ЖЕЉКО Ђ. БЈЕЛАЈАЦ[*]
МИЛОВАН Б. ЈОВАНОВИЋ[**]
Правни факултет за привреду и правосуђе
Нови Сад

УДК 351.78:004.49
Прегледни рад
Примљен: 17.03.2013
Одобрен: 27.04.2013

ПОЈЕДИНИ АСПЕКТИ БЕЗБЕДНОСНЕ КУЛТУРЕ НА ИНТЕРНЕТУ

Сажетак: Безбедносна култура се уопштено речено огледа у идентификовању опасности, њиховом отклањању или пак упућивању на оне субјекте задужене да професионално реагују и сачувају угрожене вредности. При том, вредности се једноставно могу дефинисати, као наша веровања о томе шта је добро или лоше, односно у којој мери је нешто добро или лоше, допустиво или недопустиво, корисно или некорисно, пожељно или непожељно, па самим тим рефлектују моралну димензију. Моралне норме које су некада важиле, са експанзијом информационо - комуникационих технологија, те свеопштом употребом рачунара и Интернета као глобалне мреже, почињу да трпе драстичне промене. Наиме, Интернет је наметнуо глобалну промену у брзини и начину комуникација, уневши важан утицај на квалитет живота „обичног човека“. Тај утицај видљив је у свим сферама друштвеног живота. Позитивне и корисне новине савремених информационих и компјутерских технологија, истовремено су као нус појаву донеле различите видове злоупотреба и опасности, нарочито приликом неконтролисане и бесциљне употребе Интернета. Између осталог, најчешћа асоцијација која се односи на злоупотребу Интернета у вези је са порнографијом. Подразумева се да и остали сајтови са нелегалним садржајима врше утицај на дугорочно „тровање“ деце. Поред незаобилазне и примарне улоге родитеља, неопходна је и подршка свих сегмената друштва у циљу подизања колективног нивоа свести, кроз медијске и едукативне кампање, усмерене према деци и младима, ради информисања о могућностима заштите на Интернету и начинима примене општих образаца његовог безбедног коришћења, у циљу заштите интегритета, посебно малолетних лица.

Кључне речи: интернет, безбедносна култура, злоупотребе интернета, компјутерски криминал, интернет педофилија

---

[*] zeljkobjelajac067@gmail.com
[**] miki80miki@gmail.com

Увод

Крајем XX века, Интернет је наметнуо глобалну промену у начину и брзини комуникација. Са сигурношћу се може истаћи, да је за две деценије постојања, дакле у прилично кратком временском периоду, интернет унео драстичан утицај на квалитет, живота „обичног човека". Сви смо свесни огромног значаја употребе компјутера у савременим друштвима и чињенице да нема области људске делатности у којој рачунари нису нашли своју примену. Захваљујући огромној моћи компјутера у меморисању и брзој обради великог броја података, аутоматизовани информациони системи постају све бројнији и готово незаменљиви део целокупног друштвеног живота свих субјеката (физичких, али и правних лица) на свим нивоима.

Изузимајући уобичајену и неизбежну употребу у оквиру пословних комуникација, савремени човек данас користи Интернет и као средство за завршавање свакодневних обавеза. Захваљујући широком опсегу могућности помоћу Интернета можете на пример, резервисати карте за авион, позориште, куповати и продавати разну робу, вршити услуге, гледати ТВ, подешавати клима уређај, комуницирати и обављати многе друге послове које диктира животни и радни темпо модерног човека. Стога не чуди преовлађујуће мишљење, да је на планетарном нивоу зависност од Интернета из дана у дан све већа и већа.

У почетку примене компјутерске технологије, компјутери нису били подобни за веће злоупотребе, јер њихова примена није била масовна, тако да се њима бавио само узак круг корисника – информатичких стручњака. Оно што је отворило врата ширењу могућности да се компјутерска технологија злоупотреби у различите сврхе, јесте њен брз развој, поједностављење њене употребе, као и доступност исте широком кругу корисника.

Друштвена умрежавања су вероватно најбрже растућа онлајн (*online*) активност међу младима.[1] Одговор на све израженију преокупацију младих друштвеним интернетским мрежама (Фејсбук-*Facebook*, Твитер-*Twitter*, четовање-*Chat*) траже социолози, психолози, педагози и разни други стручњаци. Њихова запажања доносе прилично помешана осећа-

[1] Sonia Livingstone, Leslie Haddon, Anke Görzig and Kjartan Ólafsson, „Risks and safety on the internet: The perspective of European children", Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. This report, based on the final dataset for all 25 countries, presents the final full findings for EU Kids Online Deliverable D4: Core findings to the European Commission Safer Internet Programme, 13. January 2011, p. 36.

ња. С једне стране, евидентно је да нове технологије људима доносе значајне погодности и бројне изазове на које се може и мора одговорити креативном интелигенцијом, с друге стране Интернет са собом носи бројне изазове и опасности, којима су нарочито изложени млади људи. Наиме, велики проценат младих људи опијен Интернетом успоставља такве облике комуникација које не доприносе унапређењу хуманости него повећању осећања дезоријентације и самоће, што доводи напослетку до равнодушности према стварном животу. У том контексту, због нових технологија и бољитка које оне доносе, постоји оправдана неизвесност и страх од конфликта у коме се могу наћи подложни појединци, где би могло постати немогуће разликовати истину од заблуде, односно могло би доћи до мешања стварног света и виртуелне стварности.

Развој телекомуникација и рачунарства трансформисао је мобилне уређаје у минијатурне умрежене рачунаре са великим потенцијалом за криминал.[2] Компјутери и компјутерска технологија отварају простор за реализацију специфичних манипулативних дела, почевши од неких традиционалних облика криминалитета, као што су проневере, утаје, крађе, до оних софистицираних којима се неовлашћено прибављају одређени подаци, а потом употребљавају за остваривање противправне користи, а у последње време нарочито су учестале расправе о интернет педофилији.

Интернет педофилија јесте посебно специфичан вид компјутерског криминалитета, јер педофили све више лутају електронским мрежама и траже жртве, које су нажалост деца, најосетљивији и најрањивији део људске популације. Стога се са правом у последње време дискутује о распрострањености педофилије на интернету, укључивши и то, да ли таква дела улазе у категорију организованог криминала, јер се по правилу ретко завршавају на појединачним случајевима. Интернет је заправо постао ново „игралиште“ доступније педофилима, где су деца перманентно изложена непримереним сексуалним садржајима и узнемиравајућим и непријатељским порукама, што разорно утиче на њихов телесни и ментални склоп, односно психо-физички развој, што може бити опредељујуће за њихов будући биопсихолошки статус.

Имајући у виду наведено, све више се потенцира афирмисање безбедносне културе на интернету, васпитавање младих и промовисање вредности и вредносних система, како од стране родитеља, тако и од целокупног друштва.

---

[2] Jonathan Clough, „Principles of Cybercrime“, *Cambridge University Press*, Cambridge, 2010, pp. 3-4.

Безбедносна култура

Под безбедносном културом може се подразумевати безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности. Према мишљењу Љубомира Стајића, безбедносна култура представља скуп усвојених ставова, знања, вештина и правила из области безбедности, испољених као понашање и процес, о потреби, начинима и средствима заштите личних, друштвених и међународних вредности од свих извора, облика и носилаца угрожавања, без обзира на место или време њиховог испољавања. Безбедносна култура има своје унутрашње и спољашње манифестације. Унутрашње се односе на промишљање безбедности, а спољашње на понашање у безбедности, као и на однос и приступ безбедности, под чим се пре свега мисли на спремност и способност да се, било материјално било духовно, одговори на изазове и претње.[3] Безбедносна култура је у тесној вези са нашим васпитањем, вредностима и вредносним системима које подржавамо.

Васпитање је трајан процес усвајања и усавршавања сензомоторних, интелектуалних, емоционалних, моралних и духовних способности детета, али и одраслог човека. Васпитање представља облик социјализације, што значи да се васпитањем детета или одраслог човека уобличава понашање тако да буде прихватљиво у друштвеној средини. Васпитање може бити физичко (учење и усавршавање сензомоторних особина и покрета тела, спортско васпитање), интелектуално (стицање знања из области науке, уметности, књижевности итд.), морално (стицање знања о томе шта је добро, а шта је лоше), естетско (стицање знања о томе шта је лепо, а шта није), религијско (стицање знања о вери, Богу, верским обичајима и традицији), безбедносно (стицање знања о безбедном понашању, заштити од претњи и угрожавања, избегавању и решавању сукоба итд.).[4] С друге стране, вредности представљају наше идеје о томе шта је добро и исправно. Управо због тога вредности садрже моралну димензију. Људи имају различите вредности, јер су одрасли у различитим околностима, што одражава њихов субјективни карактер.

---

[3] Светлана Станаревић, Филип Ејдус и остали, „Појмовник безбедносне културе“, *Центар за цивилно-војне односе*, Београд, 2009, стр. 16.
[4] Ибид, стр. 20.

У информационој безбедности, безбедносна култура је релативно нова област. Могло би се рећи, да су тек почетком овог века безбедносни истраживачи, почели да промовишу безбедносну културу неке организације као важан фактор у одржавању адекватног нивоа безбедности информационих система у истој. Међутим, нико од тих раних истраживача, није понудио прецизну дефиницију, која суштински и садржајно одражава појам „безбедносна култура“, нити је било икаквих јасних погледа о томе како је креирати. Надаље, већина радова о безбедносној култури и даље има ограничен фокус о томе како можете развити безбедносну културу. Успут, постоји широко уверење да је све што је потребно, мало свести и тренинга да се створи добра безбедносна култура. Већина веб сајтова о безбедносној култури промовише и заступа овакво мишљење. Међутим, да баш тако није једноставно установити и спроводити безбедносно прихватљив образац понашања, предочавају бројне расправе о индивидуалној безбедносној култури и уопште безбедносној култури младих на интернету.

Очито је да постоји више димензија безбедносне културе које је тешко ускладити, зато је све израженије угрожавање приватности и репутација, пљачкање новца на банкарским рачунима, чак и угрожавање личне и породичне безбедности услед неопрезног понашања на Интернету.

Негативне стране интернета

Рачунари су нашли своју примену у скоро свим областима живота и рада савременог човека. Захваљујући огромној моћи компјутера у меморисању и брзој обради великог броја података, аутоматизовани информациони системи постају све бројнији и готово незаменљиви део целокупног друштвеног живота свих субјеката (физичких, али и правних лица) на свим нивоима.

Напредак у телекомуникационој и рачунарској технологији покренуо је информациону револуцију, чији утицај може бити бар толико широк и дубок колики је био и утицај индустријске револуције XIX века. Трансформација из индустријског у информационо (пост - индустријско) друштво, која је започела средином прошлог века и још увек траје, померила је друштвени фокус од производње материјалних добара ка пружању услуга. Кључни симболи овог доба су комуникације и рачунари, са отвореним питањем: Ко ће у овом новом добу бити најуспешнији?[5]

[5] William G. Huitt, „Success in the Information Age: A Paradigm Shift“, Valdosta State University, Valdosta, Georgia, 1999, http://chiron.valdosta.edu/whuitt/13/02/2013.

Међутим, управо појачано присуство информационих технологија носи са собом и ризик.[6] Промене које је изазвала информациона технологија учиниле су да у први план дођу нови стратешки ресурси савременог друштва: знање и информација, као примарна основица стварања нових вредности информатичког доба у којем је подржавајућа технологија веома снажан алат приликом усмеравања рада од физичког ка менталном. Велике могућности у свим сферама друштвеног живота, које су развојем информационе технологије стављене пред човека, поред бројних, њему до тада непознатих предности, условиле су и његову изложеност новим и врло озбиљним ризицима.

Поред ових општих особености и запажања која одликују знатне контрадикторности, негативне стране употребе интернета попримају озбиљне конотације. Наиме, научно-технолошки развитак, упоредо са тим што је покренуо снаге које интегришу нашу планету, у циљу квалитетнијег живота њених становника, омогућио је претпоставке онима који желе да искористе одређене иновације у сврху вршења криминалних делатности. Позитивне и корисне новине савремених информационих и компјутерских технологија, донеле су и низ проблема везаних за појаву и експанзију различитих облика и форми испољавања компјутерског криминалитета. Нове форме вредности, концентрација података, нове методе и технике деловања у другачијем амбијенту, те сужавање временске скале деловања, укидање лимита на просторна ограничења деловања, уз динамичност, покретљивост, инвентивност и стабилност ризика, јесу одреднице у које се уклапају и којима се руководе појединци и криминалне организације склоне различитим видовима злоупотреба.[7]

Иако је данас немогућ живот и функционисање друштва у целини без употребе рачунара и савремене информатичке технологије, сазрела је свест да се ова корисна и потребна средства могу користити за недопуштене, противправне циљеве, у првом реду за прибављање противправне имовинске користи за неко лице или за наношење штете другима.8 Компјутерске преваре могу да се врше на веома разноврсне начине

[6] Саша Радуловић, „Претње високотехнолошког криминала и домаћа законодавна регулатива“, *Ревија за безбедност – стручни часопис о корупцији и организованом криминалу, бр. 8/08, година II*, Центар за безбедносне студије, Београд, 2008, стр. 18.

[7] Жељко Бјелајац, *Организовани криминалитет-Империја зла*, Правни факултет за привреду и правосуђе у Новом Саду, Нови Сад, 2013, стр. 282-283.

[8] Жељко Бјелајац, Јелена Матијашевић, Душко Димитријевић, „Значај успостављања међународних стандарда у сузбијању високотехнолошког криминала”, *Међународна политика, бр 1146*, Април–Јун 2012, Београд, стр. 66–85.

и компјутерски делинквенти у том погледу показују заиста велику инвентивност.[9]

Оно што је посебна карактеристика ових деликата јесте сам начин извршења, који се заснива на употреби компјутера. При том коришћење рачунара може бити испољено на целовит или сегментиран начин у инкриминисаним радњама. Наравно, компјутер може бити, а врло често и јесте основно средство за извршење ових кривичних дела, уз услов да је остварена нека кажњива последица у кривично-правном смислу. Могућности злоупотреба су бројне и разноврсне.

Злонамерни појединци, организоване хакерске групе, па и сајбер криминалци, могу да нанесу штету на следеће начине:[10]

- да заразе ваш рачунар шпијунским софтвером како би вам украли идентитет или пратили ваше Интернет и животне навике;
- да вас опљачкају крађом ваших лозинки за приступ неким онлајн сервисима (нпр: е-банкинг);
- да направе проблеме у функционисању вашег рачунара помоћу вируса и другог злонамерног софтвера
- да преузму контролу над вашим рачунаром и да га користе за напад на друге кориснике широм света;
- да вас наведу да посетите лажни сајт неког од онлајн сервиса које користите и тамо оставите личне податке;
- да упадну у вашу бежичну мрежу и бесплатно користе вашу Интернет конекцију
- да украду и потом користе ваше налоге за слање е-поште и четовање.

Дакле, појавни облици компјутерског криминалитета могу бити многобројни, али углавном се могу груписати на четири облика, а то су: крађа услуга; информацијски криминалитет; имовински и неимовински криминалитет. Област компјутерског криминалитета, односно различите видове злоупотреба и недозвољених радњи, теорија кривичног права прати, обрађује и разврстава, као дела која се односе на: компјутерске преваре, крађе добара, фалсификовање података и докумената, финансијске крађе, преваре и злоупотребе, хакерисање, крађе времена, вандализам, компјутерске шпијунаже и саботаже.

---

[9] В. више: Bellour J. C.: „Међународна превара“, *Избор бр.1*, Загреб, 1981, стр. 76-77; цитирано према: Живојин Алексић и Милан Шкулић, *Криминалистика*, Досије, Београд, 2002, оп. цит., стр. 389.

[10] http://www.rnids.rs/cir/15/02/2013.

ФБИ и Национални центар за криминал белих крагни САД (*National White Collar Crime Center*) по Енциклопедији сајбер криминала, истражују и прате следеће облике:[11]

- упаде у компјутерске мреже;
- индустријску шпијунажу;
- софтверску пиратерију;
- дечију порнографију;
- бомбардовање електонском поштом;
- „њушкање“ пасворда;
- крађу кредитних картица;
- прерушавање рачунара да личи на други.

У односу на тип почињених дела, сајбер криминал може бити:

Политички, кога чине:

а) сајбер шпијунажа и сајбер саботажа у свету рачунара,

б) хакинг – основе безбедности на интернету, заштита од компјутерских вируса, црва и тројанаца,

ц) сајбер тероризам – интернет као оружје терориста,

д) сајбер ратовање – импликације евентуалног оружаног сукоба на сајбер простору.

Економски, кога чине:

а) сајбер преваре – нигеријска подвала или прање новца,

б) хакинг – заштита од компјутерских вируса,

ц) крађа интернет услуга и времена – сузбијање злоупотребе интернета и наношење штете корисницима,

д) пиратерство софтвера, микрочипова и база података,

е) сајбер индустријска шпијунажа – шпијунажа и саботажа у свету рачунара,

ф) преварне интернет аукције – неиспоручивање производа, лажна презентација производа, надграђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта...

Производња и дистрибуција недозвољених и штетних садржаја:

а) дечија порнографија,

б) педофилија,

ц) верске секте,

д) ширење нацистичких, расистичких идеја,

е) злоупотреба жена и деце.

[11] Željko Bjelajac, „Cyber Crime and Internet Pedophilia“, *Western Balkans From Stabilization to Integration,* Institute of International Politics and Economics, Belgrade, 2011, pp. 437–456.

Манипулација забрањеним производима, супстанцама и робама:
а) дрогом,
б) органима,
ц) оружјем.
Повреде сајбер приватности:
а) надгледање е-поште,
б) спам – злоупотреба електронских система у сврху слања нежељених масовних порука без икаквог критеријума,
с) *phishing* мрежна крађа идентитета,
д) праћење е-конференција,
е) прислушкивање, снимање „причаоница",
ф) прикачињање и анализа *„cookies"*.

Дела из области високотехнолошког криминала изузетно је тешко перципирати, истраживати и процесуирати.[12] Сајбер криминалци, за разлику од других криминалаца, користе веома паметне технике, којима се припремају и врше кривична дела, па им је веома тешко ући у траг. Откривање ове врсте кривичних дела и прикупљање доказа против починилаца је доста специфично. Наиме, због недостатка материјалних доказа, као што су леш, крв, новац, накит, отисак и сл., тешко је усмеравати и водити истрагу. Већина кривичних дела из области сајбер криминала, бива откривено случајно или дуго након њиховог настанка, али ипак број откривен кривичних дела није занемарљив.

Такође, тежина компјутерских превара је утолико већа што оне далеко допиру због величине Интернета, затим, прилично се тешко откривају и доказују, а због мале упадљивости, врло често се ова дела врше веома дуго и у континуитету.[13]

Сајбер простор у Србији, прати тренд експанзије сајбер криминала на глобалном нивоу. У Србији је присутна широка лепеза сајбер криминала, од ширења вируса, пиратерије, неовлашћеног приступа рачунарским мрежама, до порнографија, злоупотребе платних картица и пљачки банака. У области сузбијања високотехнолошког криминала у Србији, највећи помак је учињен оснивањем специјализованих органа и ангажовањем посебно обучених стручњака. У оквиру МУП-а Србије формирана је посебна служба за борбу против високотехнолошког кри-

[12] Жељко Бјелајац, Јелена Матијашевић, Душко Димитријевић, „Конвенција Савета Европе о високотехнолошком криминалу", *Европско законодавство*, Год. XI, бр. 42, Београд, 2012, стр. 37–52.
[13] Жељко Бјелајац, Јелена Матијашевић, Душко Димитријевић, „Computer fraud as a part of contemporary security challenges", *Review of International Affairs 1147*, avgust-septembar 2012, str. 5-21.

минала. Такође, именован је посебан тужилац за високотехнолошки криминал и опредељена је надлежност суда за целу територију Републике Србије.

Интернет педофилија

Раније су педофили имали „сужен“ маневарски простор деловања. Одлазили су на дечија игралишта, школска дворишта и имали су уобичајене методе рада које су се састојале у посматрању, праћењу, запиткивању, чашћавању чоколадицама, жвакама, слаткишима и сл. Такав начин и приступ подразумевао је и излагање својеврсном ризику. Интернет сада обезбеђује педофилима несметано и безбрижно праћење деце, укључивање у њихове активности, игру и забаву. Такође он пружа и излаз, односно могућност бежања у анонимност када се год осети опасност од разоткривања.

Анализирајући ову појаву, тешко да би се било ко повиновао мишљењу да рачунари и интернет заправо представљају мрачну страну света. Међутим, сви би се сложили са чињеницом да бесциљна и неконтролисана употреба интернета за собом повлачи бројне опасности. „Данас интернет користи око 15% светске популације (свесно), а несвесно чак око 20% (кроз разне уређаје, телефоне, телевизију). Од тога броја половина је у узрасту од 5 година до адолесценције. Груба претрага популарног google-a на реч „енциклопедија“ ће вам понудити 1.700.000 резултата, док ће на реч „секс“ понудити 26.500.000 резултата“.14 Изнети подаци алармантни су за друштво у целини, а превасходно за родитеље, који нажалост немају јасну представу о импликацијама овог феномена, нису свесни проблема и не препознају га на адекватан начин.

Остоле специфичности електронског насиља које га разликују од насиља у непосредном односу: може бити присутно 24 часа, свих седам дана у недељи; изложеност и код куће и на местима која су раније била сигурна за дете; публика и сведоци могу бити многобројни и брзо се повећавају; анонимност повећава осећај несигурности код жртве; електронско злостављање може бити присутно међу вршњацима, али мете могу бити и одрасли, као на пример професори и учитељи; без физичког контакта са жртвом и публиком, деца и млади теже виде и разумеју штету коју њихове речи могу нанети, понекад и поруке које се шаљу из шале могу повредити, премда нису имале намеру злостављати некога.[15]

[14] http://sr.wikipidia.org./sr-el/razgovor_sa_korisnikom:Internetservis/05/03/2013.
[15] Гордана Буљан-Флендер,*Интернет и дјеца-требамо ли бринути*, http://www.psihonet.com/aktuelni_osvrti/23/03/2013.

Најчешћа асоцијација која се односи на злоупотребу интернета у вези је са порнографијом, међутим и остали сајтови са нелегалним садржајем врше утицај на дугорочно „тровање“ деце, нудећи разне облике менталног злостављања (секте, нацистички садржаји, дроге, разне врсте дијета и сл.). Посетиоци тим садржајима приступају из разних побуда, а деца то најчешће раде из разлога радозналости и дечије наивности. Као финална фаза следи „учлањење“ и лични контакт, што може имати несагледиве последице и трауматична искуства.

Ова запажања су уско повезана и са теренским истраживањем, тзв. „виртуелном девојчицом“. За 50 сати проведених на *chatu*, Астрина девојчица је примила 457 позива на разговор, у 86% случајева контакт је иницира од особе мушког пола, а у 27% случајева (125 разговора) било је присутно сексуално узнемиравање! Одабране причаонице су биле главне собе на „Крстарици“ и „*Serbian Caffeu*“, а лажни идентитет „виртуелне девојчице“ поткрепљен је профилима на *ICQ-u* и *„Skypeu”*.[16]

Када су деца у питању, начини „тешења“ су добар и проверен приступ (углавном је то добар виртуелни вршњак - пун разумевања). Након стицања поверења наредна фаза је слање фотографија, упућивање на *web* портале или заказивање „дружења“ и лични контакт. У овој последњој фази се дете присиљава путем уцене или простим системом силе на жељену активност (ово се не мора односити само на блуд, већ и на друге врсте искоришћавања, крађе, преваре...). Ко се крије у соби? У овој причи не може да се заобиђе и најпопуларније, али истовремено и најопасније подручје интернета, „*chat-room*“. Овакав сервис омогућује деци да виртуелно путују у било који део света, да разговарају с било ким, размењују поруке са људима о којима ништа не знају и који су за њих потпуни странци. Дете не зна ко је са друге стране, а то често могу и знају бити одрасли. У својој наивности и жељи да се упозна са вршњацима из других крајева и земаља, дете сасвим искрено и наивно пружа информације о себи, својим годинама, узрасту, полу, месту боравка, школи и свему другом. Путем „*chat-rooma*“ педофили сазнају све о детету; куда се креће, шта воли, какав му је распоред, у каквим је односима с родитељима, с браћом и сестрама и сл. Педофили се чак не морају активно укључити у разговор, већ скривено пратити разговор међу децом и прикупљати информације.[17]

[16] „Интернет, видови интернет криминала у нашој земљи”, *Свет компјутера,* http://sk.rs/2007/03/skin 02.html/ 19/03/2011/датум приступа/16/03/2013.
[17] http://sr.wikipidia.org./sr-el/razgovor_sa_korisnikom:Intrnetservis/16/03/2013.

Утицај информационих и комуникационих технологија на развој деце и њихова заштита од злоупотреба на интернету

Сајбер насиље, заправо, има све елементе насиља и изазива реалне последице без обзира на то што је учињено у тзв. виртуелном простору. Специфичност овог насиља је да се врши преко уређаја, што у суштини камуфлира реалну представу, јер се верује да постоји лаган излаз, тј. заштита за жртву, која се састоји у искључивању уређаја и изласку из сајбер простора. Недостатак едукације ускраћује могућност реалног сагледавања проблема, у супротном би се подразумевало да је сајбер простор временом постао део нашег животног амбијента, те да његово тренутно напуштање има идентично значење као и промена реалне средине, са околностима и последицама које тај чин производи, али и кључном чињеницом за ову прилику, да пресељењем насиље обично не престаје.

Упутно је овом приликом навести одређена запажања излагача са стручног скупа „Виртуелно детињство-фокусирање проблема, превенција и препоруке“:[18]

- Под утицајем примена информационих и комуникационих технологија, виртуелна стварност све више улази у живот све већег броја људи. Деца све масовнији корисници ИКТ, имају све пунији доживљај виртуелног детињства;
- Миленијумска генерација одрасла је уз интернет и „увек је *online*“. Дигиталне технологије су само неорганski део њиховог тела, а друштвени медији нису њихово виртуелно већ реално окружење;
- Информациона технологија је постала свакодневни део живота савремене породице. Компјутер није непознаница ни за децу предшколског узраста;
- Информационе и комуникационе технологије постале су неодвојиви део живота деце. Њиховом употребом, деца су поред велике користи и позитивних ефеката, изложена бројним опасностима. Постоји могућност да се код њих развије зависност. У виртуелном свету они се неретко сусрећу и са бројним преварама и непријатностима;
- Родитељи деце и тинејџера су често фасцинирани издржљивошћу, са којом њихови потомци издрже седети испред компјутера. У мислима су пренесени у зачарани свет информација, забаве и виртуелног дружења, заборављајући на време и своје обавезе. Забране су већином бескорисне, јер деца могу сурфовати у школи или код пријатеља, где нису под контролом;

[18] Стручни скуп „Виртуелно детињство-фокусирање проблема, превенција и препоруке“, Београд, 29. 06. 2011, www.internetservis.co.rs/virtuelo detinjstvo/21/03/2013.

- Нихилизам савремене технологије уништава осећајност, солидарност и критичку свест. Ревитализација религијских и магијских ритуала у контексту технокултуре за жртву узима људску душу, чиме доводи до технолошког уздрмавања самог статуса људског бића;
- Виртуелни свет је започео реалну битку са стварним, реалним простором. Оба света су почела да се мешају у главама деце.

Васпитавање деце, њихово образовање, усмеравање и пуштање у самосталан живот су неизбежне и неисцрпне теме. Поред бројних утицаја на наше животе, данас је заиста неспорно да компјутерска технологија и интернет, незаобилазно представљају важан део директних и индиректних утицаја. Они су до те мере изражени да је неминовна и опште корисна активност родитеља у контексту едукације и превенције, тј. познавања и суочавања са проблемом, на који начин компјутерске игрице и виртуелна стварност утичу на децу и њихов развој. На који начин пустити дете у тзв. дигитални свет, а да оно при том буде безбедно и да избегне нежељена искуства, питање је које је опште присутно и које из дана у дан добија на значају. Наиме, што се више људи ослања на Интернет то више људи рачуна на његову безбедност.

Основна правила која треба примењивати када су у питању приватност и безбедност података на Интернету, по савету стручњака су:[19]

- креирање безбедног профила;
- на Интернету не треба давати или објавити личне податке, бројеве телефона, назив школе, *e-mail* адресу и сличне податке;
- водити рачуна о типу и количини података која ваша деца размењују на Интернету;
- увек чувати лозинку у тајности;
- научите своје дете да не одговара на увредљиве поруке;
- научите своју децу да не отварају *e-mail* од непознатих људи;
- пожељно је користити софтвере за скидање непожељних *e-mail* – спамова;
- научите своје дете да блокира поруке од одређених пошиљалаца.

Међутим, упркос наизглед једноставним правилима и препорукама, постоје очигледне потешкоће у њиховој практичној спроводљивости, јер огроман део популације има апсолутно некритички однос према новим технологијама и изазовима савременог друштва. Са друге стране све је дубљи јаз између младих и старијих генерација, нарочито у погледу знања и примењивања компјутерских техника. Зато друштво постаје свесно тога да се не може рачунати на самоконтролу појединца, па се све више говори о томе да је нужно спроводити ефикасне програме

[19] http://www.kliknibezbedno.rs/latin/roditelji.html/23/03/2013.

едукације у циљу смањења ризика и заштите корисника од електронског насиља кроз доношење одређених упутстава и препорука. Те препоруке морају бити фокусиране не само на децу узраста до 18 година, већ и на одрасле кориснике Интернета, родитеље, наставнике, васпитно особље, јавне институције, али и службе безбедности које се баве спречавањем криминала.

Закључак

Појава Интернета довела је до тога да комуникација никад није била доступнија, јефтинија и бржа. Упоредо са позитивним странама Интернета, постоје и штетне појаве које су отвориле простор за разне врсте злоупотреба. Иако је данас немогућ живот и функционисање друштва у целини без употребе рачунара и савремене информатичке технологије, сазрела је свест да се ова корисна и потребна средства могу користити за недопуштене, противправне циљеве.

Употреба Интернета праћена је многим опасностима, као што су опасности од губитка, фалсификовања или крађе драгоцених информација и уништавања компјутерских система. Такође, у последње време се нарочито актуелизују питања приватности, слободе и контроле коришћења интернета. Наиме, у сваком тренутку смо перманентно изложени „*spam e-mail*“-овима, крађи идентитета, злоупотреби деце, порнографији, хакингу, коришћењу интернета као оружја ради дестабилизације виталних инфраструктурних система, као и разним другим злоупотребама. Истовремено последице сајбер криминала, односно штете настале вршењем компјутерских деликата мере се билионима долара. Поред тог финансијског аспекта, штете се могу анализирати и кроз нематеријални аспект, који се огледа у неовлашћеном откривању туђих тајни, или пак неком другом „индискретном штетном поступању“.

Врбовање жртава путем Интернета, пре свега у Интернет причаоницама, тешко је разликовати од безазленог дружења. Зато је важно да сви корисници Интернета, без обзира да ли су професионалци или обични корисници, буду упознати са претњама и техникама заштите од истих.

Данас, као никада до сада, имамо функционалну угроженост породице форсирањем индивидуализма и ривализирања. Миленијумска генерација одрасла је уз интернет и „увек је *on-line*“. Дигиталне технологије су само неорганski део њиховог тела, а друштвени медији нису њихово виртуелно већ реално окружење. Очигледно је да је виртуелни

свет започео реалну битку са стварним, реалним простором. Оба света су почела да се мешају у главама деце, зато је заштита деце од злоупотреба на интернету нужност и обавеза, како породице, тако и друштва у целини. Каже се да је заштита онолико добра колико је добра њена најслабија карика, а најслабија карика сваког система је најчешће човек, тако да је најбитније примењивати константан систем едукације свих корисника, а посебно младе популације, не заобилазећи при том категорију деце, која све чешће представљају циљну групу различитих форми злоупотреба информационо-комуникационих технологија.

Литература:

1. Aleksić Živojin, Škulić Milan, *Kriminalistika*, Dosije, Beograd, 2002.
2. Bellour J. C.: „Međunarodna prevara“, *Izbor br.1*, Zagreb, 1981, str. 76-77.
3. Bjelajac Željko, *Organizovani kriminalitet-Imperija zla*, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, 2013.
4. Bjelajac Željko, „Cyber Crime and Internet Pedophilia”, *Western Balkans From Stabilization to Integration,* Institute of International Politics and Economics, Belgrade, 2011, pp. 437–456.
5. Bjelajac Željko, Matijašević Jelena, Dimitrijević Duško, „Značaj uspostavljanja međunarodnih standarda u suzbijanju visokotehnološkog kriminala”, *Međunarodna politika*, *br 1146*, April–Jun 2012, Beograd, str. 66–85.
6. Bjelajac Željko, Matijašević Jelena, Dimitrijević Duško, „Konvencija Saveta Evrope o visokotehnološkom kriminalu”, *Evropsko zakonodavstvo*, *God. XI, br. 42*, Beograd, 2012, str. 37–52.
7. Bjelajac Željko, Matijašević Jelena, Dimitrijević Duško, „Computer fraud as a part of contemporary security challenges“, *Review of International Affairs 1147*, avgust-septembar 2012, str. 5-21.
8. Livingstone Sonia, Haddon Leslie, Görzig Anke and Ólafsson Kjartan, „Risks and safety on the internet: The perspective of European children“, Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. This report, based on the final dataset for all 25 countries, presents the final full findings for EU Kids Online Deliverable D4: Core findings to the European Commission Safer Internet Programme (13 January 2011), p. 36.
9. Radulović Saša, „Pretnje visokotehnološkog kriminala i domaća zakonodavna regulativa“, *Revija za bezbednost – stručni časopis o korupciji i organizovanom kriminalu*, br. 8/08, godina II, Centar za bezbednosne studije, Beograd, str. 18.
10. Stanarević Svetlana, Ejdus Filip i ostali „Pojmovnik bezbednosne kulture“, *Centar za civilno-vojne odnose*, Beograd, 2009.
11. Huitt G.William, *Success in the Information Age: A Paradigm Shift*, Valdosta State University, Valdosta, Georgia,1999.

12. Clough Jonathan, „Principles of Cybercrime“, *Cambridge University Press*, Cambridge, 2010, pp.3-4.
13. http://www.kliknibezbedno.rs/latin/roditelji.html
14. http://sk.rs
15. http://sr.wikipidia.org.
16. http://www.internetservis.co.rs/virtuelo detinjstvo
17. http://www.psihonet.com
18. http://www.rnids.rs

Certain Aspects of Security Culture on the Internet

Summary: Safety culture is reflected in general terms to identify hazards, eliminate them or referring to those entities responsible to respond professionally and preserve endangered values. In addition, the values can be easily defined, as our beliefs about what is good or bad, or the extent to which something is right or wrong, permissible or impermissible, useful or not useful, desirable or undesirable, and thus reflects the moral dimension. Moral norms that used to stand, with the expansion of information - communication technologies, and the pervasive use of computers and the Internet as a global network, we are beginning to suffer drastic changes. Specifically, it is imposed by the global change in the speed and manner of communication, creating an important impact on the quality of life "common man". This influence is evident in all spheres of social life. Positive and useful novelties of modern information and computer technology, both as a side effect brought different forms of abuse and danger, especially when aimless and uncontrolled use of the Internet. Among other things, the most common associations related to Internet abuse is related to pornography. It is understood that other sites with illegal content influence the long-term" poisoning" children. In addition to the inevitable, and the primary role of parents, and the necessary support from all segments of society in order to raise the collective awareness through media and education campaign, geared towards children and young people, for information on the possibilities of protection on the Internet and how to use the general form of its safe use in to protect the integrity, especially minors.