Биљана Милошевић Шошо[1]
Универзитет у Источном Сарајеву
Филозофски факултет Пале

УДК 316.728:004
DOI 10.7251/FIZN1719055M
Прегледни научни рад

СВАКОДНЕВНИ ЖИВОТ ПРЕД ИЗАЗОВИМА И РИЗИЦИМА ДИГИТАЛНОГ ДОБА

Аутор овог рада има за циљ да укаже на једну значајну димензију свакодневног живота савременог човјека, која се тиче све веће примјене и кориштења различитих могућности информационо–комуникационих технологија у животу. Свједоци смо дигиталне револуције, у којој учествујемо и креирамо наше животе, будућност. То, свакако, поред низа предности и олакшица у свакодневном животу, носи и одређене ризике, проблеме, усљед инкриминисаног облика понашања у дигиталном простору и злоупотребе технологија. У раду ћемо представити дио резултата истраживања у Републици Српској, који освјетљава присуство најзаступљенијих облика високотехнолошког криминала и на овдашњим просторима.

Кључне ријечи: дигитално доба, свакодневни живот, модерне технологије, високотехнолошки криминал, РС

УВОД

Живот савременог човјека незамислив је без употребе савремених средстава масовног комуницирања, примјене модерних технологија и ово данас поприма, готово па фразеолошки облик у свакодневном говору. То нас само упућује на чињеницу колико дубоко смо загазили у информатичко доба, колико дуго смо свједоци дигиталне револуције и свега онога што она носи са собом. Јасно је да се на темељу овога може говорити о процесу преобликовања културе, тежњи ка формирању општег или универзалног културног обрасца[2], типичног за *глобално село*[3]. У свом тексту *Културни обрасци* Дивна Вуксановић истиче да је култура дијалектична, нужно у спору са самом собом, да је теорија о културним обрасцима одличан повод да се о култури мисли не статично, него дијалектично, не догматски него

---

[1] milosevic_biljana@yahoo.com

[2] Појам културни образац међу првима је оживо ЕдвардСапир, а најисцрпнија објашњења истог дата су од стране Рут Бенедикт, америчког антрополога. Она у свом дјелу *Обрасци културе* (1934) тврди да је свака култура јединствена и складна цјелина, несводива на друге културе и на основу тога се правдају евентуални отпори према било каквој врсти промјена.

[3] Маршал Маклаун је конструисао израз *глобално село* да би означио нове процесе модернизације и глобализације уз помоћ информација, комуникација и информатичких технологија.

критички и да су културни модели или обрасци, прије свега, вриједносно утврђене парадигме, посредством којих се врши друштвено валоризовање актуелног свијета културе, културног насљеђа, као и њихових деривата (2014). Све претходно наведено, иде у прилог тези да је нагли уплив савремених, дигиталних технологија, у свакодневни живот човјека дихотомног карактера, тј. колико су емаципацијски и од велике важности, толико су и забрињавајући.

У остатку рада, позабавићемо се, управо овим, забрињавајућим аспектом који носи дигитално доба, кроз свакодневну употребу информационо-комуникационих технологија, у постојећем друштвеном контексту. Сви постојећи ризици и проблеми (првенствено се мисли на употребу интернета и активности у виртуелном свијету кроз друштвене мреже) конзумената дигиталне технологије, упућују на то да се може олако постати и жртва исте/их, а што је примарно проблемска област оних који се баве високотехнолошким криминалом, али и свих осталих који се интересују за различите облике инкриминисаних радњи у друштвеним заједницама, те посљедицама истих.

СОЦИОПАТОЛОШКА ОБИЉЕЖЈА АКТИВНОСТИ У ДИГИТАЛНОМ ПРОСТОРУ

Уназад двије деценије дигитална технологија, а самим тиме и савремена информационо-комуникациона средства су постала саставни дио свакодневног живота модерног човјека. Број корисника интернета је са 2% у 1997. години порастао на приближно 40% у 2014. години. Према неким процјенама, крајем 2015. године скоро половина свјетске популације је требало је да има приступ интернету (Кузмановић, Лајовић, Грујић и Меденица, 2016, стр. 15).[4] Многи критичари савремене културе наслућују „поводљивост“ модерног човјека за новим технологијама и да нам пријети опасност од технолошког детерминизма (Коковић, 2005). Интернет користимо (скоро) сви, а само на Балкану од скоро 20 милиона људи који ту живе – интернет користи чак 18 милиона нас, док више од 15 милиона људи са ових простора има Фејсбук профил.[5] Но, колико год да се настојала скренути пажња на ову врсту проблема, не може се занемарити чињеница да имамо потпуно нове генерације које су рођене и стасавају у дигиталој ери. За њих је то потпуно прихватљив

[4] Имена ауторки се везују за публикацију *Дигитално насиље – превенција и реаговање* која је објављена у оквиру програма *Развој капацитета система за борбу против насиља, злостављања и злоупотребе деце путем интернета* који су, уз финансијску подршку Владе Велике Британије, реализовали Министарство просвете, науке и технолошког развоја Републике Србије, Педагошко друштво Србије и УНИЦЕФ.

[5] http://www.digitalcommunicationsinstitute.com/drustveni-mediji-i-njihov-uticaj-na-nas/

животни концеп и немогуће је, а донекле и штетно, вршити било какав покушај „изопштавања“ из такве, свакодневне „рутине“. Оно што се може учинити јесте континуирано скретање пажње на „тамну страну“ дигитализације живота и заштити/их се од епитета „жртва дигиталног (сајбер) насиља“.

Компјутерски или сајбер криминал је врста делинквенције и типологија криминалних појава настала у вези са злоупотребом компјутерске технике и технологије (Бошковић, 2006, стр. 425). Утемељивач ове области Огист Бекваји [August Bequai], компјутерски криминал одређује као свако вршење кривичних дјела код којих се рачунар појављује као оруђе или објекат заштите (Игњатовић, 2011, стр. 113). Радна група формирана од Комитета за политику, информатику и комуникације ОЕБС-а описала је криминал као:

“Унос, измјену, брисање и/или прикривање података и/или програма намјерно предузиманих да би се извршио илегални трансфер фондова и других вриједних података; унос, измјену, брисање и/или прикривање података и/или програма намерно предузиманих да би се извршила превара; унос, измена, брисање и/или прикривање података и/или програма или других сметњи, намерно предузиманих да би се ометале функције рачунарских система и/или телекомуникација; нарушавање ексклузивних права власника заштићених рачунарских програма, са намером њиховог комерцијалног коришћења или препродаје; неовлашћен приступ до рачунарског или телекомуникационог система или намерно прислушкивање таквих система и нарушавање мјера њихове заштите“ (Бошковић, 2006, стр. 453).

Компјутерски криминал је глобалног карактера па тако Европска конвенција о компјутерском криминалу[6] предвиђа четири групе дјела: дјела против повјерљивости, интегритета и доступности компјутерских података и система, дјела везана за компјутере, дјела везана за садржаје (дјечија порнографија као најчешћи садржај), дјела везана за кршење ауторских и сродних права (Бошковић, 2006, стр. 458). Криминолошка литература препознаје неколико врста компјутерског криминала и то:

„*Политички* (сајбер шпијунажа, сајбер хакинг, сајбер саботажа, сајбер тероризам и сајбер ратовање) *економски* (сајбер преваре, крађа Интернет услуга и времена, пиратерија софтвера и чипова, сајбер индустријска саботажа), *производња и дистрибуција недозвољених и штетних садржаја* (дјечија порнографија, педофилија вјерске секте, ширење расистичких, националистичких и сличних ставова и идеја, злоупотреба жена и дјеце), *манипулација забрањеним производима, супстанцама и робама* (дрогама, људским органима, оружјем), *повреде сајбер приватности* које се односе на надгледање електронске поште, разне рекламне понуде, крађа налога на друштвеним мрежама, ’качење’ и анализа ’cookies’, крађа новца преко кредитних картица и крађа идентитета“ (McQuade, 2009, p. 44).

[6] https://rm.coe.int/1680081561, Budapest, 23.XI.2001. Датум приступа: 22. 9. 2017.

У наставку рада приказан је дио резултата мањег истраживања о друштвеним промјенама у Републици Српској у којем је анализирана „посвећеност“ испитаника друштвеним мрежама, заступљеност сајбер насиља и његових појавних облика, те могући, корелативни односи између одређених појава, у овом случају, налаза.

МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

Претходно поменуто истраживање је обухватило узорак од 220 испитаника, од чега 113 припадница женског пола и 102 припадника мушког пола, из седам општина у Републици Српској, старосне доби од 18 до 66 и више година, у периоду од октобра 2016. године до фебруара 2017. године. Од укупног броја испитаника њих 59,1% је незапослено, док 40% има неки радни статус. Кориштена је дескриптивна метода и статистички је мјерен степен повезаности одређених појава помоћу Пирсоновог [Pearson] коефицијента корелације. Статистичка обрада података извршена је примјеном софтверског пакета *SPSS* (*Statistical Package for Social Sciences).*

РЕЗУЛТАТИ ИСТРАЖИВАЊА

У Табели 1 приказани су резултати о учесталости кориштења друштвених мрежа у свакодневном животу наших испитаника и колико је то њихова интересна сфера на основу старосне доби, примјеном метода за категоризацију и комбиновање података *Crosstabulation,* у циљу откривања њихове просте повезаности. Како је то већ наведено у претходном дијелу рада, потпуно је за очекивати да су млади, старосне доби од 18 до 24 године, најчешћи конзументи и корисници друштвених мрежа. Њих 45-оро свакодневно посјећује друштвене мреже. Нешто мање испитаника, у доби од 25 до 31 године, њих 24-оро и, у доби од 32 до 38 година, њих 12-оро свакодневно посјећује друштвене мреже. Оно што је интересантно, јесте да и старијим испитаницима није страна посјета друштвеним мрежама. Њих 5-оро у доби од 53 до 59 година и њих двоје у доби од 60 до 66 година понекад посјете друштвене мреже.

Табела 1. Године старости * Свакодневно посјећујем друштвене мреже Crosstabulation

		Свакодневно посјећујем друштвене мреже				Укупно
		Никад	Понекад	Често	Недостаје одговор	
Године старости	од 18 до 24	6	12	45	0	63
	од 25 до 31	5	6	24	1	36
	од 32 до 38	14	13	12	2	41
	од 39 до 45	9	5	9	1	24
	од 46 до 52	12	9	5	0	26
	од53 до 59	9	5	1	0	15
	од 60 до 66	2	2	0	0	4
	више od 66	9	0	0	2	11
	Укупно	66	52	96	6	220

Такође, настојали смо спознати да ли има разлике међу испитаницима при посјећивању друштвених мрежа, сходно њиховом радном статусу. Резултати приказани у Табели 2 указују на то да свакодневно друштвене мреже најчешће посјећују незапослене особе, њих 57-оро, повремено њих 30-оро, што можемо тумачити, нажалост, вишком слободног времена и да је то једна од активности у оквиру истог, поред општег тренда, својственог за дигиталну еру. Исто тако, није занемарљив податак и међу запосленима, јер су њих 38-оро чести посјетиоци друштвених мрежа, 21 повремено прати и посјећује друштвене мреже.

*Табела 2. Да ли сте запослени * Свакодневно посјећујем друштвене мреже Crosstabulation*

		Свакодневно посјећујем друштвене мреже				Укупно
		Никад	Понекад	Често	Недостаје одговор	
Да ли сте запослени	Да	29	21	38	0	88
	Не	37	30	57	6	130
	3	0	1	0	0	1
	Недостаје одговор	0	0	1	0	1
	Укупно	66	52	96	6	220

Сагледавајући до сад добијене резултате, више је него очито да се и на овим просторима не заостаје за глобалним трендовима у сфери дигиталне комуникације, те да су нове технологије постале неминовност и да су се успјешно инфилтрирале у све сегменте свакодневног живота (Мирковић, 2016). Нешто негативнија статистика овог истраживања односи

се на број жртава сајбер насиља. Увидом у резултате (Табела 3) видиљиво је да је 1,8% испитаника често било жртва сајбер насиља, врло често, 05%, а понекад 4,5 % или 10 испитаника. На први поглед, ови резултати можда дјелују безначајно, али кад се сагледа обимност узорка, сматрамо потпуно супротно, те и то да ако се и једна особа нашла у улози жртве сајбер насиља јесте упозоравајући сигнал о присуству девијантног понашања у дигиталном простору.

Табела 3. Број жртава сајбер насиља		
	Број	%
Никад	202	91.8
Понекад	10	4.5
Често	4	1.8
Врло често	1	.5
Недостаје одговор	3	1.4
Укупно	220	100.0

У Табели 4 представљени су резултати корелативног односа између испитаника који свакодневно посјећују друштвене мреже и могућности да постану жртве сајбер насиља. Резултат нам указује да се ради о позитивној корелацији, средњег интервала и на значајну повезаност ове двије појаве (r =0,385). Корелација је значајна на нивоу 0,01, двоструко.

Табела 4. Свакодневно посјећујем друштвене мреже * жртве сајбер насиља			
		Жртве сајбер насиља	
		Недостаје одговор	Укупно
Свакодневно посјећујем друштвене мреже	Никад	0	66
	Понекад	0	52
	Често	1	96
	Недостаје одговор	2	6
	Укупно	3	220

N = 220; r = 0,385; P = 0.000

Нешто нижа, позитивна корелација (r = 0,153) постоји и између појава свакодневног посјећивања друштвених мрежа и шансе да се буде жртва крађе шифре, односно password-a, што спада у ред сајбер криминала и то у домену *повреде сајбер приватности.* Корелација је значајна на нивоу 0,05, двоструко.

Табела 5. Свакодневно посјећујем друштвене мреже *Крађа *passworda*					
		Крађа *passworda*			
		Да	Не	Недостаје одговор	Укупно
Свакодневно посјећујем друштвене мреже	Никад	4	62	0	66
	Понекад	5	47	0	52
	Често	23	72	1	96
	Недостаје одговор	1	4	1	6
	Укупно	33	185	2	220

N = 220; r = 0,153; P = 0,000

У Табели 6 и Табели 7 приказали смо резултате који говоре да постоји значајан однос између нивоа оних који свакодневно посјећују друштвене мреже и могућности да им се нуде садржаји за проституцију и садржаји за дјечију проституцију у форми рекламног облика. У првом случају ради се о корелацији средњег интервала (r = 0,322), а у другом, такође, о корелацији средњег интервала (r = 0,329) које су значајне на нивоу 0,01 и то двоструко. У овом примјеру, имамо преклапање економског сајбер криминала и повреде сајбер приватности као типова инкриминисаног понашања у сајбер простору.

Табела 6. Свакодневно посјећујете друштвене мреже* Нуде Вам се садржаји понуда за проституцију			
		Нуде Вам се садржаји понуде за проституцију	
		Да	Не
Свакодневно посјећујем друштвене мреже	Ниакд	3	63
	Понекад	6	46
	Често	8	85
	Недостаје одговор	0	4
	Укупно	17	198

N = 220; r = 0,322; P = 0,000

Табела 7. Свакодневно посјећујем друштвене мреже * Нуде Вам се садржаји са понудама за дјечију проституцију			
		Нуде Вам се садржаји са понудама за дјечију проституцију	
		Да	Не
Свакодневно посјећујем друштвене мреже	Никад	2	64
	Понекад	2	50
	Често	4	89
	Недостаје одговор	0	4
	Укупно	8	207

N = 220; r = 0,329; P = 0,000

Слободу коју нуди сајбер простор и његове апликације, попут друштвених мрежа, увелико користе и неки други поборници инкриминисаног облика понашања, те је врло извјесно да ће скоро сваки корисник друштвених мрежа бити у прилици да се сусретне са понудом чија садржина обилује промоцијом расистичких или националистичких идеја и мотива. Такву врсту могућности приказали смо кроз резултате у Табели 8, која указује на позитиван корелативни однос, нешто нижег интезитета (r = 0,288) и која је значајна на нивоу 0,01 двоструко.

Табела 8. Свакодневно посјећујем друштвене мреже * Нуде Вам се понуде са расистичким, националистичким садржајима			
		Нуде Вам се понуде са расистичким, националистичким садржајима	
		Да	Не
Свакодневно посјећујем друштвене мреже	Никад	5	61
	Понекад	8	44
	Често	24	69
	Недостаје одговор	0	4
	Укупно	37	178

N = 220; r = 0,288; P = 0,000

У наставку рада приказаћемо добијене резултате корелативног односа између нивоа самих жртава сајбер насиља и најучесталијих облика сајбер криминала у модерном времену. Резултати приказани у Табелама 9, 10 и 11 указују на постојање изузетно високих позитивних корелација између жртава сајбер насиља и злоупотребе рачунарске мреже у форми крађе кредитних картица, с циљем нарушавања финансијских трансакција и наношења материјалне штете, крађе интернет услуга и времена те крађе идентитета кроз нарушавање налога на друштвеним мрежама.

У Табели 9 имамо позитивну корелацију нивоа жртава сајбер насиља и крађе кредитних картица и средстава (r =0,722), изузетно високог интезитета, значајну на нивоу 0,01, двоструко. Иначе, од свих облика сајбер криминалитета, овај облик компјутерског криминалитета спада у ред најраширенијих, по моделу (modus operandi) и врло је прилагођен свим варијантама финансијских превара, са различитим начинима дјеловања (Бошковић, 2006, стр. 461).

Табела 9. Жртве сајбер насиља* Крађа кредитних картица и средстава

		Крађа кредитних картица и средстава			Укупно
		Да	Не	Недостаје одговор	
Жртве сајбер насиља	Никад	7	194	1	202
	Понекад	1	8	1	10
	Често	0	4	0	4
	Врло често	0	1	0	1
	Недостаје одговор	0	0	3	3
	Укупно	8	207	5	220

$$N = 220; r = 0,722; P = 0,000$$

Табела 10 представља приказ резултата корелативног односа између нивоа жртава сајбер насиља и нивоа крађе интернет услуга и времена као једног од типова сајбер криминала и то економског, који обухвата сајбер преваре, хакинг, крађу интернет услуга и времена, пиратство софтвера, микрочипова и база података, сајбер индустријску шпијунажа, лажне интернет аукције. Добијени Пирсонов коефицијент корелације је изузетно висок (r = 0,698), а значајност је на нивоу од 0,01, двоструко.

Табела 10. Жртве сајбер насиља * Крађа интернет услуга и времена					
		Крађа интернет услуга и времена			Укупно
		Да	Не	Недостаје одговор	
Жртве сајбер насиља	Никад	16	185	1	202
	Понекад	0	9	1	10
	Често	1	3	0	4
	Врло често	1	0	0	1
	Недостаје одговор	0	0	3	3
	Укупно	18	197	5	220

$$N = 220;\ r = 0{,}698;\ P = 0{,}000$$

Проблеми крађе идентитета све су чешћи јер су друштвене мреже постале свеприсутне у савременом друштву те је једна од инкриминисаних активности овог типа и крађа профила на друштвеним мрежама. То је постало специфичан проблем дигиталног доба, при чему нису само на удару појединци, већ различите институције, које имају свој/е профиле на друштвеним мрежама. Отклањање овог проблема захтијева дужи временски период, јер се докази у дигиталном свијету обрађују методом дигиталне форензике, попут реконструкције рачунарских података које је починилац кривичног дијела претходно избрисао, што додатно указује на тежину оваквог проблема. Ово је такође једна од техника којом се служе у сфери социјалног инжењеринга[7] као методе манипулације савременим човјеком у дигиталном простору. Управо у Табели 11 имамо приказане резултате корелативног односа између нивоа жртве сајбер насиља и нивоа крађе профила на друштвеним мрежама и ради се о ниској, позитивној корелацији (r = 0,203) на нивоу значајности од 0,01, двоструко.

[7] Социјални инжењеринг је метода наговарања људи да испуне захтјеве нападача. Ради се о начину стицања информација и података до којих нападач легитимним путем не би могао доћи. При томе се не искориштавају пропусти имплементација операцијских система, протокола и апликација, него се напад усмјерава на најслабију карику цјелокупног ланца – људски фактор. Преузето са:
http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-172.pdf.

Табела 11. Жртве сајбер насиља * Крађа профила на друштвеним мрежама					
		Крађа профила на друштвеним мрежама			Укупно
		Да	Не	Недостаје одговор	
Жртве сајбер насиља	Никад	21	181	0	202
	Понекад	8	2	0	10
	Често	4	0	0	4
	Врло често	1	0	0	1
	Недостаје одговор	2	0	1	3
	Укупно	36	183	1	220

$$N = 220;\ r = 0{,}203;\ P = 0{,}000$$

ДИСКУСИЈА

Савремено доба донијело је нека нова обиљежја комуникације и обављања свакодневних активности захваљујући новим технологијама и достигнућима информатичке или дигиталне револуције. Дјеловање у виртуелном простору, захваљујући интернету, полако мијења досадашње навике и стил живљења, код већине нас, утичући на тај начин и на преобликовање некадашње културе живљења. Поред низа предности које са собом носи дигитална ера, попут брзине и лакоће обављања различитик активности, доступности информација, она са собом носи и неке негативне конотације, на што су указали резултати наше анализе о присуству сајбер криминала у различитим појавним облицима на простору Републике Српске. Током самог истраживања, нашу пажњу смо усмјерили на коришћење друштвених мрежа у свакодневници, те евентуалним посљедицама од тога, као и на дио најзаступљенијих инкриминисаних радњи у виртуелном свијету. Резултати нас упућују на то да више од половине испитаника свакодневно посјећује пажњу друштвеним мрежама, без претјеране разлике у смислу њиховог радног ангажмана, а донекле и старосне доби. Надаље, резултати анализе указују на то да свакодневна посјета друштвеним мрежама јесте потенцијално пријетећа опасност за постајање жртвом сајбер насиља, те изложености економском, политичком сајбер криминалу као и изложености повредама сајбер приватности. Они испитаници, који су имали несрећу да постану жртве сајбер насиља, у значајном мјери су то постали на основу крађе кредитних картица и финансијских средстава или крађе интернет услуга и времена, односно крађе профила на друштвеним мрежама. С обзиром да се ради о инкриминисамим, девијантним облицима понашања у виртуелном свијету, сасвим је очекивано да су за њих предвиђени и правни акти који регулишу такву врсту дјеловања, конкретно се мисли на

Кривични закон Републике Српске[8], од члана 292а до члана 292е. Но, и поред предвиђених санкција за оваке активности, у сваком случају би се требало превентивно дјеловати, посебно код млађег узраста, јер постоје још велике могућности различитих облика дјеловања у виртуелном простору, поред осталих латентних социопатских одредница живота у дигиталној ери.

ЛИТЕРАТУРА

Бенедикт, Р. (1976). *Обрасци културе*. Београд: Просвета.

Бошковић, М. (2006). *Криминологија.* Нови Сад: Правни факултет.

Бошковић, М. (1998). *Организовани криминалитет*. Београд: Полицијска академија.

Бранковић, С. (2014). *Методологија друштвених истраживања*. Београд: Завод за уџбенике.

Вуксановић, Д. (2014). Културни обрасци. *P.U.L.S.E*. Преузето са: http://pulse.rs/kulturni-obrasci-divna-vuksanovic/ Датум приступа: 10. 9. 2017.

Европска Конвенција о комјутерском криминалу, Будимпешта, (2001). Видјети: https://rm.coe.int/1680081561

Игњатовић,Ђ. (2011). *Криминологија*. Београд: Досије студио.

Кривични закон Републике Српске, Службени гласник РС. Бр.73 (2010)

Коковић, Д. (2005). *Пукотине културе*. Нови Сад: Прометеј.

Кузмановић, Д., Лајовић, Б., Грујић, С., Меденица, Г. (2016). *Дигитално насиље-превенција и реаговање.* Београд: Министарство просвјете, науке и технолошког развоја републике Србије и Педагошко друштво Србије.

Lorimer, R. (1998). *Masovne komunikacije*. Beograd: CLIO.

McQuade III, C. S. (2009). Cubercrime Attacks. *In Encyclopedia of Cubercrime*. London: Greenwood Press.

McLuhan, M. (2008). *Razumijevanje medija*. Zagreb: Tehnička knjiga.

Мирковић, А. (2016). Друштвени медији и њихов утицај на нас. Digital Communcations Institute.

[8] http://mup.vladars.net/vtk/regulativa/docs/ZAKON%20O%20IZMJENAMA%20I%20DOPUNAMA%20KZ%20RS%20(Sluzbeni%20glasnik%20RS%2c%20broj-%2073.10)%20lat.pdf

Преузето са:
http://www.digitalcommunicationsinstitute.com/drustveni-mediji-i-njihov-uticaj-na-nas/ Датум приступа: 15. 9. 2017.
CARNet CERT I LS&S. *Socijalni inzenjering*, Br. 172 (2006).

Biljana Milosevic Soso
Faculty of Philosophy
University of East Sarajevo

DIGITAL AGE - CHALLENGES AND RISKS IN EVERYDAY LIFE

Summary

The author of this paper aims to point to an important dimension of the everyday life of a modern day man, increasing use of various possibilities of information and communication technologies. We witness digital revolution, in which we participate and it somehow create our lives and future. Certainly, in addition to a number of advantages and benefits, it also carries certain risks, problems, due to the incriminated behavior in the digital (virtual) space and the abuse of technology. The paper will also present research results which shows presence of the most common forms of high-tech crime in the Republic of Srpska.

Research focused on use of social media in everyday life, possible consequences, as well as the part of the most commonly incriminated actions online. The results show that more than half of the respondents were using various social media on a daily basis, without excessive differences in terms of their employment or age. Furthermore, the results of the analysis indicate that the daily social networks interaction is threatening danger of becoming a victim of cyber crimes as well as economic, political crimes and cyber privacy violations.

All legal activities should be preventive, especially protecting young online users. The survey included a sample of 220 respondents, 113 women and 102 men, in seven municipalities in the Republic of Srpska, aged 18 to 66 and over, from October 2016 to February 2017. Out of the total number of respondents, 59.1% were unemployed, while 40% have some form of employment. A descriptive method, statistically measured, was Pearson's correlation coefficient showing degree of connection between certain phenomena. The results suggest that more than half of the respondents were using social media on a daily basis, regardless of employment status, gender, or their age. Furthermore, the results of the analysis indicate that the daily visit to social media is in a potential danger

of becoming a victim of various cyber crimes, such as exposure to economic or political cyber crime, and exposure to cyber privacy violations. Those unlucky respondents to become victims of cyber crimes usually have become due to credit card fraud, theft of Internet services time, theft of profiles on social media or online harassment. In order to protect digital space, it is necessary to act and educate young people, because there is still a large number of different forms of action preventing sociopathic determinants of life in the digital era.