривични законик[8], Закон о одговорности правних лица за кривична дела[9], Законик о кривичном

7 „Службени гласник РС" бр.61/2005 од 18.5.2005.године

8 „Службени гласник РС" бр.85/2005, 88/2005, 107/2005, 72/2009 и 111/2009

9 „Службени гласник РС" бр.97/2008

поступку[10], Закон о полицији[11], Закон о електронском потпису[12], Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине[13] и Правилник о условима за пружање интернет услуга и осталих услуга преноса података и садржају одобрења[14].

Велики је помак постигнут регулисањем кривичноправне заштите од компјутерског криминалитета пу националном законодавству предвиђањем кривичних дела против безбедности рачунарских података (Глава ХХВИИ КЗ РС): оштећење рачунарских података и програма (чл.298), рачунарска саботажа (чл.299), прављење и уношење рачунарских вируса (чл.300), рачунарска превара (чл.301), неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302), спречавање и ограничавање приступа јавној рачунарској мрежи (чл.303).

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала уређено је образовање, организација, надлежност и овлашћење посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења у случајевима извршења кривичних дела против безбедности рачунарских података одређена Кривичним закоником и кривичних дела против интелектуалне својине, имовине и правног саобраћаја 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, ако број примерака ауторских дела прелази 500 или настала материјална штета прелази изнс од 850.000 динара. Закон предвиђа постојање посебног тужилаштва и службе за борбу против високотехнолошког криминала.

Конвенција о високотехнолошком криминалу и заштита права на приватност

У вези са компјутерским злоупотребама поставило се питање заштите појединачног личног права - права на приватност. Запажено је да од свих савремених техничких средстава помоћу којих је могуће сазнати приватни живот појединца и контролисати га, компјутер и компјутерска техника спадају у најсавршенија и најмоћнија. Компјутер је у стању да сакупи, прими, обради, међусобно повеже велики број података везаних за појединца, да их чува на дужи рок и на веома малом простору. Компјутерској злоупотреби приватности нарочито су изложене одређене групе људи о којима је прикупљен већи број

10 „Службени гласник РС” бр.72/2011

11 „Службени гласник РС” бр.101/2005 и 92/2011

12 „Службени гласник РС” бр.135/2004

13 „Службени гласник РС” бр.46/2006

14 „Службени гласник РС” бр.100/2008, који је престао да важи 8.6.2001.године

података, то су на пример они који се најчешће користе одређеним друштвеним услугама и чије је понашање девијантно или криминално.

Конвенција не регулише посебно питање права на приватност и заштите података о личности у виртуелном простору или компјутерским комуникацијама. Индиректно, Конвенција то чини санкционишући недозвољени приступ рачунарским подацима, њихиово фалсификовање и преварно понашање, као и кривична дела везана за дечију порнографију која се могу сматрати повредом права на приватност. Ипак, целокупна регулатива је везана за техничка, а не суштинска питања заштите од оваквих криминалних понашања.

Интернет корисници могу да заштите своју приватност преко контролисаног откривања личних информација. Они корисници који желе више да заштите своју приватност могу да покушају да постигну интернет анонимност – на тај начин је могуће коришћење интернета без давања могућности трећем лицу да се повеже са интернет активностима за личну идентификацију интернет корисника.

Савремене државе су се нашле пред проблемом како да успоставе равнотежу између права појединца на приватност и права јавности да буде информисана, два права која иако делују супротно чине делове истог темеља модерног демократског друштва у оквиру кога држава има право да у циљу своје заштите ограничава право приватности појединца.

Заштита података, по дефиницији коју даје Џозеф Катаначи (Joseph Cannataci)[15], значи заштиту појединца од злоупотребе или неадекватне употребе личних података од стране неког лица, приватне организације или државе. У вези са заштитом приватности података поставља се низ питања функционалног, организационог и безбедносног карактера, као што су: ограничавање располагања одређеним врстама података, обавеза давања информација државним органима од стране недржавних субјеката, обавештавање грађана о њиховим подацима, технички стандарди система, стручност лица која обрађују податке, мере обезбеђења хардвера, софтвера, и сл.

Најчешће злоупотребе и повреде приватности коришћењем података који се налазе на друштвеној мрежи су крађа идентитета, прогањање и узнемиравање, манипулација личним подацима који се односе на запошљавање, злоупотреба фотографија на интернету и др.

Крађа идентитета као део компјутерског криминалитета састоји се у неовлашћеном коришћењу личних података (датум рођења, тренутно пребивалиште, број телефона, занимање, пријатељи, личне слике) који су постали јавно доступни.[16] Крађа идентитета на Интернету представља облик преваре

15 Cannataci, Joseph A.: Privacy and Data Protection Law: International Development and Maltese Perspectives, Complex, 1987.

16 Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case). strana 8, http://www.heinz.cmu.edu/~acquisti/papers/

којом се од корисника рачунара путем лажне поруке електронске поште или веб-сајта сазнају лични и финансијски подаци. Извршиоци кривичног дела могу да постигну свој циљ на неколико начина, нпр. коришћењем друштвених мрежа како би се са туђег рачунара прикупиле лозинке, корисничка имена и бројеви кредитних картица које корисник користи на рачунару.

Прогањање и узнемиравање коришћењем интернета дефинише се као упорно и циљано злостављање појединца путем електронских начина комуникације.[17] Овакво понашање може да буде само „виртуелно" и ограничено само на компјутерски комуникациони простор, али се може пренети из „виртуелног" у „стварни" свет и тада представљати увод у најопасније облике виктимизације. Слично правим прогонитељима, интернет прогонитељи покушавају да надгледају активности своје жртве, да пронађу што више података о њој, да контактирају особе са којима је жртва блиска, да на незаконит начин читају пошту своје жртве и да прате њене активности. Жртва постаје несигурна, уплашена, застрашена и не сагледава начин на који може да утиче на престанак узнемиравања и прогањања. Узнемиравање посредством интернет мреже може да се састоји и од слања претњи и порука које имају за циљ да узнемире или повреде особу којој су послате.

Злоупотреба фотографија на интернету представља такав облик повреде приватности када се неовлашћено користе и приказују фотографије са налога корисника без сагласности. Већина корисника компјутерских система има дигиталне камере и своје фотографије поставља на сопствене корисничке налоге, ризикујући да те фоторграфије постану предмет злоупотребе.[18]. Фотографија било које особе може бити приказана на начин који јој можда може шкодити на неком личном плану, а временом друштвена мрежа може преузети фотографију тако да велики број корисника има шансу да ту фотографију види, подели са неким или проследи.

Проблем постоји јер Конвенција, као ни национални закони, не регулише ниједно од наведених криминалних понашања. Крађа идентитета се може посматрати у оквиру криминалитета рачунарских превара, прогањање и узмениравање се може сагледавати само као слично кривично дело у реалном а не виртуелом времену, док злоупотреба фотографија може бити кажњива само уколико се ради о дистрибуцији дечије порнографије. Већина кривичних закона не штити особе чије су фотографије направљене у јавности јер се сматра да сама радња сликања не спада у угрожавање приватности.

---

privacy-facebook-gross-acquisti.pdf, приступ 4.8.2012.године

17 Yar, M.: Cybercrime and society, SAGE Publications, Lonodon, 2006.,s.122.

18 "In the Face of Danger: Facial Recognition and the Limits of Privacy Law ", Harvard Law Review, 2007., http://hlr.rubystudio.com/media/pdf/facial_recognition_privacy_law.pdf, приступ 12.8.2012.године

Могућности за превенцију злоупотребе права на приватност

Да би се смањио број злоупотреба компјутерских система и угрожавање права на приватност њихових корисника, неопходно је створити одговарајуће законске механизме и правну регулативу за откривање и санкционисање ових друштвено неприхватљивих криминалних понашања. Такође, веома је важно да се надлежним органима пријављују кривична дела компјутерског криминалитета како би се смањила „тамна бројка криминалитета" и остварило боље превентивно деловање, препознавање и праћење оваквих дела као и превазилажење проблема непријављивања ових кривичних дела.

Успешно остваривање превенције злоупотребе друштвених мрежа је изузетно значајно јер овај облик криминалитета производи тешке и често неотклоњиве последице. Детаљно законско регулисање, откривање и санкционисање свих облика злоупотреба компјутера и комојутерских система уз повећану пажњу, стално праћење и контролу од стране администратора и корисника само су најзначајнији фактори превентивног деловања. Свакодневни развој интернета захтева велику пажњу и умешност у откривању компјутерског криминалитета. Због тога је неопходно добро компјутерско образовање корисника како би на време уочили злоупотребу путем интернета, препознали и на време пријавили сваки облик он лине напада на приватност и тиме утицали на смањење велике „тамне бројке" компјутерског криминалитета.

Међународна и национална правна регулатива којима се забрањује компјутерски криминалитет треба да буду веома флексибилни и да прате свакодневни развој компјутерске технологије и иновација. Само развијањем компатибилних стандарда и правних прописа овакве иновације могу да се развијају уз смањење ризика од њихове злоупотребе. Начин на који успемо да обликујемо правне стандарде и законе везане за ову врсту криминалитета имаће утицаја на животе милиона људи. Компјутери постају технолошки све моћнији, а човечанство све зависније од њихове примене, што отвара велико поље за њихову злоупотребу и за вршење кривичних дела.

Литература

«In the Face of Danger: Facial Recognition and the Limits of Privacy Law «, Harvard Law Review, 2007.,

http://hlr.rubystudio.com/media/pdf/facial_recognition_privacy_law.pdf,

"Стив Рамбам - Приватност је мртва – преболите то", Google video, http://www.documentary24.com/privacy-is-dead-get-over-it--317/,

Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case). http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf,

Константиновић Вилић, С, Николић Ристановић В., Костић М.: Криминологија, Пеликан принт, Ниш, 2009., с.182,183.

http://kidshealth.org/parent/positive/talk/cyberbullying.html,

http://sr.wikipedia.org/wiki/,

Cannataci, Joseph A.: Privacy and Data Protection Law: International Development and Maltese Perspectives, Complex, 1987.

Council of Europe – Convention on Cybercrime, Budapest 23.11.2001., ETS No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm,

Yar, M.: Cybercrime and society, SAGE Publications, Lonodon, 2006.,

Резиме

Проналазак и развој компјутера представља резултат фасцинантног развоја људске мисли и проналазаштва. Са повећањем употребе рачунара, рачунарских мрежа, интернета и броја корисника, повећавају се и могућности за њихову злоупотребу.

Смањење ризика од злоупотребе могуће је једино развијањем јединствених стандарда за коришћење рачунара, рачунарских мрежа и интернета, као и доношењем и применом одговарајућих правних стандарда којима се инкриминишу понашања везана за њихову злоупотребу. У вези са компјутерским злоупотребама поставило се питање заштите појединачног личног права - права на приватност. Компјутерској злоупотреби приватности нарочито су изложене одређене групе људи о којима је прикупљен већи број података, то су на пример они који се најчешће користе одређеним друштвеним услугама и чије је понашање девијантно или криминално.

Међународна и национална правна регулатива којима се забрањује компјутерски криминалитет треба да буду веома флексибилни и да прате свакодневни развој компјутерске технологије и иновација. Потписивањем, ратификацијом и имплементацијом у српско законодавство Конвенције Савета Европе о високотехнолошком криминалитету постигнуто је доста тога, али је остао нерешен проблем заштите права на приватност, које овом Конвенцијом није обухваћено.

Само развијањем компатибилних стандарда и правних прописа овакве иновације могу да се развијају уз смањење ризика од њихове злоупотребе. Начин на који успемо да обликујемо правне стандарде и законе везане за ову врсту криминалитета имаће утицаја на животе милиона људи. Компјутери постају технолошки све моћнији, а човечанство све зависније од њихове примене, што отвара велико поље за њихову злоупотребу и за вршење кривичних дела.

Кључне речи: компјутерски криминалитет, злоупотреба, право на приватност, међународна и национална правна регулатива, Савет Европе

***Prof. dr Miomira Kostić**, Full Professor, Faculty of Law, Nis*
***Vida Vilić**, PhD Student, Faculty of Law, Nis*

Measures for protection the right to privacy according to Council of Europe Convention on cybercrime

Summary

The invention and development of a computer is the result of a fascinating development of human thought and invention. With the increasing use of computers, computer networks and the number of Internet users, increase the possibility for misuse.

Reducing the risk of misuse is possible only by the development of uniform standards for the use of computers, computer networks and the Internet, as well as the ratification and implementation of the proper legal standards to criminalize such conduct. Regarding computer misuse, what happened with the right to privacy? Computer misuse policy in particular should be adressing to certain group of people who gathered more data, use certain social services, and whose behavior is deviant or criminal.

International and national legal regulations that prohibit cyber crime need to be very flexible and to follow the daily development of computer technology and innovation. By signing, ratifying and implementing Council of Europe Convention on Cyber Crime in Serbian legislation we have achieved a lot, but one issue remain unresolved - the issue of the right to privacy, which is not covered by this Convention.

Only the development of compatible standards and regulations such innovations can be developed with reduced risk of misuse. The way we shape the legal standards and laws regarding this type of crime will impact the lives of millions of people. Computers are becoming more and more technological powerful, humanity becomes more dependent, which makes an open field for their abuse and criminal activity.

***Key words**: computer crime, misuse, right to privacy, international and national legislation, the Council of Europe*