УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Вида М. Вилић

ПОВРЕДА ПРАВА НА ПРИВАТНОСТ ЗЛОУПОТРЕБОМ ДРУШТВЕНИХ МРЕЖА КАО ОБЛИК КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

докторска дисертација

Ниш, 2016.

UNIVERSITY OF NIŠ
FACULTY OF LAW

Vida M. Vilić

VIOLATION OF RIGHT TO PRIVACY ON SOCIAL NETWORKS AS A FORM OF CYBER CRIMINALITY

doctoral dissertation

Niš, 2016.

Подаци о докторској дисертацији

Ментор:	*Проф. др Миомира Костић, редовна професорка* Универзитет у Нишу, Правни факултет
Наслов:	Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета
Резиме:	Рад садржи теоријско-емпиријско сагледавање компјутерског криминалитета и злоупотребе друштвених мрежа, посебно оних облика којима се повређује право на приватност као једно од основних људских права. Према времену настанка, компјутерски криминалитет припада новијим облицима криминалитета, чије је појављивање резултат великог напретка технологије у области телекомуникација. Употребом компјутерске технике, посебно интернета и друштвених мрежа, велики број корисника изложен је свакодневној виктимизацији, уколико подаци пренети путем друштвених мрежа буду злоупотребљени. Због тога је рад посвећен злоупотреби друштвених мрежа као девијантном понашању, које није увек законом санкционисано као криминално понашање, али је свакако друштвено неприхватљиво и противно друштвеним нормама понашања. Компјутерски криминалитет и злоупотреба друштвених мрежа, као девијантно понашање и део компјутерског криминалитета, одликује високи степен анонимности извршилаца, стална доступност жртве и виктимизација великих размера, мултијурисдикциона природа, отежан рад органа гоњења, прикупљања доказа, пресуђивања и кажњавања. Друштвене мреже на интернету, као најраширенији и најпопуларнији начин комуникације у савременом свету, довеле су до тога да је приватни живот постао саставни део јавног живота. Озбиљан недостатак коришћења друштвених мрежа представља велика изложеност корисника разним облицима

	злоупотребе, као што су: крађа идентитета, преваре, дигитално насиље (сексуално насиље и узнемиравање, вршњачко насиље, прогањање, сајбер мобинг, говор мржње, тероризам), вандализам, трговина људима и људским органима, пиратерија, као и замена реалног света виртуелним и патолошка зависност од коришћења и злоупотребе интернета. Теоријско изучавање и емпиријско истраживање компјутерског криминалитета и злоупотребе друштвених мрежа треба да допринесе изградњи бољег система заштите и веће безбедности корисника друштвених мрежа. Постојећа законска регулатива на међународном и националном плану односи се углавном на злоупотребу рачунарског хардвера и софтвера, који приликом извршења кривичних дела могу да буду средство извршења или објекат напада (нпр. компјутерске крађе, преваре, оштећење рачунарских података и програма, саботажа, прављење и уношење рачунарских вируса), док се поједини облици злоупотребе друштвених мрежа уопште не инкриминишу, што значајно доприноси повећаној виктимизацији, посебно у домену приватности.
Научна област:	**Право (S 110)**
Научна дисциплина:	Криминологија **(S 160)** Кривично право, кривични поступак **(S 149)**
Кључне речи:	компјутерски криминалитет, интернет, друштвене мреже, право на приватност, компјутерске злоупотребе
УДК:	343.91::004.738.5 343.533::004.738.5
CERIF класификација:	S149
Тип лиценце Креативне заједнице:	**CC BY-NC**

Data on Doctoral Dissertation

Doctoral Supervisor:	LL.D Miomira Kostić, University of Niš, Faculty of Law
Title:	Violation of right to privacy on social networks as a form of cyber criminality
Abstract:	The paper contains a theoretical and empirical understanding of cyber crime and the misuse and abuse of social networks, especially those forms which violate the right to privacy as one of the basic human rights. Cybercrime is a new kind of crime which appeared as a result of great technological advances in the field of telecommunications. A large number of Internet and social networks users are exposed to daily victimization due to the use of computer technology, if the information transmitted through social networks is misused or abused. Therefore, the paper is dedicated to the misuse and abuse of social networks, which could be considered as a deviant behavior, which is not always legally sanctioned as criminal behavior, although it is certainly socially unacceptable and opposite to the social norms of behavior. Computer criminality and the misuse and abuse of social networks, considered as a deviant behavior and as a part of computer crime, are characterized by the perpetrators' anonymity, permanent availability of the victim and the high level of victimization, multi-juridical nature, difficult prosecuting procedure and gathering of the evidence, as well as the imposition of a legal sanction. Social networks, as the most common and most popular way of communication in the modern world, have led to the fact that the private life has become an integral part of public life. A serious lack due to the use of social networks is the great exposure of the user to various forms of abuse, such as identity theft, fraud, digital violence (sexual violence and harassment, bullying, stalking, cyber bullying, hate speech, terrorism), vandalism, human trafficking and organ

trafficking, bootlegging, as well as replacement of the real world with virtual life and creation of pathological dependence on the use of the Internet.

Theoretical study and empirical research of computer crime and social networks' misuse and abuse should contribute to the developement of one better system of protection and security improvement for all users of social networks. Current international and national legislation is mainly related to the abuse of computer hardware and software, which during the commission of crimes can be a means of execution or target of attack (eg, computer theft, fraud, damage of computer data and programs, sabotage, creation of computer viruses), while certain forms of abuse of social networks are still not incriminated, which significantly contributes to increased victimization, particularly in the area of privacy.

Scientific Field: **Juridical sciences (S 110)**

Scientific Discipline: Criminology **(S 160)**
Criminal law, criminal proceedings **(S 149)**

Key Words: Computer criminality, Internet, Social networks, Right to privacy, Computer abuse and misuse

UDC: 343.91::004.738.5
343.533::004.738.5

CERIF Classification: S149

САДРЖАЈ

„Приватност је веома вредна ствар.

Свако жели место где би с времена на време могао да буде сам.

И, када добије такво место, право је свакога који за то зна да то задржи само за себе.”

Џорџ Орвел (George Orwell), „1984“

УВОДНА РАЗМАТРАЊА

Интернет свакодневно користи велики број људи широм света, како би међусобно комуницирали, ступали у различите друштвене односе и везе, развијали личне и професионалне односе. Према подацима Републичког завода за статистику Републике Србије, 63,2% домаћинстава је у 2014. години поседовало рачунар у домаћинству, док је 62,8% користило интернет.[1] Интернет представља глобални информациони систем у савременом друштву, то је светска комуникациона мрежа или „мрежа свих мрежа“, која се састоји од великог броја засебних рачунара повезаних у мрежну структуру. Као глобална светска мрежа, интернет даје виртуелном простору глобалну димензију, што значи да омогућава везу између било које две тачке на планети кроз сајбер простор. Сајбер простор је истовремено и социјални простор који настаје спајањем два вида комуникације: комуникације посредством рачунарских мрежа и пословне комуникације подржане рачунарским системом.

Једну од најмоћнијих иновација у краткој историји постојања интернета представља настанак друштвених мрежа, које су још више проширile могућности комуникације међу људима, без обзира на то где се налазе. Неке од интернет апликација су довеле до тешкоћа са заштитом приватности, отварајући расправе да ли је код друштвених мрежа заправо реч о комерцијалном интересу, или стварању нових комуникација и повезивању људи широм планете. Приватност појединца, са друге стране, обухвата читав спектар различитих права, али је злоупотреби путем интернета највише изложен део права који се односи на податке о личности. Ризици злоупотребе података о личности односе се, пре свега, на крађу идентитета и крађу путем злоупотребе података о личности (online куповина, безбедна лозинка, безбедан e-mail), али и на злоупотребу података о личности у комерцијалне сврхе (неовлашћена продаја, нежељени „спам“ мејлови и сл).

Управо својом популарношћу и великим бројем корисника, друштвене мреже су створиле својеврстан „надзор“ над свакодневним активностима људи,

[1] Републички завод за статистику Републике Србије, http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2, претражено 09. 02. 2015.године

њиховим навикама, њиховим кретањем и дружењем. Уз све могућности које пружају интернет и друштвене мреже, небројено је велики број прилика за упознавање нових људи, стицање и развијање личних и професионалних односа, стварање различитих друштвених околности. Поред низа предности које интернет и друштвене мреже пружају, забележен је и пораст злоупотреба везаних за виртуелни простор.

Последњих година се све више говори о „мрачној страни сурфовања интернетом“ или „darknetu“, „Deep Web-u“, „дубокој мрежи“, где су подаци и информације закључани лозинкама, заробљени иза paywallova, или је потребан посебан софтвер да би се до њих дошло. Процењује се да је ово „дигитално подземље“ много веће од интернета и да хакери, криминалци, терористи, педофили потпуно несметано обављају своје актовности. У Darknetu се може купити: дрога, фалсификован новац, фалсификоване исправе, оружје, муниција и експлозив, наручени убиства, људски органи а постоји и посебан систем online плаћања уз прикривање идентитета.[2] С обзиром на то да се ради о новој области злоупотребе компјутера и мреже, недостају свеобухватна торијска и емпиријска истраживања о овој појави.

Предмет овог рада је теоријско-емпиријско сагледавање једног од најраспрострањенијих облика компјутерског криминалитета који обухвата повреду права на приватност злоупотребом друштвених мрежа. У данашње време честе су научне и стручне расправе о томе да ли криминалитет у области информационих технологија представља само наставак класичних облика криминалитета са којима се свакодневно суочавамо, или је посебан облик криминалитета који захтева ново дефинисање. У сваком случају, бар према времену настанка, компјутерски криминалитет припада новијим облицима криминалитета, чије је појављивање резултат великог напретка технологије у области телекомуникација. Све већа употреба интернета и друштвених мрежа, као и коришћење компјутерске технике у свакодневном животу, представљају огроман напредак са становишта друштвеног развоја. С друге стране, употребом компјутерске технике, посебно интернета и друштвених мрежа, велики број корисника изложен је свакодневној виктимизацији, уколико подаци пренети

[2] Анонимус: “Deep Web - Мрачна страна интернета”, Лагуна, Београд, 2015.

путем друштвених мрежа буду злоупотребљени. Стога је приступ овој теми криминолошко – виктимолошки јер се поред сагледавања најчешћих појавних облика компјутерског криминалитета и одговарајуће законске регулативе, анализира могућност и степен виктимизације корисника злоупотребом података који су објављени на друштвеним мрежама. Посебан део рада посвећен је злоупотреби друштвених мрежа као девијантном понашању, које није увек законом санкционисано као криминално понашање, али је свакако друштвено неприхватљиво и противно друштвеним нормама понашања.

Основни циљ рада је да се на основу теоријског изучавања и емпиријског истраживања компјутерског криминалитета и злоупотребе друштвених мрежа допринесе изградњи бољег система заштите и веће безбедности корисника друштвених мрежа. Како би се изградио бољи систем заштите корисника друштвених мрежа од бројних видова криминалитета којима су свакодневно изложени, неопходно је указати на потребу криминолошко виктимолошког проучавања друштвених мрежа, с обзиром на распрострањеност њиховог коришћења у свету и на велики број могућности за злоупотребу података пренетих путем ових мрежа. Досадашња проучавања и постојећа законска регулатива на међународном и националном плану односе се углавном на злоупотребу рачунарског хардвера и софтвера, који приликом извршења кривичних дела могу да буду средство извршења или објекат напада (нпр. компјутерске крађе, преваре, оштећење рачунарских података и програма, саботажа, прављење и уношење рачунарских вируса).[3]

Постављене хипотезе проверене теоријским изучавањем и емпиријским истраживањем су:

---

[3] Нову дисциплину „Сајбер (cyber) криминологија", која објашњава и анализира криминалитет на интернету, описује међусобни однос између науке о компјутерима, науке о интернету и криминологије, формулисао је Jaishankar 2007. године. *Видети:* Zucker, Susan: „Cyber Forensics: Part II", National Clearinghouse for Science, Technology and the Law at Stetson University, College of Law, http://www.ncstl.org/evident/Jan08Zucker, претражено 28.08.2015. године.
Сајбер криминологија се дефинише као „студија о узрочности криминалитета који се појављује у cyber простору и њеовог утицаја на дешавања у физичком простору". Jaishankar је Cyber криминологију увео из два разлога: пре свега због тога што је радња кривичног дела повезана са cyber форензиком и због тога што треба да постоји независна дисциплина која ће да проучава и испитује cyber кривична дела са становишта друштвених наука. *Видети:* Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, Edited by K. Jaishankar, CRS Press, 2011., http://ruangbacafmipa.staff.ub.ac.id/files/2012/02/Cyber_Criminology__Exploring_Internet_Crimes_and_Criminal_Behavior.pdf, претражено 28.08.2015. године

(1) Употреба информационих технологија у свету и у Србији веома је распрострањена и има тенденцију даљег интензивног развоја. Данас се не може замислити дневно, уобичајено функционисање друштва без употребе компјутера и интернета. Промењен је начин прикупљања, чувања, обраде и презентације информација, а појава интернета омогућила је приступ немерљивој количини информација и комуникацију широм света.

(2) Појава интернета и друштвених мрежа вишеструко је утицала на савремени живот и развој специфичних облика криминалитета, који се огледају у злоупотреби информационо комуникационе технологије и система.

(3) Компјутерски криминалитет представља најраспрострањенији облик транснационалног криминалитета, и он се по својим друштвеним и економским обележјима знатно разликује од традиционалног и организованог криминалитета.

(4) Компјутерски криминалитет и злоупотреба друштвених мрежа, као девијантно понашање и део компјутерског криминалитета, одликује високи степен анонимности извршилаца, стална доступност жртве и виктимизација великих размера, мултијурисдикциона природа, отежан рад органа гоњења, прикупљања доказа, пресуђивања и кажњавања.

(5) Друштвене мреже на интернету, као најраширенији и најпопуларнији начин комуникације у савременом свету, довеле су до тога да је приватни живот постао саставни део јавног живота и да не постоји никаква гаранција приватности за податке који се пласирају путем интернета и друштвених мрежа.

(6) Озбиљан недостатак коришћења друштвених мрежа представља велика изложеност корисника разним облицима злоупотребе, као што су: крађа идентитета, преваре, дигитално насиље (сексуално насиље и узнемиравање, вршњачко насиље, прогањање, сајбер мобинг, говор мржње), тероризам, вандализам, трговина људима и људским органима, пиратерија, као и замена реалног света виртуелним и патолошка зависност од коришћења и злоупотребе интернета.

(7) Предности приступа интернету и друштвеним мрежама огледају се у већој могућности за размену информација, социјалну интеграцију, личну и професионалну промоцију, упознавање људи истих схватања и интереса, стицање добити на основу успешно остварених комуникација, изградњу пословних веза и сл.

(8) Приватност је добила нову димензију, нови концепт, то је информациона приватност, која се односи на прикупљање, обраду, чување и дељење података о појединцу.

(9) Извршиоци кривичних дела компјутерског криминалитета, као и корисници који злоупотребљавају друштвене мреже и њихове жртве су из различитих националних, верских, расних, политичких група, из разних социјалних окружења, различитог су социјалног и правног статуса, различитог пребивалишта. Корисници интернета и друштвених мрежа су у највећем броју млађе особе, а са старошћу опада број корисника.

(10) Постојећа законска регулатива о заштити приватности и компјутерском криминалитету показује значајан напредак у Србији у односу на ранији период, али је неопходно извршити још низ промена како би се постигао већи степен заштите и безбедности корисника, и како би се превентивно деловало на сузбијање компјутерског криминалитета и злоупотребе друштвених мрежа.

Систематизација рада, поред уводног дела и закључка, обухвата пет целина – први део о праву на приватност и друштвеним мрежама, други део о злоупотреби друштвених мрежа као једном од облика компјутерског криминалитета, трећи део о правној регулативи за борбу против компјутерског криминалитета и криминалне активности на друштвеним мрежама, четврти део о превенцији и мерама заштите од компјутерског криминалитета на друштвеним мрежама и пети део који садржи резултате емпиријског истраживања. Осим тога, у раду је садржан и речник основних компјутерских појмова, подаци о хронолошком настанку и врстама друштвених мрежа, индекс појмова и списак коришћене литературе.

У првом делу посебна пажња је посвећена појму и садржини права на приватност уопште, информационе приватности, као и права на приватност корисника друштвених мрежа. Дат је приказ правног оквира заштите права на приватност у Републици Србији, кључних теоријских приступа друштвеним мрежама, као и политике приватности на најчешће коришћеним друштвеним мрежама (Facebook, Twitter и LinkedIn). Такође, наведена су интернет права и принципи за заштиту људских права, безбедносни ризици на друштвеним мрежама и препоруке за њихово смањивање.

Други део рада *„Злоупотреба друштвених мрежа као облик компјутерског криминалитета“* садржи четири целине: Појам, појавни облици и остале феноменолошке карактеристике компјутерског криминалитета; Обележја извршилаца кривичних дела компјутерског криминалитета – „хакера“, злоупотреба друштвених мрежа као девијантно понашање и најчешћи узроци компјутерског криминалитета и криминалних активности на друштвеним мрежама. Посебна пажња је посвећена појму злоупотребе друштвених мрежа и облицима испољавања: крађа и злоупотреба идентитета, прогањање преко интернета, сексуално насиље, сексуална експлоатација и сексуално злостављање деце, вршњачко насиље, сајбер мобинг, говор мржње на друшвеним мрежама, преваре путем интернета, трговина људима и трговина људским органима, интернет (сајбер) тероризам, интернет вандализам, злоупотреба фотографија.

У *трећем делу* приказана је међународна и домаћа правна регулатива за борбу против компјутерског криминалитета и различитих криминалних активности на друштвеним мрежама, као и санкционисање различитих појавних облика компјутерског криминалитета. Такође, дат је и компаративни преглед правног регулисања компјутерског криминалитета у земљама бивше СФРЈ.

У четвртом делу наведене су мере превенције и заштите од компјутерског криминалитета на друштвеним мрежама. Приказане су и анализиране главне препоруке за сузбијање и спречавање повреде приватности на друштвеним мрежама, које су резултирале из емпиријског дела рада.

Пети део заснован је на приказу емпиријског истраживања случајно одабраног узорка корисника/корисница друштвених мрежа. Описан је предмет, циљ и метод истраживања, дефинисан узорак и упитник као инструмент за прикупљање података и приказани су резултати истраживања. Значај емпиријског дела рада је у сагледавању структуре корисника друштвених мрежа, података који корисници најчешће наводе у својим „профилима“, као и ставова корисника о могућностима за повреду њихове приватности.

На крају рада, уз закључак, посебну целину у раду представљају: објашњење појмова који се најчешће користе у тзв. компјутерском језику и интернет комуникацији и који су коришћени у раду; хронолошки настанак и врсте друштвених мрежа, као и анализа карактеристика најчешће коришћених друштвених мрежа и њихова географска (не)ограниченост и индекс појмова.

ГЛАВА I

ПРАВО НА ПРИВАТНОСТ И ДРУШТВЕНЕ МРЕЖЕ

1. Појам приватности и информационе приватности

У изворном смислу, приватност означава жељу неке особе да не буде узнемиравана.[4] Приликом теоријског разматрања појма приватности и садржине тог појма у англосаксонској литератури се помињу судија Луј Брандајс (Louis Brandeis) и адвокат Семјуел Ворен (Samuel Waren), који су 1890. године у чланку „The Right to Privacy" формулисали најтачнији и најодређенији појам приватности, као „право да се буде остављен на миру" (*„right to be left alone"*).[5] Овако формулисана, приватност подразумева заштиту личне аутономије, моралног и физичког интегритета, право на избор животног стила и начина живота, интеракцију између људи и сл.

Право на приватност представља једно од основних људских права, како међународно, тако и уставно право јавноправног и грађанскоправног значаја, које делује према свима (*erga omnes*) и штити човека од узнемиравања од стране државне власти и других људи. Супротно од јавности, приватност подразумева тајност и неузнемираваност. Односи се на приватни живот појединца/појединке у коме је оправдано очекивати мир и спокојство, неометање у интими.[6] Право на приватност дозвољава појединцу да селективно приказује свету око себе онолико колико тај појединац жели.[7]

---

[4] Николић, Милан: „Практични аспекти заштите приватности корисника и безбедности електронских комуникационих мрежа и услуга у Србији", http://www.telekomunikacije.rs/arhiva_brojeva/peti_broj/milan_nikolic:_prakticni_aspekti_zastite_privatnosti_korisnika_i_bezbednosti_elektronskih_komunikacionih_mredja_i_usluga_u_srbiji_.305.html, претражено 15. 06. 2014.године

[5] Harvard Law Review, Vol IV No 5, цит. према Шурлан, Тијана: Међународноправна заштита права на приватност, www.spmisao.rs/mp-content/uploads/2014/03-tijana-surlan-pdf. претражено 28. 10. 2015. године

[6] Сурцо, Рамо: Право на приватност с посебним освртом на интернетску друштвену мрежу Facebook, www.rijaset.ba/.../05_pravo_na _privatnos... претражено 20. 10. 2015.године

[7] Јовановић, Светлана: „Приватност и заштита података на интернету", Твининг пројекат ЕУ – зборник *Везе cyber криминала са иregуларном миграцијом и трговином људима*, Министарство унутрашњих послова Републике Србије, 2014. година, стр. 94.

Теоријски појам приватности није претрпео значајније промене протеком времена. Ипак, до промена је дошло у примени овог права у савременом добу, које карактерише глобално друштво и информацијска технологија. Брзина и доступност информација, посебно електронских, угрозили су поштовање права на приватност, како од стране појединаца, тако и од стране држава.

Приватност у електронским комуникацијама обухвата прикупљање, обраду и давање информација о кориснику трећим лицима, при чему појединци/појединке када бележе активности и личне податке сами одређују када, како и у којој мери информације о њиховој приватној сфери треба и могу да буду доступне другима.[8] Поједини аутори[9] приватност дефинишу као сложен појам, који обухвата личну аутономију, демократску партиципацију, управљање сопственим идентитетом и друштвену координацију. Централно место ове мултидимензионалне конструкције чини жеља да се лични подаци задрже за себе и да други људи не дођу до њих.

Савремени комуникациони системи могу у потпуности да испуне своју улогу уколико су поуздани и у служби и на располагању корисницима. Поверљивост информација које корисници деле у виртуелном простору са другима не сме да буде угрожена, а корисници морају да буду сигурни у идентитет пошиљаоца, и у то да примљена информација мора да буде идентична послатој. Свако одступање од овог правила умањује поверење корисника.

Лична добра попут живота, слободе, имена, части и угледа, сматрана су неодвојивим делом личности. У права личности спада и право на приватност, којим се од објављивања у јавности штите подаци и записи везани за нечији приватан живот. Човек заправо не штити само декларативно своја лична добра јер на њих има апсолутно право, већ их штити од напада, како од стране друштвене заједнице, тако и од појединих физичких, или правних лица.

Појам „приватност“ се често користи у обичном језику, као и у филозофским, политичким и правним дискусијама, али и даље не постоји

---

http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/Cyber%20kriminal,%20iregularne%20migracije%20i%20trgovina%20ljudima.pdf, претражено 23. 07. 2015. године

[8] *Ibid.*

[9] Cho, Hichang, Rivera-Sánchez, Milagros, Lim, Sun Sun: „A Multinational Study on Online Privacy: Global Concern and Local Responses. New Media & Society”, vol.11, 2009., стр. 395-416, http://nms.sagepub.com/content/11/3/395.short, претражено 12. 11. 2014.године

јединствена дефиниција, или опште прихваћено значење овог појма. Концепт права на приватност има добро познате историјске корене у Аристотеловим делима, када је он први покушао да дефинише приватност као све оно што је везано за породицу и човека, а стоји насупрот политичне активности, као "јавне ствари".[10] Приватност се често третирала као *интерес* који има изражену моралну вредност, док је понекад била дефинисана и као морално или законско *право* појединца да буде заштићен од стране друштва или закона.[11]

Постоји доста критика овако дефинисаног права на приватност. Према једној од критика, право на приватност не постоји, јер било који интерес који се штити као приватни интерес може да буде једнако добро заштићен неким другим правом, а најпре својинским или имовинским правом и правом на телесни интегритет и безбедност.[12] Друга критика се позива на тврдњу да је право на приватност, које жели да се заштити, економски неисплативо,[13] тј. као право чија заштита није заснована на било којој познатој правној доктрини.[14] Трећа критика је феминистичка критика права на приватност, која се позива на постулат да је посебно наглашавање потребе заштите права на приватност заправо штетно за жене, јер се овим правом манипулише, како би се жене контролисале и биле под сталном доминацијом мушког пола, под привидом жеље за њиховом заштитом.[15]

Приватност може да се сагледа и дефинише из различитих аспеката: као политичко право, као грађанско право и као право које постоји да би штитило

---

[10] Privacy: Stanford Encyclopedia of Philosophy, 2002, http://plato.stanford.edu/entries/privacy/, претражено 16. 02. 2015.године

[11] *Ibid.*

[12] Thomson, Judith Jarvis: "The Right to Privacy", Philosophy and Public Affairs, 4: 295–314, 1975., http://www.eecs.harvard.edu/cs199r/readings/thomson1975.pdf, претражено 18. 02. 2015.године

[13] Posner, Richard :"The Economics of Justice", Cambridge: Harvard University Press, 1981, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2449&context=faculty_scholarship, претражено 18. 02. 2015.године

[14] Bork, Robert :"The Tempting of America: The Political Seduction of the Law", New York: Simon and Schuster, 1990, http://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1896&context=lawreview, претражено 18. 02. 2015.године

[15] MacKinnon, Catharine: „Toward a Feminist Theory of the State", Cambridge: Harvard University Press, 1989, http://books.google.co.uk/books/about/Toward_a_Feminist_Theory_of_the_State.html?id=Shn5xHywtHIC претражено 18. 02. 2015.године

интересе грађана.[16] Као политичко право, право на приватност може да се дефинише као "сигурност грађана да држава неће да се уплиће у њихове личне ствари".[17] Приватност као грађанско право не подразумева сакривање ствари, већ контролисање нечег што припада тој особи, њену аутономију и интегритет,[18] односно "право човека да контролише који ће се детаљи његовог живота сазнати".[19] У погледу ограничења права на приватност битно је до које границе се може откривати приватност једне особе, а да се притом не повреди њено право на приватност. Сматра се да је *противправност* она граница која се не сме прећи приликом коришћења података из приватне сфере појединца. Приватност може да се дефинише као право појединца на заштиту од упада у његов лични живот или послове, живот његових чланова породице, било директно одређеним радњама или објављивањем личних информација.[20]

Право на приватност, као индивидуално право, може да се схвати као контрола, измена, управљање и брисање информација о себи самом када сама особа то одлучи.[21] У контексту друштвених мрежа, приватност и личне информације обухватају све податке које једна индивидуа објављује на свом профилу, а које подразумевају слике, коментаре, податке о кретању и дружењу

---

[16] Barnes, Susan: "A privacy paradox: Social networking in the United States", часопис "First Monday", volume 11, number 9, 2006., http://firstmonday.org/article/view/1394/1312, претражено 23. 05. 2014. године

[17] Schement,Jorge Reina, Curtis, Terry: " Tendencies and tensions of the information age: The production and distribution of information in the United States", New Brunswick, N.J.: Transaction Publishers, 1995., стр.136, https://books.google.rs/books?id=PzlLOqLko5cC&pg=PR4&lpg=PR4&dq=Tendencies+and+tensions+of+the+information+age:+The+production+and+distribution+of+information+in+the+United+States%22,+New+Brunswick,+N.J.:+Transaction+Publishers,+1995&source=bl&ots=m-IJ9Z-5XE&sig=iEzjOOcvhpLvlXy9EAH1lM71OIA&hl=sr&sa=X&ei=j7HHVP63JKnlywO2z4CIBw&ved=0CCcQ6AEwAg#v=onepage&q=Tendencies%20and%20tensions%20of%20the%20information%20age%3A%20The%20production%20and%20distribution%20of%20information%20in%20the%20United%20States%22%2C%20New%20Brunswick%2C%20N.J.%3A%20Transaction%20Publishers%2C%201995&f=false претражено 15. 01. 2015. године

[18] Garfinkel, Simson: "Database nation: The death of privacy in the 21st century", Sebastopol, Calif.: O'Reilly, 2000., страна 4, http://monoskop.org/images/3/3f/Garfinkel_Simson_Database_Nation_The_Death_of_Privacy_in_the_21st_Century.pdf, претражено 15. 01. 2015. године

[19] *Ibid.*

[20] Shah, Mahmood: "Online Social Networks: Privacy Threats and Defenses", Springer, vol. XVI, 2013., http://www.springer.com/978-3-7091-0893-2, претражено 12. 02. 2015. године

[21] Westin, Alan.: "Privacy and Freedom", Bodley Head, London, 1970, http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr, претражено 18. 02. 2015. године

и слично. [22] Овако посматрано, могућност злоупотребе права на приватност на друштвеним мрежама може да се сагледа кроз две концептуалне категорије: друштвену злоупотребу или организациону злоупотребу права.[23]

Приватност може да се подели на просторну, комуникацијску и информациону приватност.[24] *Просторна приватност* се односи на приватност у оквиру сопственог дома и другог простора у коме особа води сопствени живот одвојено од других. Овај облик приватности обухвата поштовање права на сопствени простор, како у оквиру дома и породице, тако и на радном месту. *Комуникацијска приватност* се односи на дописивање, и остале облике комуникације са другим људима.

Информациона приватност је повезана са развојем информационих технологија и односи се на прикупљање података о особи, управљање тим подацима и њихово коришћење. Схваћена у ужем смислу, информациона приватност представља захтев појединаца, група или институција да самостално одлуче када ће, како и које информације о себи уступити другима.[25] У ширем смислу, појам информационе приватности обухвата *информациону сигурност,* што подразумева да појединац у условима постојања информационог друштва одлучује када, коме, колико и како ће да саопшти личне податке, водећи рачуна о својим правима и потребама, као и о правима и потребама заједнице у којој живи.[26] Информациона приватност обједињује правне вредности заштите права појединаца у друштву развијених информационих технологија, а овај концепт заштите личних података, везан за комуникацију преко електронских мрежа, другачије се назива и "е-приватност".[27]

---

[22] King, Jennifer, Lampinen, Airi, Smolen, Alex: " Privacy: Is There An App for That?", Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2011, https://www.truststc.org/pubs/864.html, претражено 23. 11. 2014. године

[23] Krasnova, Hanna, Gunther, Oliver, Spiekermann, Sarah, Koroleva, Ksenia:"Privacy concerns and identity in online social Networks", Identity in the Information Society, vol. 2, no.1, 2009, стр.39-63. http://download.springer.com/static/pdf/675/art%253A10.1007%252Fs12394-009-0019-1.pdf?auth66=1424106684_18f9ff6659fd034e563c2b1309efc0ba&ext=.pdf, претражено 23. 11. 2014. године

[24] Бобан, Марија: „Право на приватност и право на приступ информацијама у савременом информацијском друштву", Зборник радова Правног факултета у Сплиту, год. 49, 3/2012., стр. 595, http://hrcak.srce.hr/file/129212, претражено 06. 08. 2015.године

[25] *Ibid.,* стр. 581.

[26] Бобан, Марија, *op.cit.,* 2012., стр. 582.

[27] *Ibid.*, стр. 585.

Право на информациону приватност обухвата право на обавештеност, право на одговарајуће коришћење података, право приступа и увида (право контроле), право исправке и право на правна средства.[28]

Право на приватност, као индивидуално право, може да се схвати као контрола, измена, управљање и брисање информација о себи самом када сама особа то одлучи.[29] У контексту друштвених мрежа, приватност и личне информације обухватају све податке које једна индивидуа објављује на свом профилу, а које подразумевају слике, коментаре, податке о кретању и дружењу и слично. [30] Овако посматрано, могућност злоупотребе права на приватност на друштвеним мрежама може да се сагледа кроз две концептуалне категорије: друштвену злоупотребу, или организациону злоупотребу права.[31]

Друштвена (интерперсонална) злоупотреба може да се односи на индивидуе које користе друштвене мреже и које неовлашћено "преносе" и "шире" туђе личне поверљиве податке другим лицима (нпр. када неко, користећи свој статус пријатеља неког корисника, његове податке преноси неком трећем лицу или могућем послодавцу).

Организациона (институционална) злоупотреба је наметнута прихватањем правила саме друштвене мреже, јер су овде претње по приватност корисника компаније које одржавају постојање друштвене мреже и њене сервисе и платформе (нпр. продаја личних података о корисницима рекламним компанијама).

Упркос свакодневном развоју информационих технологија и нових појавних облика могућих злоупотреба, корисници интернета очекују да сваки информациони систем мора да одбије нападе који имају капацитете за његово угрожавање. Такође, тешкоћу представља и то што корисници добровољно и самоиницијативно на интернету објављују велики број својих личних података, без размишљања о томе да ли ће ови подацу бити злоупотребљени или не. Најчешћи начини непоштовања права на приватност на интернету су неовлашћен приступ, прикупљање и обрада личних података корисника,

[28] Дракулић, Мирјана: „Основи компјутерског права", Друштво операционих истраживача Југославије – ДОПИС, Београд, 1996., стр.65, наведено код Јовановић, Светлана, *op.cit.,* 2014., стр. 97
[29] Westin, Alan, *op.cit.,* 1970, стр. 97
[30] King, Jennifer, Lampinen, Airi, Smolen, Alex, *op.cit.,* 2011, стр. 97
[31] Krasnova, Hanna, Gunther, Oliver, Spiekermann, Sarah, Koroleva, Ksenia, *op.cit.,* 2009, стр. 97

злоупотреба прикупљених података, пресретање послатих информација и сл. Ипак, према извештају Европске комисије о интернет сигурности грађана Европе из 2012. године,[32] већина испитаника се изјаснила да је променила своје понашање приликом коришћења интернета, јер више не дају своје личне податке нити отварају електронску пошту, која им долази од непознатих људи и чија им се садржина чини сумњивом. Једна половина испитаника је изјавила да је у периоду од годину дана више пута променила своје шифре из безбедносних разлога, а посебно због повећања сигурности личних података и новчаних трансакција које су извршене преко интернета. Једна трећина испитаника је рекла да је бар једном до сад примила електронску поруку коју би могли да сматрају интернет преваром, покушајем потенцијалне крађе идентитета, покушајем хаковања налога на некој од друштвених мрежа, или потенцијалним злостављањем, или сексуалним узнемиравањем.

1.1. Право на приватност и право на информисаност

Коришћење информационо комуникационих технологија захватило је сва подручја живота људи, њиховог рада, забаве и бројних других приватних и пословних активности, тако да је скоро све у друштву постало on line, почев од потписивања уговора до вршења кривичних дела. Уз помоћ интернета и других пратећих технологија друштво се трансформише кроз три специфична подручја: приватност, слобода изражавања и слободан проток информација. Друштвене промене у савременом друштву, које се односе на информационо комуникационе технологије, седамдесетих година прошлог века утицале су на сагледавање једног новог феномена – информатичког друштва. Информације постају важан елемент слободе и права на ширење информација, које у великој мери зависи од легитимности и могућности управљања збиркама података.[33] У модерном информатичком друштву технолошки напредак омогућава обраду, чување, приступ и пренос информација у било ком облику, независно од удаљености, времена и количине. И поред тога што данас не постоји општеприхваћена дефиниција појма „информатичког друштва“, у литератури се

[32] European Commission - Special Eurobarometer 404: CYBER SECURITY REPORT, 2013., стр. 89, http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf, претражено 15. 07. 2015. године
[33] Бобан Марија, *op.cit.* стр. 576.

наводе три конституционална елемента информатичког друштва: информација и знање; пролиферација информатичке и комуникационе технологије; приступ и коришћење информатичке и комуникационе технологије.[34] Информација је податак који се користи и који за примаоца има одређен ефекат, односно значење. Да би била корисна, информација, поред осталог, мора бити тачна, исправна, потпуна, једноставна, поуздана и благовремена. Информисање или проток информација значајно је како са социолошког, тако и са психолошког и правног аспекта, па је право на јавно информисање, као и право на приватност, основно људско право, самостално право у групи права везаних за слободу личности, које је гарантовано како међународним тако и националим прописима, пре свега уставом.

Када говоримо о праву на приватност морамо да истакнемо да се насупрот овог права сагледавају право на информисаност и право на приступ информацијама који не би требало да угрожавају право на приватност. Законско регулисање ова два права треба да доведе до њихове избалансираности и несупротстављања. У појединим случајевима постоји легитиман интерес јавности да има увид у одређене информације и легитиман интерес грађана да буду „остављени на миру“, односно да податке о себи учине недоступним јавности. У таквим случајевима потребно је проценити ком принципу треба дати предност, али на такав начин да се други принцип афирмише у највећој могућој мери.

Право на информисаност регулисано је у Србији Уставом Републике Србије[35] и Законом о јавном информисању и медијима,[36] којим су постављена ограничења права на приватност, како слобода изражавања и право на информисаност не би били несразмерно ограничени. Устав Републике Србије гарантује право на обавештеност (чл. 51), што значи да свако има право да истинито, потпуно и благовремено буде обавештаван о питањима од јавног значаја и да свако, у складу са законом, има право на приступ подацима који су у поседу државних органа и организација којима су поверена јавна овлашћења. Према одредбама Закона о јавном информисању и медијима (чл. 1), јавно

[34] Ален, Рајко: „Информацијско управно право“, Хрватска јавна управа, год. 9 (2009) бр.1 стр. 174.
[35] Устав Републике Србије („Службени гласник РС“ бр. 98/2006)
[36] Закон о јавном информисању и медијима („Службени гласник РС“ бр. 83/2014, 58/2015)

информисање се остварује путем медија. Правила о јавном информисању обезбеђују и штите изношење, примање и размену информација, идеја и мишљења путем медија у циљу унапређивања вредности демократског друштва, спречавања сукоба и очувања мира, истинитог, благовременог, веродостојног и потпуног информисања и омогућавања слободног развоја личности (чл. 2 – циљ законског регулисања). Предмет законског регулисања су, поред осталог, информације о личности и њеном приватном животу, као и изузеци од правила обавезног пристанка за објављивање података из приватног живота. Када се ради о заштити приватности, приватног живота и личних записа, Закон о јавном информисању и медијима предвиђа да се информација из приватног живота, односно лични запис (писмо, дневник, забелешка, дигитални запис и сл) не може објавити без пристанка лица чијег се приватног живота информација тиче, односно лица чије речи, лик, односно глас садржи, ако се при објављивању може закључити које је то лице, ако би објављивањем било повређено његово право на приватност или које друго право. Посебно су заштићени малолетници одредбом да се не смеју учинити препознатљивим у информацији која може да повреди њихово право или интерес (чл. 80).

Међутим, ради остваривања слободе изражавања и права на информисаност, у Закону је наведена дуга листа изузетака од овог правила, када није потребан пристанак на објављивање, чиме се постављају ограничења права на приватност и чине доступним подаци из приватног живота појединаца уколико, како Закон предвиђа (чл. 82), у конкретном случају интерес јавности да се упозна са информцијом односно записом претеже у односу на интерес да се спречи објављивање. Пристанак за објављивање није потребан у следећим случајевима: ако је лице информацију, односно запис, наменило јавности, односно доставило медију у циљу објављивања; ако се информација, односно запис, односи на личност, појаву или догађај од интереса за јавност, посебно ако се односи на носиоца јавне или политичке функција, а објављивање информација је у интересу националне безбедности, јавне сигурности или економске добробити земље ради спречавања нереда или злочина, заштите здравља или морала или заштите права и слободе других; ако је лице својим јавним изјавама, односно понашање, у приватном, породичном или професионалном животу привукло пажњу јавности и на тај начин дало повода за објављивање информације, односно записа; ако је информација саопштена,

односно ако је запис начињен у јавној скупштинској расправи или у јавној расправи у неком скупштинском телу; ако је објављивање у интересу правосуђа, националне безбедности или јавне безбедности; ако се лице није противило прибављању информације, односно прављењу записа, иако је знало да се то чини ради објављивања; ако је објављивање у интересу науке или образовања, ако је објављивање потребно ради упозорења на опасност (спречавање заразне болести, проналажење несталог лица, спречавања преваре; ако се запис односи на мноштво ликова или гласова (навијача, концертне публике, демонстраната, уличних пролазника и сл.); ако се ради о запису са јавног скупа; ако је лице приказано као део пејзажа, природе, панораме, насељеног места, трга, улице или као део сличног призора.

Последњих неколико година у феминистичкој литератури се доста расправља о слободи изражавања, информисаности путем интернета и друштвених мрежа, интернетској цензури, као и о томе како информатичко комуникациона технологија (ИКТ) утиче на информисаност о женским правима. Информатива технологија ипак није родно неутрална јер су због културолошких предрасуда жене често искључене из процеса развоја технологије и њене примене. Бољи приступ информацијама и умреженост коју пружа ИКТ могли би значајно да допринесу процесу економског оснаживања жена, супротстављању патријархарту и *on line* насиљу и стварању праведнијег друштва. Због тога су на 59. заседању Комисије Уједињених Нација о положају жена у извештају организације APC (Association for Progressive Communication) као основни циљеви WRC (Women's Rights Programme) истакнути и борба за слободу говора жена, спречавање „технолошког насиља“ над женама, супротстављање негативним последицама информатичко технолошког развоја и извештавање у медијима на начин да се не угрожава њихова приватност. Такође је констатовано да је приватност значајан сегмент у борби за права жена и да цензурисање информација о сексуалном здрављу, репродуктивним правима и насиљу над женама спречава жене у остваривању права гарантованих међународним документима.

У дигиталном свету женска приватност је значајно угрожена и повезана са новим и застрашујућим облицима *online* насиља. Посебно су новинарке и

блогерице изложене озбиљним облицима *online* узнемиравања, сексуалног и насилног карактера, које се често оправдава слободом говора.[37] Истраживања показују да су у дигиталном окружењу новинарке три пута чешће мета врло агресивних коментара него њихове мушке колеге.[38] Као учеснице у јавном говору и информисању, изношењу свог мишљења и става, новинарке су често изложене претњама, сексуалном узнемиравању, cyber сексизму и cyber ухођењу, што показује да је у online комуникацији веома видљив тренд родне неједнакости.[39] Претње, увредљиви коментари, агресивно понашање и омаловажавања који се у бруталним облицима јављају на мрежи имају за циљ, поред осталог, да жене, али и све људе из маргиналних група, који су дискриминисани, уклоне из дигиталог простора. Због тога је веома важно да друштвене мреже предузму одређене мере у спречавању ових појава, али и да се гради феминистички покрет offline и online, који ће се залагати за заштиту приватности и објективну информисаност.

[37] Вујновић, Андреа: "Како информацијско-комуникацијска технологија утјече на женска права", Vox Feminae 3-8/11/2015, http://www.voxfeminaes.net/feministyle/item/7420-kako-informacijsko-kominikacijska-tehnologija-utječe-na-ženska-prava, претражено 02. 11. 2015. године

[38] Жикић, Биљана: " О online комуникацији: интервју са др Снјежаном Миливојевић", Српски културни центар "Данило Киш", http://dkis.si/o-online-komunikaciji-intervju-sa-prof-dr-snjezanom-milivojevic/, претражено 08. 11. 2015. године

[39] Новинаркама се сликовито описује шта ће им се десити: силовање, убиство, напад на децу и друге чланове породице. Emma Watson је одмах пошто је наступила у Уједињеним Нацијама у кампањи He For She добила претње да ће јој објавити наге фотографије. Британска новинарка и феминисткиња Caroline Criado-Perez покренула је јавну акцију да се на британским новчаницама појаве жене, после чега је била изложена таквој online кампањи да је угасила свој Twiter налог, јер више није могла да поднесе вулгарне претње да ће бити убијена, масакрирана и описе силовања коме ће бити изложена. Азарбејџанска новинарка је сличне претње добијала као 'национална издајица' и оне су укључивале опис силовања и место где ће бити закопана када буде убијена. *Ibid.*

1.2. Право на приватност као основно људско право – међународноправна регулатива

Право на приватност, као основно људско право, има посебан значај у корпусу људских права. Међународноправни нормативни оквир права на приватност чини неколико међународних докумената. Они заједно образују општи нормативни оквир за конституисање и разумевање права на приватност, али се међусобно разликују у начину примене, тумачењу и санкционисању. Заштита права на приватност на међународном и националном нивоу односи се на приватну сферу живота, породични живот, неповредивост дома и преписке, части и угледа појединца. **Универзална декларација о људским правима** (1948) је први свеобухватни документ о људским правима, који је Генерална скупштина Уједињених нација усвојила као резолуцију. Ипак, иако Универзална декларација није била упућена државама на ратификацију, несумњив је њен утицај на касније донете међународне конвенције о људским правима и унутрашње правне системе држава. У чл. 12 Универзалне декларације прописано је да „нико не сме бити изложен произвољном мешању у његову приватност, породицу, дом или преписку, нити нападима на част или углед. Свако има право на заштиту закона против оваквог мешања или напада“.[40] **Међународни пакт о грађанским и политичким правима** (1966)[41] такође садржи одредбе о заштити права на приватност, јер у чл. 17 предвиђа да „нико не може бити предмет самовољних или незаконитих мешања у његов приватни живот, његову породицу, у његов стан или његову преписку, нити незаконитих повреда нанесених његовој части или његовом угледу”.

Европска конвенција за заштиту људских права и основних слобода (Рим, 1950)[42] је најважнији међународноправни документ о људским правима на тлу Европе, који уз донете Протоколе, утврђује најсвеобухватнији и најефикаснији систем заштите људских права и основних слобода. С обзиром на то да приватан живот представља приватну сферу, право је човека да живи како

[40] „Повереник” - www.poverenik.rs, Правни оквир, Међународни документи, претражено 12. 10. 2015. године
[41] Међународни пакт о грађанским и политичким правима (1966) (“Службени лист СФРЈ“ бр. 7 од 04. 02. 1971)
[42] Европска конвенција за заштиту људских права и основних слобода (Рим, 1950), („Службени лист СЦГ“ Међународни уговори бр. 9/2003)

жели, заштићен од јавности и напада на духовни и морални интегритет, као и право да успоставља комуникације са другим људима и емотивне везе ради задовољења сопствених потреба и развоја личности. Стога Конвенција као једно од основних права и слобода предвиђа право појединца на поштовање приватног и породичног живота (чл. 8). Овом одредбом Конвенције гарантује се свакоме право на поштовање приватног и породичног живота, дома и преписке, што значи да се појединцу гарантује заштита од ометања од стране власти, других појединаца и институција, укључујући и средства масовних комуникација. Као аспекти права на приватан живот појављују се: право на име, право на сексуалну оријентацију, право на тајност медицинских података, право на физички интегритет. Право на поштовање породичног живота означава право чланова породице на заједнички живот и на развијање међусобних односа. Право на поштовање преписке односи се не само на писану преписку, већ и на различите видове комуникације телефоном, факсом, електричном поштом, али и свим другим иновираним средствима комуникације и информисања у дигиталном свету.

Конвенцијом су предвиђена и одређена ограничења права на приватност. Према тексту Конвенције, јавне власти се неће мешати у вршење овог права осим ако то није у складу са законом или је неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала или ради заштите права и слобода других. На тај начин је одређен и обим приватног живота: право на поштовање приватног живота ограничава се у мери у којој појединац сам доведе свој приватни живот у додир са јавним животом или у везу са другим заштићеним интересима. Сродне гаранције права на приватност према одредбама Конвенције односе се на слободу мисли, савести и вероисповести (чл. 9) и слободу изражавања (чл. 10).

Конвенција о правима детета (1989)[43] као универзални међународни уговор, садржи одредбе о праву на приватност деце. Члан 16 Конвенције предвиђа да „ниједно дете не сме бити изложено произвољном или незаконитом

[43] Закон о ратификацији Конвенције УН о правима детета ("Службени лист СФРЈ" – Међународни уговори бр. 15/90, „Службени лист СРЈ"- Међународни уговори бр. 4/96 и 2/97)

мешању у његову приватност, породицу, дом или преписку, као ни незаконитим нападима на његову част и углед".

Према **Резолуцији Скупштине Савета Европе**,[44] која се односи на мас медије и људска права и приватни живот, наведено је да се право на приватност састоји из права појединца да живи са минимумом утицаја са стране, да се оно тиче приватног, породичног живота у дому, физичког и моралног интегритета, части и угледа, недопуштености клеветања, недопуштености изношења нерелевантних и изненађујућих чињеница, неовлашћеног објављивања приватних фотографија, заштите од објављивања информација које су као тајна саопштене појединцима.

На нивоу Европске Уније, од донетих докумената неопходно је споменути **Повељу Европске Уније о основним правима**,[45] која је усвојена 18. 12. 2000. године. Члан 8 Повеље регулише право на заштиту података о личности, а посебно је у светлу заштите података и приватности на друштвеним мрежама битан став 2 овог члана, којим је прописано да је за обраду података неопходна претходна сагласност власника личног податка.[46]

Европска Унија усвојила и неколико Директива које се односе на заштиту приватности путем заштите података о личности.

Најсвеобухватнија је **Директива 95/46/ЕС**,[47] која представља алтернативну визију заштите права на приватност, првенствено кроз заштиту појединца као потрошача, као и заштиту приватности коју угрожавају економски интереси великих корпорација и државе. Директива се односи и на податке који се аутоматски сакупљају и обрађују путем рачунарских система и на податке који су сакупљени традиционалним начинима који не захтевају

---

[44] Council of Europe, Cons.Ass; Twenty-First Ordinary session (Third Part), Text adopted (1970); Council of Europe, Collected Texts, Strasbourg, 1979; https://books.google.rs/books?isbn=9041102663, претражено 02. 11. 2015. године

[45] Повеља Европске Уније о основним правима (енгл. Charter of fundamental rights of the European Union), http://www.europarl.europa.eu/charter/pdf/text_en.pdf, претражено 15. 05. 2015. godine

[46] На овај начин, применом ове одредбе, друштвеним мрежама је забрањено да предузимају било какву радњу којом се мења сврха и циљ објављеног податка, без претходне сагласности корисника – власника личног податка.

[47] Директива 95/46/ЕС Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046, 1995, претражено 18. 02. 2015. године и http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012, претражено 18. 02. 2015. године

рачунарску обраду. Обрада података о личности је дозвољена уколико је власник податка дао свој недвосмислен пристанак, подаци су неопходни да би лице закључило одређен правни посао, испунило неку законску обавезу, поступало у јавном интересу или вршило службена овлашћења која су му дата. Лични подаци морају бити сакупљени у складу са правом и поштено, а смеју се користити само у тачно одређене прописане сврхе. Лице чији се лични подаци обрађују има право да добије све потребне информације о циљу обраде података, право да приступи својим подацима, право на приговор на обраду података као и право на правни лек уколико је по националним прописима дошло до повреде права појединца услед обраде података. Директива има за циљ да подстакне доношење националних правних прописа који би омогућили правилну заштиту прикупљених података о личности. Из једног овако схваћеног права на приватност, посебан акценат је почео да се баца и на заштиту овог права због компјутерских злоупотреба и у виртуелном простору. Примена ове директиве је у пракси веома значајна у случајевима повреде права на приватност на појединим друштвеним мрежама, од којих су најчешће повреде: непостојање недвосмислене и изричите сагласности за обраду и прикупљање података, прикупљање података без претходно дате могућности да се корисник о томе изјасни, подешавања опције приватности су на веома ниском нивоу заштите и нису лако измењива.[48]

[48] Поједини аутори су проучавали да ли је политика приватности друштвене мреже Facebook и заштита личних података који се објављују у складу са одредбама ове директиве. Како корисници немају довољно информација о политици приватности Фејсбука и како се њихови подаци примају и обрађују пре него што корисници уопште могу да реагују, повређен је чл. 6 ст. 1 (а) Директиве. Ова одредба је повређена непостојањем адекватне транспарентности у поступцима Фејсбука и упозорења корисницима. Циљ снимања, прослеђивања и сигурности о пријатељима на Фејсбуку је проблематичан и није у складу са чл. 6 ст. 1 (б) Директиве јер за прикупљање личних података и фотографија, као и за брисање налога које траје од две недеље па до 90 дана, не постоји легитиман циљ тј.сврха чувања ових података, чиме даља обрада података изгледа прекомерна. На овај начин се крше и одредбе чл. 6 ст. 1 (ц) и (д). Посебно је уочљива повреда приликом брисања корисничког профила, која заправо не омогућава брисање већ само деактивацију профила док сви подаци остају на Фејсбуковим серверима за случај да корисник жели да поново „врати" профил. Давањем начелне сагласности на обраду личних података коју корисник ове друштвене мреже даје приликом приступања мрежи је у супротности са чл. 7 (а) Директиве јер не постоји специфичнаи недвосмислена сагласност корисника. Ова одредба је повређена и аутоматским софтвером за препознавање лица са постављених фотографија и сугерисањем имена особа које се налазе на сликама. Опција „tag" (или „обележавање") такође представља грубо кршење ове одредбе. Овом опцијом Фејсбук даје могућност својим корисницима да на фотографији обележе неког другог корисника или пријатеља. Сами корисници нису у могућности да спрече некога да их „обележи" на фотографији јер се фотографије најпре објављују, а обележени корисник може да види објаву

Како је долазило до интензивног развоја телекомуникација и рачунарских обрада података о личности, па самим тим и до потребе да се прецизирају услови располагања, чувања и дистрибуције личних података,[49] Европски Парламент и Савет донели су 1997.године **Директиву 97/66/ЕС**,[50] а неколико година касније и **Директиву 2002/58/ЕС** о обради података о личности и заштити приватности у сектору електронских комуникација.[51] Директива 2002/58/ЕС спредставља допуну Директиве 95/46/ЕС у смислу приписивања боље и свеобухватније заштите права на приватност у електронским комуникацијама. Њом се утврђује оквир заштите приватности, података о личности и интегритета јавних мрежа електронских комуникација. Ова директива је допуњена 2009. године изменама које се тичу повреде тајности података о личности, употребе Интернет колачића (енгл. Cookies) и овлашћења

тек када је фотографија објављена па уклањање ознаке представља бесмислену радњу пошто су остали корисници већ имали прилике да је виде. Корисницима није дата могућност избора да ли желе да се њихови лични подаци прослеђују у рекламне сврхе. Применом опције "*Friend Finder*" од стране Фејсбука прекршен је поред чл. 6 ст. 1 (а) (б) (ц) и чл.10 Директиве, јер Фејсбук у својој политици приватности не напомиње могућност слања позива за приступање мрежи у име корисника без његове посебне сагласности. Чл. 7 (а) Директиве није испоштован ни одредбом 14.6. политике приватности Фејсбука, где је прописано да приликом промене политике приватности ове друштвене мреже "свако даље коришћење мреже након промене услова мреже представља пристанак корисника на ове услове", чиме и даље не постоји дат недвосмислен и изричит пристанак корисника нити је дато објашњење о начину и сврси коришћења сакупљених података. Повређени су и чл. 17 ст. 2, чл. 25 и чл. 26 Директиве јер сагласност и заштита података нису од стране свих земаља одређени на одговарајућем заштитном нивоу. *Видети:* Прља, Драган, Дилигенски , Андреј: "Фејсбук и заштита података у ЕУ", Страни правни живот 3/2012, Институт за упоредно право, Београд, стр. 190-220, http://www.comparativelaw.info/spz20123.pdf, претражено 12. 06. 2014. године

[49] Томић, Наташа, Петровић, Далибор: „Друштвено умрежавање и заштита приватности корисника интернета", XXVII Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају – PosTel 2009, Београд, http://postel.sf.bg.ac.rs/downloads/simpozijumi/POSTEL2009/RADOVI%20PDF/Menadzment%20procesa%20u%20postanskom%20i%20telekomuikacionom%20saobracaju/9.%20N.%20Tomic,%20D.%20Petrovic.pdf, претражено 05. 08. 2015. године

[50] Директива 97/66/ЕС Европског парламента и Савета о обради података о личности и заштити приватности у телекомуникационом сектору (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML, претражено 18.02.2015.године

[51] Директива 2002/58/EC о обради података о личности и заштити приватности у сектору електронских комуникација – Директива о приватности и електронским комуникацијама (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, претражено 18.02.2015.године

оператора да предузимају акције против емитера незатражених порука и спамовања.

Једна од претњи праву на приватност и слободном приступу информацијама на Интернету је **Трговински споразум против фалсификовања (Споразум о заштити ауторских праа на Интернету, енгл. The Anti-Counterfeiting Trade Agreement, ACTA).**[52] Циљ овог Споразума[53] је да се пооштри борба за поштовање интелектуалне својине, као и сузбијање Интернет пиратерије и фалсификата било које врсте, али су веома брзо поједине земље чланице почеле са наводима да се овим Споразумом заправо угрожавају нека од основних људских права попут права на приватност, слободе изражавања, права на лечење и приступу медикаментима и право на правично суђење.[54]

Коначан текст Споразума садржи одредбе које се односе на заштиту права интелектуалне својине које могу да доведу до доношења неадекватних националних прописа у области Интернет комуникација и on-line услуга, а које озбиљно могу да угрозе приватност и слободу изражавања корисника Интернета. Конкретно, страхује се да би одредбе Споразума могле да доведу до бројних последица, попут непоштовања основних људских права и владавине права,[55] нестандардних начина санкционисања који нису у складу са владавином права,[56] постојања сумње да постоји масовно надгледање података

---

[52] The Anti-Counterfeiting Trade Agreement – ACTA, https://www.eff.org/files/filenode/acta1105_en.pdf, претражено 20. 08. 2015. године

[53] Споразум је потписан 01. 10. 2011. године, а потписале су га следеће државе: САД, Јапан, Канада, Мароко, Нови Зеланд, Сингапур и Јужна Кореја. Споразум су током 2012. године потписале и следеће државе чланице Европске Уније: Аустрија, Белгија, Бугарска, Чешка Република, Данска, Финска, Француска, Грчка Мађарска, Ирска, Италија, Летонија, Литванија, Словенија, Луксембург, Малта, Пољска, Португал, Румунија, Шпанија, Шведска и Уједињено Краљевство. *Видети:* Stop ACTA, http://www.stopacta.info/, претражено 20. 08. 2015. године

[54] Малетић, Варвара, Дакић, Јелена: „Интернет, социјалне мреже и људска права“, INFOTEH-JAHORINA Vol. 11, 2012., стр. 774, http://infoteh.etf.unssa.rs.ba/zbornik/2012/radovi/RSS-5/RSS-5-8.pdf, претражено 06. 08. 2015. године

[55] Нпр. прослеђивање сакупљених личних података корисника Интернета појединим институцијама без претходно донете судске одлуке, *Видети:* ACTA: Updated Analysis of the Final Version, https://www.laquadrature.net/en/acta-updated-analysis-of-the-final-version, претражено 22. 08. 2015. године

[56] У чл.27 Споразум прописује обавезу држава да подрже спровођење кривичних и грађанских санкција у Интернет окружењу, што чак подразумева и полицијске процедуре и кажњавања ван регулрних судских поступака, на захтев приватних компанија које би могле овакве санкције и да спроводе. Споразум, са друге стране, не обезбеђује ефикасне правне лекове како би у овим поступцима заштитио основна права и спровођење фер суђења, у складу са принципима владавине права.

које није у складу са Повељом о људским правима,[57] подривање демократије, основних слобода и владавине права,[58] увођење оштрих начина кривичног кажњавања и сл.[59]

Споразум је у Европском парламенту изазвао приличне дискусије на тему угрожавања основних људских права, па је Европска Унија овај документ проследила Европском суду правде како би се изјаснио да ли заиста постоји могућа повреда грађанских људских права и да ли је имплементација овог Споразума у складу са темељним правима и слободама Европске Уније. Постоји неколико разлога због којих се Споразум карактерише као документ који превише задире у приватност и грађанска права потрошача а која се односе на Интернет. Пре свега, због преговора који су вођени у тајности, Споразум није прошао све одговарајуће поступке провере и усклађивања са националним и међународним документима, а прва верзија текста Споразума је званично објављена 2010. године када је било немогуће даље преговарати о спорним одредбама. Затим, земље потписнице морају да усвоје нове мере које би садржале рестриктивна правила примене одредаба Споразума како би заштитиле права корисника на слободу говора, приватност, могућност увођења иновација. Споразумом је створено наднационо тело „ACTA Komitet“ („ACTA Comitee“), који чине неизабрани чланови који надгледају имплементацију Споразума и тумаче га, без законске обавезе да буду транспарентни у случајевима које решава.[60]

[57] Споразум захтева од Интернет посредника да откривају личне податке свих оних за које помисле да су можда учинили неки орекршај, што ствара проблеме грађанима широм Европе. Управо због овога, Споразум се критикује јер даје првенство различитим државним носиоцима права, а не слободи говора, заштити приватности и осталим основним правима. Још једна од критика упућена је због постојања могућности да Споразум може да омогући да се врши неприметно надгледање милиона појединаца и корисника, без обзира на то да ли су они под сумњом или не као и систематско сакупљање података преко Интернета.

[58] Одредбе Споразума угрожавају слободу говора, права на приватност и слободе комуникација и удруживања, тако што се приоритет даје заштити приватног сектора и примени репресивних мера усмерених ка заштити интелектуалне својине, што је у супротности са Европском конвенцијом о људским правима.

[59] EDRi:Protecting digital freedom, https://edri.org/ACTAfactsheet/, претражено 22. 08. 2015. године

[60] Electronic Frontier Foundation, The Anti-Counterfeiting Trade Agreement – ACTA, https://www.eff.org/issues/acta, претражено 20. 08. 2015. године

1.3. Правни оквир заштите права на приватност у Републици Србији

1.3.1. Устав Републике Србије

Устав Републике Србије[61] у неколико чланова гарантује права која проистичу из права на приватност. Приватност обухвата, између осталог, право на неповредивост стана, право на тајност писама и пошиљки и заштиту података о личности. Према уставним одредбама стан је неповредив и нико не може без писмене одлуке суда ући у туђи стан или друге просторије против воље њиховог држаоца, нити у њима вршити претрес. Изузетно, улазак у туђи стан без одлуке суда или претресање стана без присуства сведока дозвољено је ако је то неопходно ради непосредног лишења слободе учиниоца кривичног дела или отклањања непосредне и озбиљне опасности за људе или имовину (чл. 40).

Уставом се гарантује неповредивост тајности писама и других средстава комуницирања. Одступање од овог правила дозвољено је само на одређено време и на основу судске одлуке ако је то неопхдно ради вођења кривичног поступка или заштите безбедности земље (чл.41).

У погледу заштите података о личности, Устав предвиђа да се прикупљање, држање, обрада и коришћење података о личности детаљније уређује посебним законима. Изричито је забрањена и санкционисана неовлашћена употреба личних података која није у складу са сврхом њиховог сакупљања, осим у случајевима када је то посебним законом означено као могуће. Свако лице има право да, уколико сматра да се његови подаци злоупотребљени, затражи адекватну судску заштиту (чл. 42).

1.3.2. Закон о заштити података о личности

Закон о заштити података о личности (ЗЗПЛ)[62] уређује услове за прикупљање и обраду података о личности, права лица и заштиту права лица чији се подаци прикупљају и обрађују, предвиђа ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности,

[61] Устав Републике Србије („Службени гласник РС” бр. 98/2006)
[62] Закон о заштити података о личности („Службени гласник РС” бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012)

обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона (чл.1).

У чл. 3 Закона дефинисан је појам података о личности, који представља сваку информацију која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и сл), по чијем налогу, у чије име, односно за чији рачун је информација похрањена, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и сл, односно посредно, путем увида у документ у којем је информација садржана и сл), или без обзира на друго својство информације.

Циљ Закона је да приликом обраде података о личности сваком физичком лицу, без обзира на држављанство и пребивалиште, расу, године живота, пол, језик, вероисповест, политичко и друго уверење, националну припадност, социјално порекло и статус, имовинско стање, рођење, образовање, друштвени положај или друга лична својства. обезбеди остваривање и заштиту права на приватност и осталих права и слобода (чл.2). У Закону је изричито наглашено да се одредбе Закона не примењују када се ради о подацима који су доступни свакоме и који су објављени у јавним гласилима и публикацијама (чл.5 ст.1 тач.1) и подацима које је неко лице, способно да се стара о себи, само о себи негде објавило (чл.5 ст.1 тач.4). С обзиром на наведене одредбе, може се закључити да је закон немогуће применити на заштиту корисника друштвених мрежа приликом злоупотребе објављених личних података од стране неког трећег лица.

У чл. 8 предвиђено је да обрада података није дозвољена када физичко лице није дало пристанак за обраду података, када се обрада података врши без законског овлашћења, када је начин обраде недозвољен или када није јасна сврха обраде. Под обрадом података подразумева се свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са

наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин. На овај начин Закон ипак оставља могућност заштите личних података који су објављени а за које не постоји изричито дат пристанак, што је у потпуности у складу са забраном прописаном у чл.146 Кривичног законика којим је санкционисано неовлашћено прикупљање личних података.

Обраду података без пристанка лица које је податке објавило Закон дозвољава само када је неопходно заштитити нечији живот, здравље или физички интегритет, као и у сврху поштовања правних прописа (чл.13).

1.3.3. Закон о слободном приступу информацијама од јавног значаја

Закон о слободном приступу информацијама од јавног значаја (ЗСПИЈЗ)[63] уређује права на приступ информацијама од јавног значаја којима располажу органи јавне власти, ради остварења и заштите интереса јавности да зна и остварења слободног демократског поретка и отвореног друштва. Овим законом се такође установљава се Повереник за информације од јавног значаја као самосталан државни орган, чија је дужност, поред остало, да прати поштовање обавеза органа власти у вези прикупљања информација од јавног значаја и да о томе извештава јавност и Народну скупштину. Закон дефинише шта се сматра информацијом од јавног значаја наглашавајући да је то инфомација којом располаже орган јавне власти, настала у раду или у вези са радом органа јавне власти, садржана у одређеном документу, а односи се на све оно о чему јавност има оправдан интерес да зна. При томе, како се наводи у закону, да би се нека информација сматрала информацијом од јавног значаја, није битно да ли је извор информација орган јавне власти или неко друго лице, није битан носач информација (папир, трака, филм, електронски медији и сл.), датум настанка информације, начин сазнавања инфомације, као и друга слична својства.

Законом о слободном приступу информацијама од јавног значаја штити се приватност и друга права личности на тај начин што орган власти тражиоцу информација онемогућава остварење права на приступ информацијама од јавног значаја ако тражилац злоупотребљава то право, ако је тражење неразумно или

[63] Закон о слободном приступу информацијама од јавног значаја („Службени гласник РС” бр. 120/2004, 54/2007, 104/2009 и 36/2010)

се тражи превелики број информација (чл. 13). Осим тога, предвиђено је да орган власти неће дозволити тражиоцу информације да оствари право на приступ информацијама од јавног значаја уколико би се тиме повредило право на приватност, право на углед или неко друго право лица на које се тражена информација лично односи (чл. 14 ст.1). Остала искључења и ограничења слободног приступа информацијама од јавног значаја односе се на случајеве кад би се остварењем права на приступ информацијама од јавног значаја: угрозио живот, здравље, сигурност или неког друго важно добро неког лица; угрозило, омело или отежало спречавање или откривање кривичног дела, оптужења за кривично дело, вођење преткривичног поступка, вођење судског поступка, извршење пресуде или спровођење казне или неког другог правног поступка, фер поступања и правичног суђења; озбиљно угрозила одбрана земље, национална или јавна безбедност или међународни односи; битно умањила способност државе да управља економским процесима у земљи или битно отежало остварење оправданих економских интереса; повредило чување државне, пословне или друге тајне (чл. 9).

Истовремено, предвиђен је и изузетак од права на приватност и друга права личности у три случаја: ако је лице на то пристало; ако се ради о личности појави или догађају од интереса за јаност, а нарочито ако се ради о носиоцу државне и политичке функције и ако је информација важна с обзиром на функцију коју то лице врши; ако се ради о лицу које својим понашањем, нарочито у вези са приватним животом, дало повода за тражење информације (чл.14 ст. 2).

1.3.4. Закон о електронским комуникацијама

Електронска комуникација, као умрежени систем протока информација и електонских комуникационих односа, правно је регулисана Законом о електронским комуникацијама.[64] У Закону је дефинисан низ појмова који се односе на електронске комуникације (*Значење појединих израза* чл. 4) Тако је интернет у склопу електронске комуникационе мреже дефинисан као глобални електронски комуникациони систем сачињен од великог броја међусобно

[64] Закон о електронским комуникацијама („Службени гласник РС” бр. 44/2010, 60/2013 – одлука УС и 62/2014)

повезаних рачунарских мрежа и уређаја, који размењују податке користећи заједнички скуп комуникационих протокола (чл. 4 тач. 15). Као један од основних циљева и начела регулисања односа у области електронских комуникација, наведено је обезбеђивање високог нивоа заштите података о личности и приватности корисника, у складу са Законом о заштити података о личности и другим законима (чл. 3 тач. 12). У том смислу Закон великим бројем одредби регулише питање приватности, личних подака у електронској комуникацији, достављање података и заштиту тајности, безбедност и интегритет јавних комуникационих мрежа и услуга, тајност електронских комуникација, законито пресретање и задржавање података и др.

У погледу достављања података и заштите тајности, предвиђено је низ обавеза оператора, који је дужан да, на захтев Агенције за електронске комуникације, достави све податке и информације неопходне ради обављања послова из надлежности Агенције, посебно оне који су потребни за обезбеђивање заштите података о личности и приватности корисника, процењивање безбедности и интегритета електронских комуникационих мрежа и услуга, укључујући политике безбедности, обезбеђивања континуитета рада и заштите података (чл. 41 тач. 8). Посебно су наведене обавезе оператора према кориснику (претплатник, прималац) у погледу незатражених порука (чл. 118). Закон полази од принципа да је коришћење система електронске комуникације (систем за аутоматско позивање и комуникацију без људске интервенције, факса, електронске поште, друге електронске поруке) допуштено само уз претходни пристанак корисника. Због тога је оператор обавезан да кориснику система омогући филтрирање незатражених, шкодљивих електронских порука, као и једноставан начин за подешавање или искључивање филтера (чл. 119). Осим тога, оператор је дужан да јавно објави електронску адресу за пријављивање незатражених и шкодљивих електронских порука и да, по пријему доказа о незатражеим и шкодљивим порукама које су послате од стране његових претплатника, утврди чињенично стање и, у зависности од степена злоупотребе, опомене претплатника или му привремено онемогући коришћење услуге и о томе га без одлагања обавести. Уколико дође до поновљене злоупотребе, оператор има право да претплатнику трајно онемогући коришћење услуга, односно раскине уговор о коришћењу услуга.

Приватност корисника заштићена је и одредбама о обради података о саобраћају и локацији. Оператор јавних комуникационих мрежа или оператор јавно доступих електронских комуникационих услуга, који обрађује и чува податке о саобраћају претплатника и корисника (подаци неопходни за израду рачуна, оглашавање и продају услуга), дужан је да пре отпочињања обраде података обавести претплатника или корисника о врстама података који ће бити обрађивани и трајању обраде (чл. 122). Податке о локацији корисника оператор може обрађивати само под условом да се корисник учини непрепознатљивим или ако он на обраду претходно пристане, али само у оној мери и за оно време које је потребно за те сврхе (чл. 123).

Осим заштите приватности корисника, Законом о електронским комуникацијама се штити национална и јавна безбедност. Оператор је дужан да у циљу безбедности и интегритета електронских мрежа, тајности комуникација и заштите података о личности, саобраћају и локацији, примени адекватне техничке и организационе мере примерене ризицима. О ризику повреде безбедности и интегритета јавних комуникационих мрежа и услуга (неовлашћен приступ, значајан губитак података, угрожавање тајности комуникација, безбедност личних података и др.) оператор је дужан да обевести претплатнике (чл. 124).

Законом се преплатнику или кориснику гарантује тајност података и предвиђа да пресретање електронских комуникација којим се открива садржај комуникације није допуштено без пристанка корисника, осим на одређено време и на основу одлуке суда, ако је то неопходно ради вођења кривичног поступка или заштите безбедности земље. С тим у вези, предвиђено је законито пресретање електронских комуникација уз обавезу задржавања података и заштиту задржаних података (чл. 126-130).

1.3.5. Кривични законик Републике Србије

Право на приватност заштићено је и одредбама Кривичног законика Републике Србије[65] на тај начин што је инкриминисана свака повреда права на приватност од стране власти, других појединаца и институција, укључујући и

[65] Кривични законик Републике Србије ("Службени гласник Републике Србије" бр. 85/2005, 88/2005-испр., 107/2005-испр., 72/2009, 11/2009, 121/2012, 104/2013, 108/2014)

средства масовних комуникација. Код свих кривичних дела различит је објекат радње извршења (стан, просторије, лице, писмо, пошиљка, спис, снимак, рачунар), али је исти општи заштитни објекат – приватност. Кривичноправна заштита права на приватност је субсидијарне природе, што значи да се у већини случајева она примењује када се заштита приватности не може постићи другим средствима или кроз друге гране права. С друге стране, кривичноправна заштита је фрагментарна, што значи да се користи само у тежим случајевима повреде права на приватност.[66] Кривични законик конкретизује заштиту права на приватност предвиђањем појединих кривична дела којима се штите следећа права:

1. приватност веровања и исповедања вере (повреда слободе исповедања вере и вршења верских обреда – чл. 131 КЗ РС);
2. приватност дома (нарушавање неповредивости стана – чл. 139 КЗ РС и незаконито претресање – чл. 140 КЗ РС);
3. подаци о личности (неовлашћено откривање тајне – чл. 141 КЗ РС, неовлашћено прикупљање личних података – чл. 146 КЗ РС, одавање пословне тајне – чл. 240 КЗ РС, неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података – чл. 302 КЗ РС, повреда тајности поступка – 337 КЗ РС, одавање службене тајне – 369 КЗ РС);
4. приватност писама и других пошиљки (повреда тајности писама и других пошиљки – чл. 142 КЗ РС),
5. приватност разговора (неовлашћено прислушкивање и снимање – чл. 143 КЗ РС);
6. приватност лика и личног живота (неовлашћено фотографисање – чл.144 КЗ РС, неовлашћено објављивање и приказивање туђег списа, портрета и снимака – чл. 143 КЗ РС);
7. част и углед (увреда - чл. 170);
8. приватност породичног живота (изношење личних и породичних прилика – чл. 172 КЗ РС).

[66] Стојановић, Зоран: „Границе, могућност и легитимност кривичноправне заштите, савремена администрација, Београд, 1987., стр. 79-80, цит. према Синђелић, Жарко: „Право на приватност – кривичноправни, кривичнопроцесни и криминалистички аспекти", докторска дисертација, Београд, 2012., www.doiserbia.nb.rs/phd/university. aspx?-BG20107404sinđelić, приступљено 22. 10. 2015. године

2. Друштвене мреже на Интернету и приватност

2.1. Појам и развој друштвених мрежа

Проналазак и развој компјутера свакако је последица значајног развоја људске мисли и проналазаштва. Појединци, групе и државе зависе од компјутера и интернета јер на тај начин обављају или тим путем нуде највећи број својих услуга. Ипак, иако коришћење компјутера представља непроцењиву помоћ на било ком пољу рада, компјутер може да буде употребљен и за вршење кривичних дела.

Интернет се данас користи у већини земаља света и сваким даном расте број његових корисника. Према подацима о обиму коришћења интернета, од 2000. до 2008. године број корисника интернета је повећан за око 305% у односу на раније периоде, а процењује се да око 3 милијаде људи у свету на неки начин има приступ интернет мрежи.[67]

Према доступним подацима, велики је број корисника интернета широм света: у Северној Америци је регистровано око 158 милиона корисника, у Европи 95 милиона, Азији 90 милиона, Јужној Америци 14 и у Африци 3 милиона корисника.[68] У периоду од 2000-2008. године, број корисника интерета је, на пример, у Азији порастао за 406%, а у Африци за 1031%.[69] У Русији је број активних интернет корисника последњих година повећан са 3,5 на 8 милиона.[70] Број интернет корисника у Србији је четири пута порастао у односу на 2006. годину, када је у Србији било 1.400.000 корисника.[71]

Са аспекта безбедности, интернет се може посматрати као фактор угрожавања безбедности, али и као фактор успостављања нарушене безбедности. Ипак, у данашње време много чешће је коришћење интернета за

---

[67] ITU releases 2014 ICT figures: Mobile-broadband penetration approaching 32 per cent, Three billion Internet users by end of this year – подаци Специјализоване Агенције Уједињених Нација (ITU), http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.VTy_iiGqqkr, претражено 24. 04. 2015. године

[68] World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm, претражено 07. 11. 2014. године

[69] *Ibid.*

[70] *Ibid.*

[71] Жунић-Павловић, Весна, Ковачевић-Лепојевић, Марина, Ментус, Татјана: „Негативне последице социјалног умрежавања на интернету“, Комуникација и људско искуство – тематски зборник радова, Филозофски факултет Универзитета у Нишу, 2013., стр. 138

угрожавање и нарушавање безбедности. Интернет се користи за организовање терористичких акција, ширење пропаганде, неморалних садржаја, разних националистичких, дискриминаторских и других друштвено неприхватљивих идеја. У литератури су заступљена различита схватања о утицају интернета на кориснике у смислу подстицања агресивности и вршења кривичних дела уз помоћ информационих технологија. Заступљена су и таква схватања која негирају криминални утицај интернета и истичу да је његов утицај на осећања, ставове и понашање људи много више позитиван него што има етиолошки значај криминогеног фактора.

Модерни свет интернета значајно је промењен настанком друштвених јавних мрежа, које су постале једна од најпопуларнијих услуга на интернету. Виртуелни простор је раније био пун занимљивих и корисних информација, али је било веома мало могућности да се овај простор учини интерактивним и да се у креирању података активно учествује, што је омогућено појавом друштвених мрежа. Ову привилегију да објављују информације значајне за широке народне масе имао је ограничен број људи. Данас је све већа масовност корисника друштвених мрежа, али исто тако је заступљена неедукованост корисника о безбедносним ризицима и могућностима за заштиту.

Како се повећавао број и популарност друштвених мрежа, растао је и број корисника, што је довело и до појаве негативних последица и настанка посебног облика криминалитета који се манифестује преко друштвених мрежа и у виртуелном простору уопште, као и до стварања новог облика зависности – зависности од интернета и друштвених мрежа.[72] Осим тога, сматра се да су

[72] Видети „Све више зависника од друштвених мрежа“, Интернет магазин Мондо од 29. 01. 2012. године, http://www.mondo.rs/s232269/Magazin/Sve_vise_zavisnika_od_drustvenih_mreza.html, претражено 12. 05. 2013. године: У Београду је 2010. године основано дефектолошко саветовалиште “Ентера”, према чијим подацима су “гејмери” (особе које су зависне од играња видео игара, прим.аут.) некад чинили више од 90% зависника од компјутера, али да се из године у годину повећава број људи који постају зависни од друштвених мрежа, а у највећој мери друштвене мреже Facebook. Међу особама које постану зависници од компјутера највише је мушкараца, узраста од 15 до 25 година. Разноврстан садржај чини друштвене мреже погодним за стварање зависности, јер особе почињу да их стално користе и да не раде ништа друго. Забележен је и случај пацијенткиње која се лечила у овом саветовалишту због овакве зависности јер је престала да иде на посао и дала отказ. “Рекорд” по броју сати проведених за рачунаром међу особама које су се лечиле у овом саветовалишту држи мушкарац који је компјутер користио непрекидно 36 сати. Чести су случајеви зависности у којима мушкарци путем друштвених мрежа ступају у неку врсту емоционалне прељубе, јер им друштвена мрежа служи као место где дневно могу ступити у контакт са великим бројем жена и да је управо из овог разлога у овом саветовалишту у једном периоду била оформљена посебна група за терапију

друштвене мреже идеално место за губљење времена - због прекомерног коришћења друштвених мрежа долази до одлагања обавеза за касније, што може изазавати стрес, осећање кривице, губитак личне продуктивности, губитак концентрације и негодовање других због неиспуњавања одговорности и обавеза.

Претеча друштвених мрежа настала је 1978. године у Чикагу, у Сједињеним Америчким Државама, када су двојица компјутерских зналаца аматера направили нешто попут виртуелне "огласне табле" (енгл. Bulletin board system - BBS),[73] на којој су могле да се остављају поруке, обавештења и размењују информације о различитим догађајима кроз тзв. "постове". Ова година се заправо сматра годином рудименталног почетка развоја малих виртуелних заједница. Године 1992. основана је прва виртуелна заједница за студенте и младе људе, а 1997. године први пут су почели да у виртуелним заједницама настају профили корисника, да се формирају групе пријатеља а настаје и могућност корисника да комуницирају путем "ћаскања" (енгл. Chat).[74] Прва права друштвена мрежа настала је 1999. године у Великој Британији под симболичним називом "Поново окупљени пријатељи" (енгл. Friends Reunited),[75] који је указивао на разлог удруживања корисника ове мреже у виртуелна друштва – потрага за пријатељима са којима сте некада ишли у школу.

У данашње време друштвене мреже представљају начин за повезивање људи широм планете. Уз помоћ друштвених мрежа, свет је у могућности да

само за овај тип зависности. Зависник од интернета се може препознати по томе што све више времена проводи за компјутером, не може да контролише своју потребу, уколико му неко забрани да користи компјутер одлази у играонице, код деце се јављају проблеми са школом, а ако покушате да укажете особи да има проблем она ће постати агресивна или негирати проблем. Стручњаци из овог саветовалишта кажу да за дијагностификовање зависности мора да постоји најмање три од шест симптома - снажна жеља за употребом Интернета и немогућност контроле; појава апстиненцијалне кризе уколико особа није за рачунаром; пораст толеранције тј. све већег броја сати проведених пред рачунаром; прогресивно занемаривање осталих обавеза и интересовања; коришћење рачунара иако постоји свест о томе да то ствара одређене последице и жеља да се прекине и успостави апстиненција. Третирање зависности од Интернета разликује се од осталих терапија зависности по томе што пацијент иако је на одвикавању може да користи рачунар, али му није дозвољено да учествује у друштвеним мрежама, јер циљ терапије није да особа буде у доживотној апстиненцији од употребе Интернета, као што је случај код других зависности, него да се врати на ниво корисне употребе интернета.

[73] The Brief History of Social Media: Where people interact freely, sharing and discussing information about their lives, http://www2.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html, претражено 07. 02. 2015. године

[74] *Ibid.*

[75] *Ibid.*

визуализује везе између појединаца.[76] Чак иако вредност ових веза не осликава у потпуности реалан живот и стварне односе, друштвене мреже помажу да се сазнају везе између људи, како би се људи боље разумели и утврдили међусобну повезаност.[77]

У последњих неколико година, број друштвених мрежа убрзано расте јер се повећала потреба за овим видом умрежавања људи и разменом различитих садржаја путем друштвених мрежа.

У Републици Србији, подаци указују на постојање истих трендова и тенденција повећања броја друштвених мрежа и њихових корисника. Истраживање о употреби информационо-комуникационих технологија, које је урадио Републички завод за статистику почетком 2012. године у складу са "Евростат" методологијом објављено у пословном порталу Economy[78] показало је да у Србији 55,2% домаћинстава поседује рачунар,[79] што представља повећање за 3,1% у односу на 2011. годину. У истраживању је наведено да интернет прикључак поседује 47,5% домаћинстава, што чини повећање за 6,3 % у односу на 2011. годину, као и да сваки дан више од 2.100.000 становника користи Интернет а налог на друштвеним мрежама има 92,1 % популације од 16 до 24 године.

Повећањем употребе интернета и броја корисника, веће су и разноврсније и могућности за злоупотребу интернет мреже. У вези са компјутерским злоупотребама поставило се питање заштите појединачног личног права - права на приватност.

Развој модерних технологија у великој мери је угрозио личну приватност у виртуелном простору. Сама чињеница да је личне податке могуће сакупљати, чувати, дистрибуирати, умножавати, објављивати и чинити доступним широком кругу људи, створила је несигурност и осећај недовољне заштићености. Пре неку деценију, док су рачунарске технологије тек биле у развоју, сви ови подаци пребацивани су из виртуелног простора на различите дигиталне медије, чинећи „дигиталне досијее". Развојем информационих технологија, омогућено је

---

[76] Top 10 Social Networking Sites, http://news.discovery.com/tech/top-ten-social-networking-sites.html, претражено 05. 08. 2012. године
[77] *Ibid.*
[78] Пословни портал Economy, http://www.economy.rs/ , претражено 27. 09. 2012. године
[79] 55% домаћинстава у Србији поседује рачунар, 47,5 одсто интернет, http://teslio.com/blog/post/tbloger/3865, претражено 27. 09. 2012. године

повезивање различитих база података, што је додатно повећало ризик од нарушавања приватности њихових корисника.

Појавом интернета, пренос дигиталних података и информација постао је још лакши. У почетку, „примитивни“ почетни интернет је омогућавао корисницима анонимност – информације су прослеђиване преко IP адреса које нису могле да препознају ни ко је пошиљалац нити ко је прималац информације. Данашњи „прогресивни“ модел интернет комуникација је у потпуности другачији и опаснији по приватност својих корисника.

„Колачићи“ (енгл. Cookies) и „бубе“ (енгл. Bugg) створили су виртуелни простор који не штити приватне интересе, већ фаворизује и намеће као императив принцип сталног посматрања свих корисника. Овакви рачунарски програми сакупљају са интернета информације попут лозинки, прегледаваних интернет садржаја, садржаја послатих порука. Резултат је немогућност корисника интернета да се неприметно и анонимно креће виртуелним простором. На овај начин, персонализација виртуелног простора све више се изједначава са манипулацијом личним подацима и прикривеном експлоатацијом корисникових жеља и потреба.[80]

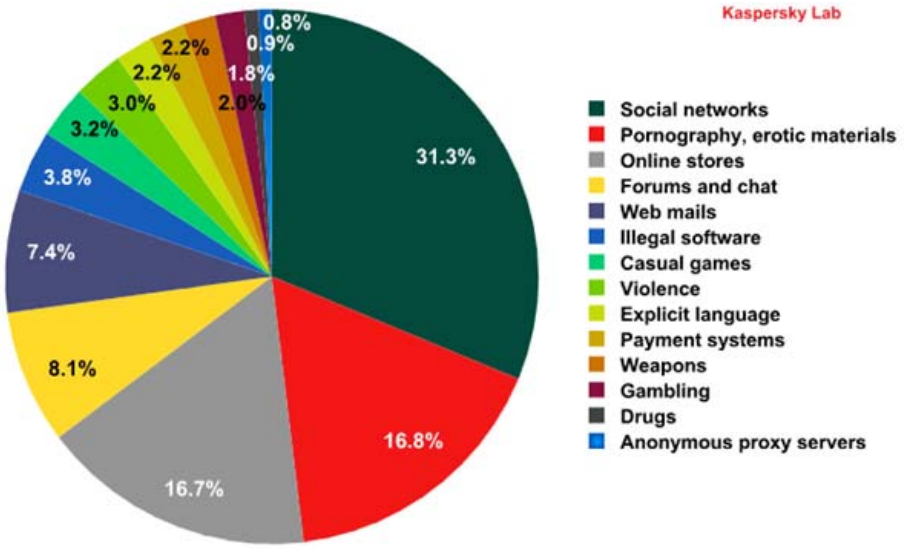
Једну од најмоћнијих иновација у краткој историји постојања интернета представља настанак друштвених мрежа, које су омогућиле најразличитије комуникације људи, без обзира на ком крају света се налазе. Неке од интернет апликација су довеле до злоупотребе приватности корисника друштвених мрежа, отвориле су расправе да ли је код друштвених мрежа заправо реч о комерцијалном интересу, или о стварању нових комуникација и повезивању људи широм планете.

Поједина истраживања[81] су показала да је активност на друштваним мрежама најчешћи разлог због чега људи проводе време на интернету: да заправо 31,3% корисника интернета време проводи на интернету само у оквиру своје активности на некој од друштвених мрежа чији је регистровани корисник.

---

[80] Spinello, Richard.:”Privacy and Social Networking Technology”, International Review of Information Ethics Vol. 16 (12/2011), стр. 44, http://www.i-r-i-e.net/inhalt/016/spinello.pdf, претражено 01. 03. 2013. године

[81] STUDY: Kids Try To Access Social Networks Nearly Twice As Much As Porn Sites, http://www.adweek.com/socialtimes/kaspersky-lab-study-kids-parental-control/422432, претражено 10. 01. 2015. године



Графикон 1: Неки од разлога коришћења интернета [82]

Друштвене мреже и друштвено умрежавање представља једноставан чин одржавања и/или ојачавања постојећег круга пријатеља и/или познаника и самим тим ширење тих кругова.[83] Овако се поред постојећих формира и упознаје нова мрежа пријатеља и познаника, што доводи до настанка мрежа појединаца и стварање заједница.[84]

Постоје и схватања према којима друштвено умрежавање доприноси квалитету социјалних интеракција, употпуњава и охрабрује комуникацију у физичком свету, подстиче развој толеранције на различитости, превазилажење класних, верских, узрасних, културних, политичких разлика, подстиче креативност, академске способности, социјалне вештине, сазревање и развој идентитета.[85]

Управо својом популарношћу и великим бројем корисника, друштвене мреже су створиле својеврстан „надзор" над свакодневним активностима људи, њиховим навикама, њиховим кретањем и дружењем. У ранијем периоду, виртуелни простор био је пун занимљивих и корисних информација, али је било веома мало могућности да овај простор буде интерактиван и да се у креирању података активно учествује. У данашње време друштвене мреже представљају

[82] *Ibid.*
[83] Кушић, Синиша: "Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike facebook generacije", Живот и школа, бр. 24 (2/2010), год. 56, стр.103
[84] *Ibid.*
[85] Жунић-Павловић, Весна и др., *op.cit.,*2013, стр. 139

начин за повезивање људи широм планете. Уз помоћ друштвених мрежа, свет је у могућности да визуализује везе између појединаца.[86]

Иако су први облици сервиса за друштвену мрежу настали раних деведесетих година XIX века, када су биле попут соба за ћаскање где је више корисника могло да необавезно међусобно комуницира а приступ је био дозвољен само преко регистрације или надимка (енгл. Nickname), сервиси за друштвену мрежу се у XXI веку усложавају и дају кориснику већи приступ подацима. Стварају се сајтови који ће полако заменити старе видове комуникације: оне поред првобитне улоге у комуникацији, имају улогу маркетинга, промовишући друге веб-сајтове и низ различитих услуга.

Друштвена (социјална) мрежа (енгл. Social network) најчешће се дефинише као друштвена структура састављена од појединаца (или организација) који се називају „чворови“, а који су повезани једним или више специфичних типова међузависности, као што су вредности, визије, идеје, финансијски интереси, пријатељство, сродство, заједнички интерес, финансијска размена, недопадање, сексуални односи или односи поверења, знања или престижа.[87]

Друштвене мреже се могу дефинисати и као скуп интернет програма који служе да би се људи у комуникацији повезали са својим пријатељима, рођацима, колегама и клијентима, при чему њихови интереси могу да буду друштвени, пословни или мешовити.[88] Оне омогућавају људима да буду део виртуелне заједнице у којој могу да развијају различите односе,[89] а представљају термин који се користи за облик људске интеракције, при којој се, путем постојећих познаника, упознају нове особе ради остваривања друштвених или пословних контаката. [90]

---

[86] Top 10 Social Networking Sites, http://news.discovery.com/tech/top-ten-social-networking-sites.html, претражено 05. 08. 2012. године

[87] Видановић, Иван: „Речник социјалног рада“, Удружење стручних радника социјалне заштите Србије, Друштво социјалних радника Србије, Асоцијација центра за социјални рад Србије, Унија Студената социјалног рада, 2006, Београд, стр. 437-438

[88] Social networking, http://www.investopedia.com/terms/s/social-networking.asp , претражено 07. 06. 2014. године

[89] Social networking, http://www.techterms.com/definition/socialnetworking, претражено 07. 06. 2014. године

[90] Сигурносни ризици друштвених мрежа - Хрватска академска и истраживачка мрежа, www.cert.hr, претражено 17. 03. 2015. године

Често означена и као „виртуелна заједница“ или „скуп личних профила различитих људи“, друштвена мрежа представља презентацију на интернету која на једном месту спаја људе како би разменили мишљења, причали, поделили идеје и интересовања и стварали нове контакте.[91] Оваква активност на интернету представља карактеристичан друштвени медиј, чији садржај за разлику од других медија креирају стотине па чак и милиони људи.

Под друштвеним мрежама подразумевају се и везе између „чворова“ - међусобно испреплетаних односа појединаца и организација.[92] Појединци користе одређене интернет странице како би створили своје јавне личне карте (профиле) и стварали одређене односе са другим људима који имају приступ њиховом профилу.[93] Профили представљају јединствене странице на којима сваки појединац може себе да представи другима,[94] у оној мери и на начин на који то жели.

Поједини аутори, попут Ренди Дојермајера (Randy Duermyer), сматрају да се друштвена мрежа може одредити као скуп индивидуа који деле своја заједничка интересовања.[95] Тачка повезаности ових индивидуа може да буде окружење у коме живе, вера, пословни интереси, заједнички пријатељи или уверења која деле. [96]

Насупрот дефинисању друштвених мрежа као скупа индивидуа, постоје и аутори попут Бојда и Елисон (Boyd & Ellison) који сматрају да друштвене мреже представљају услуге које се базирају на коришћењу интернета помоћу којих појединци 1) могу да стварају своје јавне или полујавне профиле унутар једног ограниченог система, 2) стварају уређен списак корисника са којима контактирају и размењују информације и 3) да претражују листе контаката оних

[91] Social network, http://www.computerhope.com/jargon/s/socinetw.htm, претражено 08. 06. 2014. године
[92] Social network, http://www.webopedia.com/TERM/S/social_network.html, претражено 07. 06. 2014. године
[93] Social networking site, http://www.webopedia.com/TERM/S/social_networking_site.html , претражено 07. 06. 2014. године
[94] Кушић, Синиша, *op.cit.,* 2010, стр.104
[95] Duermyer, Randy: “ Social Networks - Define Social Networks“, http://homebusiness.about.com/od/homebusinessglossar1/g/social-networks.htm, претражено 07. 06. 2014. године
[96] *Ibid.*

са којима су повезани у систему.[97] Активност на друштвеним мрежама или „умрежавање“ (енгл. Networking) има за циљ да иницира успостављање контакта, углавном између људи који се међусобно не познају. [98]

Анализирањем језичких тумачења појма „друштвена мрежа“, приметне су разлике у садржини коју овај појам обухвата. Друштвена мрежа представља специфичну интеракцију друштвених и личних односа, односно интернет страницу или апликацију која омогућава њеним корисницима да међусобно комуницирају на тај начин што размењују информације, коментаре, поруке, слике и сл.[99] Под друштвеном мрежом подразумева се и интернет заједница људи који су окупљени око заједничких интересовања користе компјутерске технологије да би међусобно комуницирали и размењивали информације, а све то преко интернет портала који омогућава њихову комуникацију. [100]

Друштвене мреже могу да буду, у односу на природу веза због којих се људи спајају, *хоризонталне,* уколико су корисници почели да се повезују без тачно одређених циљева или из забаве, и *вертикалне*, уколико се баве тачно одређеним активностима или интересовањима (нпр. проналажење посла, упознавање и сл). [101]

Поред појма „друштвене мреже” често коришћен је и термин „друштвеног умрежавања” (енгл. Social networking), па се веома често ова два појма користе као синоними, иако постоји разлика. „Умрежавање”, за разлику од друштвених мрежа, обухвата иницирање и покретање односа, најчешће између особа које се не познају.[102] Иако је умрежавање могуће и на друштвеним мрежама, оно није њихов примарни циљ. Оно што чини специфичност друштвених мрежа је да оне омогућавају појединцима да артикулирају и учине видљивим своје већ постојеће мреже контаката и познаника, а не да упознају

---

[97] Boyd, M.Danah, Ellison, B.Nicole: “Social Network Sites: Definition, History,and Scholarship”, Journal of Computer-Mediated Communication Volume 13, Issue 1, International Communication Association, октобар 2007, стр. 211, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full, претражено 11. 12. 2014. године

[98] *Ibid.*

[99] Oxford dictionaries, http://www.oxforddictionaries.com/definition/english/social-network , претражено 07. 06. 2014. године

[100] Social network, http://dictionary.reference.com/browse/social+network, претражено 07. 06. 2014. године

[101] Financial times, http://lexicon.ft.com/Term?term=social-network , претражено 07. 06. 2014. године

[102] Кушић, Синиша, *op.cit.,* 2010, стр.105

непознате особе.[103] Друштвене мреже заправо првенствено служе да корисници комуницирају с особама које су већ део њиховог "реалног", свакодневног света, јер иако друштвене мреже омогућују и олакшавају упознавање нових особа један од циљева њиховог постојања је и одржавање и/или ојачавање односа са људима који се међусобно већ познају или друже.

Све друштвене мреже функционишу преко сервиса за друштвену мрежу. Сервис за друштвену мрежу дефинише са као интернет услуга која омогућава појединцима да 1) направе јавни или полу-јавни профил у оквиру једног ограниченог система, 2) контролишу листу других корисника са којима су повезани, и 3) контролишу односе које имају са корисницима унутар мреже.[104]

Поједине маркетиншке агенције (нпр. Pew Internet[105]) су истраживале профиле корисника различитих друштвених мрежа, у жељи да сазнају ко су људи који свакодневно посећују виртуелно место за дружење и комуникацију. Подаци добијени приликом овог истраживања које је спроведено у периоду од 23.-26. јануара 2014. године показују да је у јануару 2014. године 74% одраслих особа активно користило друштвене мреже на којима су имали регистроване профиле.[106] Истраживање је показало да су то у највећем броју жене (74% жена је одговорило да користи друштвене мреже, док своје налоге на друштвеним мрежама има 62% мушкараца), старости од 18-49 година, средњошколског образовања. Исто истраживање спроведено септембра 2014. године показало је да 71% пунолетних особа које користе друштвене мреже имају налог на друштвеној мрежи Facebook, 23% користе Twitter, 26% Instagram, 28% Pinterest и 28% пословну друштвену мрежу LinkedIn.[107]

[103] *Ibid.*
[104] Boyd, M.Danah, Ellison, B.Nicole, *op.cit.,* 2007, стр. 216
[105] Pew Research Center, http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/ , претражено 07. 02. 2015. године
[106] *Ibid.*
[107] *Ibid.*

2.2. Приватност корисника друштвених мрежа

Друштвене мреже су створиле праве детаљне базе личних података из живота својих корисника,[108] а ове базе се свакодневно допуњују чиме се повећава број информација које су јавне и доступне свим актерима виртуелне интеракције на интернету. Чим се лични податак објави на интернету он постаје јаван и доступан свима да га прочитају и употребе, па корисник губи контролу ко има увид у његову интиму и информације које је објавио. Корисници најчешће прецењују своју моћ контроле над подацима које објављују преко друштвених мрежа, при чему нису свесни ни свој техничког незнања везаног за коришћење самих друштвених мрежа и подешавања приватности корисничких профила.

Основна сврха постојања друштвених мрежа је интеракција и комуникација преко интернета, а корисници се међусобно представљају својим личним страницама (тзв. „профилима“) и на тај начин визуелизацију своје односе. Однос између приватности и профила корисника на друштвеној мрежи вишеструка: у неким приликама корисници желе да информације које објављују о себи буду доступне само уском кругу људи, док у неким другим ситуацијама корисници су спремни да открију своје тајне непознатим и анонимних странцима. Све ове информације, уколико се злоупотребе, могу да проузрокују тешке последице, у распону од крађе идентитета па до узнемиравања и прогањања, од претрпљене срамоте, преко различитих врста искриминације или чак до уцењивања. Упркос свести да све приватност на друштвеним мрежама може бити повређена, лични подаци се и даље добровољно објављују на оваквим сајтовима.

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.

---

[108] Viégas, B. Fernanda: “Blogger’s expectations of privacy and accountability: An initial survey”, Journal of Computer–Mediated Communication, volume 10, number 3, 2005, стр.18, http://jcmc.indiana.edu/vol10/issue3/viegas.html, претражено 23. 05. 2014. године

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.

Развој модерних технологија у великој мери је угрозио личну приватност у виртуелном простору. Сама чињеница да је личне податке могуће сакупљати, похрањивати, дистрибуирати, умножавати, објављивати и чинити доступним широком кругу људи створила је несигурност и осећај недовољне заштићености. Кључне области у којима долази до електронског сакупљања личних података и до могућности њихове злоупотребе су електронско пословање, пружање медицинских услуга и коришћење различитих врста интернет сервиса. [109] Пре неку деценију, док су рачунарске технологије тек биле у развоју, сви ови подаци пребацивани су из виртуелног простора на различите дигиталне медије, чинећи “дигиталне досијее”. Са развојем информационих технологија, омогућено је повезивање различитих база података, што је додатно повећало ризик од нарушавања приватности њихових корисника.

Појавом интернета пренос дигиталних података и информација постао је још лакши. У почетку, “примитивни” почетни интернет је омогућавао корисницима анонимност – информације су прослеђиване преко ИП адреса које нису могле да препознају ни ко је пошиљалац нити ко је прималац информације. Данашњи „прогресивни” модел интернет комуникација је у потпуности другачији и опаснији по приватност својих корисника, јер повреде приватности и угрожавање безбедности могу потицати од других корисника друштвене мреже, од трећих лица али и од самог пружаоца услуге друштвене мреже.

Постоје четири основна разлога због чега долази до могућности кршења права на приватност на друштвеним мрежама:[110]

---

[109] Спасић, Видоје: „Неки аспекти приватности у сајберспејсу“, Зборник Правног факултета у Нишу, Ниш: Правни факултет, 2005. - бр. 46 (2005), стр. 209

[110] Shah, Mahmood, *op.cit.,* 2013.

1. ***несавршеност корисника друштвене мреже*** – односе се углавном на несавршености човека као људског бића и на његову потребу да своју приватност дели са другим људима; свест о сопственој и туђој приватности не постоји у оперативној меморији човека па корисник тако „ода" осетљиву информацију да и није тога свестан;
2. ***мане у програмима (софтверима) који се користе на друштвеним мрежама*** – доводе до тога да су на друштвеним мрежама механизми за контролу приватности веома слаби и незаштићени од свих директних злонамерних напада, попут крађе личних података, стварања лажних профила и сл.;
3. ***ненамерно одавање личних података*** – до личних података на друштвеној мрежи се може доћи и методом искључивости (нпр.када на основу године дипломирања можемо закључити које је корисник годиште иако то није написао у профилу); нажалост, против оваквог "цурења" података корисник се најтеже бори јер на друштвеним мрежама постоји небројено много информација и података од којих корисник не може да се сачува нити припази;
4. ***сукоб интереса*** – већина друштвених мрежа се финансира од огласа које рекламне агенције постављају, па ова чињеница доводи до сукоба интереса када је реч о личним подацима корисника које друштвене мреже могу да уступају рекламним агенцијама; корисници желе да њихови подаци недоступни људима које нису означили као „пријатеље" док рекламне агенције желе да дођу у посед што већег броја личних информација како би боље и лакше пласирали своје производе или услуге.

Заштита података, по дефиницији коју даје Џозеф Канатачи (Joseph Cannataci)[111] значи заштиту појединца од злоупотребе или неадекватне употребе личних података од стране неког лица, приватне организације или државе. 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

[111] Cannataci, Joseph A.: "Privacy and Data Protection Law: International Development and Maltese Perspectives", Complex series, 1987.

начин је могуће коришћење интернета без давања могућности трећем лицу да се повеже са интернет активностима за личну идентификацију интернет корисника.

Приватност на интернету укључује право на личне информације у вези са чувањем, употребом, обезбеђењем од трећих лица и приказивање личних информација преко интернета, као и идентификационе информације које се односе на посетиоца одређене интернет странице. Приватност у виртуелном простору може да се дефинише и као „ограничени приступ личним подацима/ограничена контрола личних података“.[112]

а) ***Ограничени приступ личним подацима*** подразумева да постоји приватност корисника интернета и да се лични подаци корисника не користе и прослеђују без њихове сагласности.

б) Суштина ***ограничене контроле личних података*** огледа се у томе да сваки појединац мора да ограничи број података које ће објавити на интернету, како би спречио све могуће злоупотребе својих података.

Већина корисника друштвених мрежа објављује велики број приватних и личних података, које одмах постају доступне небројеним корисницима широм света. Уколико корисник добровољно објави податке о себи или из свог живота (принцип „ограничене контроле личних података“), администратор друштвене мреже обавезан је да тражи сагласност корисника мреже да даље прослеђује податке које је он објавио на мрежи (принцип „ограниченог приступа личним подацима“). На овај начин се објављени подаци штите али до одређене мере: уколико дође до упада у системе, злоупотребу објављених података је немогуће спречити. Интересантно је да су бројна истраживања показала да корисници различитих друштвених мрежа свесно деле своје приватне податке преко друштвених мрежа: међу 4000 студената који имају профил на Фејсбуку незнатно мали проценат је променило основно подешавање приватности којим су сви подаци јавни и доступни свим корисницима интернета[113] а међу 20.000

[112] Tavani and Moor, 2001., наведено код Spinello, Richard, *op.cit.,* 2011.
[113] Gross and Acquisti (2005) наведено код Utz, Sonja, Kramer, C. Nicole: “The privacy paradox on social network sites revisited: The role of individual characteristics and group norms”, Cyberpsychology: Journal of Psychosocial Research on Cyberspace, volume 3, number 2, article 1, 2009, http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1, претражено 10. 12. 2014. године

профила на друштвеној мрежи MySpace само 27% је своје профиле учинило приватнима.[114]

Приватност се може дефинисати као „стање брижљиво ограниченог приступа личним подацима".[115] Свако поступање другачије од описаног представља злоупотребу права на приватност, а сакупљање осетљивих личних података о некоме без његове сагласности и знања може за циљ да има манипулацију тим подацима.

У електронским комуникацијама, приватност може да се схвати као „слобода од систематског посматрања и бележења активности и личних података, односно право појединаца да сами одређују када, како и у којој мери информација о њиховим комуникацијама треба и може да буде доступна другима".[116] Овако схваћена приватност корисника може бити повређена на више начина: упадом у зону приватности (приступом, прикупљањем и обрадом), злоупотребом (одавањем или деловањем на основу доступне информације) и пресретањем и уклапањем информација (профилисањем).[117] Приватност на интернету такође може да се схвати као скуп информација нераскидиво везаних за појединца које дају печат његовој индивидуалности, а које су правно заштићене од неовлашћеног приступа, као и од повреде сваког другог лица, а тичу се имена, слике, брачног или породичног живота, навика, хобија или другог личног интересовања појединца.[118]

Најбољи начин за заштиту приватности свих интернет корисника је управо принцип контролисаног откривања личних информација. 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. Објављивање „постова" и личних информација на интернету може бити штетно за приватност појединца јер су

---

[114] Thelwall (2008) наведено код Utz, Sonja, Kramer, C. Nicole, *op.cit.,* 2009
[115] Spinello, Richard, *op.cit.,* 2011., стр. 44
[116] Nikolić, Milan: "Praktični aspekti zaštite privatnosti korisnika i bezbednosti elektronskih komunikacionih mreža i usluga u Srbiji", http://www.telekomunikacije.rs/arhiva_brojeva/peti_broj/milan_nikolic:_prakticni_aspekti_zastite_privatnosti_korisnika_i_bezbednosti_elektronskih_komunikacionih_mredja_i_usluga_u_srbiji_.305.html#_ftn18 , 30. 07. 2014. године
[117] *Ibid.*
[118] Спасић, Видоје*, op.cit.,* 2005, стр. 210

информације (блогови, слике и интернет стране) које су једном објављене на интернету трајне.

Поред кршења приватности корисника друштвених мрежа од стране других појединаца, у сферу приватног веома често залази и сама држава користећи податке који се складиште у виртуелном простору. У овом случају, поставља се питање до које је мере за функционисање једног модерног друштва потребно и оправдано прикупљање личних података, као и колики је обим права осталих корисника друштвених мрежа приликом коришћења и располагања туђим личним подацима.

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.

На кршење права на приватност у виртуелном свету указао је Едвард Сноуден (Edward Snowden),[119] бивши компјутерски аналитичар, који је јуна 2013. године сакупио информације које се односе на прекорачење овлашћења владиних програма за праћење, која су била противзаконита и које су откривале обмане у званичним тврдњама владе које су јавно објављиване. Тачније, Сноуден је установио да је америчка Национална агенција за безбедност (НСА) шест година спроводила програме којима су праћени сви подаци и комуникације људи на друштвеним мрежама, као и да је Влада САД преко сервера великих Интернет компанија имала потпуни приступ огромној количини података и могућност праћења стотине милиона људи на Интернету широм света у реалном времену. Microsoft је све сакупљене податке прослеђивао НСА од 2007. године, Yahoo и AOL од 2008. године, Google и Facebook од 2009. године, YouTube од 2010. године а Apple од 2013. године.[120] Сноуден је објаснио да се у САД, а затим и у осталим моћним државама света,

[119] Видети: Bio., http://www.biography.com/people/edward-snowden-21262897, претражено 03. 03. 2015. године

[120] Наведено код: Дилигенски, Андреј, Прља, Драган, *op.cit.*, 2014., стр. 102

користе одређени програми којима је могуће прикупити личне податке са интернета (тзв. метаподатке) наводно у циљу сакупљања обавештајних и безбедносних података под оправдањем разлога националне одбране.[121] Све информације до којих је дошао, Сноуден није хтео лично да објави, већ их је објављивао преко новинара Глена Гринвалда, Лоре Појтрес, Јуана Мекаскила и Бартона Гелмана.

Један од ових програма за прикупљање личних података са интернета био је PRISM[122] програм, затим BULLRUN[123], EDGEHILL и најновије откривен LEVITATION[124] који се примењује у Канади.[125] Коришћењем ових и сличних програма, држава је у могућности да открије где корисник друштвене мреже живи, са ким је повезан, ко су му пријатељи, у зависности од садржаја објављених слика у кога је корисник заљубљен, с ким је у вези, која су му политичка и верска интересовања.

Сноуден је навео да постоји програм у Великој Британији, који се зове Оптички нерв[126] део алијансе „Петоро очију" (енгл. Five Eyes)[127] која окупља САД, Велику Британију, Канаду, Аустралију и Нови Зеланд, а омогућава Британцима да укључе веб камеру било ког корисника друштвене мреже и да податке који се налазе на рачунару и да пресреће комуникацију људи преко сервиса за инстант поруке.

---

[121] Реконструкција – Женски фонд, http://www.rwfund.org/kriticne-teme/izvori-epistemologije-kriticki-zivot/edvard-snouden/, претражено 08.04.2015.године

[122] PRISM је тајни програм Америчке безбедносне агенције за прислушкивање Интернет комуникације страних земаља помоћу великих Интернет компанија, лансиран 2007. године, више на Everything you need to know about PRISM, http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet, претражено 08. 04. 2015. године

[123] Bullrun је тајни, строго поверљиви програм за дешифровање који користе Америчка безбедносна агенција и њен британски еквивалент. Иако не постоји прецизна техничка спецификација овог програма у откривеним документима, одређени наводи британских тајних служби наговештавају да је програм омогућио приступ подацима које је до употребе овог програма било немогуће дешифровати, више на Project Bullrun – classification guide to the NSA's decryption program, http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide, претражено 08. 04. 2015. године

[124] CSE tracks millions of downloads daily: Snowden documents, http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120, претражено 08. 04. 2015. године

[125] *Ibid.*

[126] Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo, претражено 08. 04. 2015. године

[127] Unmasking the Five Eyes' global surveillance practices, http://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices, претражено 08. 04. 2015. године

Поред овог открића, Сноуден тврди да су судови ти који омогућавају овакве повреде права на приватност необезбеђивањем адекватне правне заштите објављеним подацима и игнорисањем постојања злоупотребе нечије приватности.[128] Када се погледају истраге које су вођене након објављивања ових извештаја, резултата је ипак било. У САД је формирана независна комисија[129] која је, заједно са ревизорским телом, на основу пуног приступа поверљивим информацијама утврдила да су сви наведени програми непотребни и да врше противправни масовни надзор а не надзор над појединцима за које се предпоставља да постоји разлог.[130] Европски суд правде је ставио ван снаге Директиву о задржавању података[131] која је налагала провајдерима и оператерима телекомуникационих услуга да чувају податке о својим клијентима у периоду до 24 месеца и да их на захтев прослеђују различитим службама, а која је била примењивана на територији земаља Европске Уније. И међународне организације су се такође укључиле у ове истраге. Савет Европе је потврдио да ниједан од наведених и сличних програма није неопходан и ефикасан, да треба да се укину и да су у сукобу са поштовањем основних људских права. Уједињене нације су подржале овај став.

На Northeastern University у Сједињеним Америчким Државама спроведена је студија од стране Алана Мислова (Alan Mislove) и његових колега са Макс Планк института за софтверске системе, у оквиру које је направљен алгоритам чија је сврха била покушај проналажења личних карактеристика корисника друштвене мреже Facebook на основу листе његових пријатеља.[132] Студија је показала да се само 5% људи сетило да заштити листу пријатеља и своје личне податке које су изнели на мрежу док остали то нису у потпуности

---

[128] *Ibid.*

[129] У САД је нпр.формиран Одбор за праћење приватности и грађанских слобода (The Privacy and Civil Liberties Oversight Board - PCLOB), https://www.pclob.gov/, претражено 09. 04. 2015. године

[130] Roller, Emma: „This is what secton 215 of the Patriot Act does“, www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html , претражено 09. 04. 2015. године

[131] European Union Law – Data Retention Directive, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, претражено 09. 04. 2015. године

[132] Hayden, Erik.: „On Facebook, You are who you know“, 2010, http://www.psmag.com/culture-society/on-facebook-you-are-who-you-know-10385/, претражено 12. 08. 2012.с године

учинили у погледу различитих области из живота - 19% свих корисника је омогућило јавни приступ свим информацијама о себи. [133]

Интересантно истраживање посвећено свести о праву на приватност на друштвеним мрежама спроведено је и у Уједињеним Арапским Емиратима и Египту,[134] као афричким земљама са највећим бројем корисника интернета и друштвених мрежа. Испитано је укупно 325 корисника интернета (157 мушког и 168 женског пола) старости од 14 до 57 година, а постављано им је 26 питања која су била класификована у 4 различите групе: (1) које су најпопуларније друштвене мреже? (2) који су разлози коришћења друштвене мреже, а који су разлози напуштања друштвене мреже? (3) које личне податке корисници објављују преко друштвене мреже стављајући их на своје корисничке профиле? и (4) како корисници реагују на непознате људе које упознају преко интернета? Највећи број анкетираних се изјаснило да воде просечну бригу о својој приватности на интернету (68.2%), док је само 17.07% одговорило да поштују све мере понашања безбедног по приватност на интернету.[135] Интересантно је да је 37.07% испитаника одговорило да са непознатим људима не ступа у контакт преко интернета, а 37% прво постави питање због чега га та особа контактира уколико се не познају.[136] Такође, направљена је интересантна компарација одговора које су давали мушкарци и одговора које су давале жене. Није било значајне разлике у погледу процентуалног односа мушкараца и жена који користе интернет, али је зато уочено да особе женског пола много више страхују за своју сигурност на интернету, да су мушкарци чешће активни на друштвеним мрежама и да им верују више него жене, па самим тим жене се и више труде да заштите своју приватност када приступају друштвеним мрежама.[137]

---

[133] *Ibid*.
[134] Mohamed, Azza Abdel-Azim: "Online Privacy Concerns Among Social Networks'Users", Cross-cultural communication, Vol. 6, No. 4, 2010, стр. 80, www.cscanada.org, претражено 03. 04. 2014. године
[135] *Ibid.*, стр. 81
[136] *Ibid.*, стр. 82
[137] *Ibid.*, стр. 85

Годишњи извештај сигурносне фирме Sophos[138] показао је да је током 2011. године у свету нападнуто 67% корисника друштвених мрежа, највише друштвене мреже Facebook, што представља 90% више у односу на 2009. годину.[139] Резултат истраживања у које је било укључено 1.4 милиона корисника друштвене мреже Facebook показало је да је приметан пораст интересовања корисника друштвене мреже у циљу заштите приватности.[140]

[138] Вугделија, Наталија, Савић, Ана, Савић Срђан: "Безбедност рачунарских система у савременом електронском пословању", http://infoteh.etf.unssa.rs.ba/zbornik/2011/radovi/E-III/E-III-10.pdf, претражено 06. 08. 2013. године

[139] Друштвене мреже: Cyber криминал лани порастао за 90 посто, http://www.24sata.info/tehnologija/internet/53981-Drustvene-mreze-Cyber-kriminal-lani-porastao-posto.html, претражено 06. 08. 2013. године

[140] Dey, Ratan, Jelveh, Zubin, Ross, Keith,: "Facebook Users Have Become Much More Private: A Large-Scale Study", 2011., http://cis.poly.edu/~ratan/facebookusertrends.pdf, претражено 04. 08. 2013. године

2.3. Правила (политика) приватности на најчешће коришћеним друштвеним мрежама

Друштвене мреже и компаније, које обезбеђују сајтове за друштвено умрежавање, своја богатства и популарност граде на посматрању понашања и односа у друштву, као и на циљано оглашавање различитих ствари, при чему се масовно користе сакупљени подаци о корисницима друштвених мрежа и дневници њихових редовних активности на друштвеним мрежама. Управо из овог разлога друштвене мреже веома често личне податке својих корисника „деле“ са различитим компанијама, а најчешће са компанијама које се баве маркетингом и рекламним послом, препуштајући им заједно са личним подацима о корисницима и њихова интересовања.[141]

Иако је велики број корисника друштвених мрежа свестан чињенице на друштвеним мрежама приватност може да буде повређена или бар угрожена, велики број личних података корисници и даље настављају да објављују путем друштвених мрежа. Неки од разлога за добровољно откривање личних података које су поједини аутори препознали су жеља за пажњом, незаинтересованост или опуштен став према поштовању своје или туђе приватности, непотпуно пласираље информација, поверење у безбедност података на друштвеној мрежи као и поверење у пријатеље на друштвеној мрежи.[142]

Већа популарност сајтова за друштвено умрежавање довела је до интензивнијег разматрања заштите приватности. Спокео (Spokeo) не представља класичну друштвену мрежу, али представља претраживач за повезивање људи који користи податке скупљене агрегацијом. Наиме, сајт садржи информације као што су старост, статус везе, имућност, информације о ближим члановима породице, као и адресе регистрованих корисника. Ове информације су сакупљене помоћу података који већ постоје на интернету а

[141] Catanese, A. Salvatore, De Meo, Pasquale, Ferrara, Emilio, Fiumara, Giacomo, Provetti, Alessandro: “Crawling Facebook for Social Network Analysis Purposes”, 2011, http://arxiv.org/pdf/1105.6307.pdf, претражено 15. 02. 2015. године

[142] Gross, Ralph, Acquisti, Alessandro: “Information revelation and privacy in online social networks” - In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, стр. 77., ACM, 2005, http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, претражено 15. 02. 2015. године

које су корисници друштвених мрежа наводили, али сајт не гарантује за тачност података. [143]

Повреда права на приватност најчешће се врши у оквиру друштвених мрежа са највећим бројем регистрованих корисника, као што су Facebook, Twitter и LinkedIn. Питања која се намећу су да ли су корисници друштвених мрежа и даље власници свих информација и да ли је могуће трајно уклањање налога и брисање једном објављених података?

2.3.1. Facebook (FB)

Политика приватности и доступности објављених личних података на овој друштвеној мрежи мењала се током њеног постојања.[144] У почетку, како је Facebook представљао друштвену мрежу која је била намењена само студентима једног кампуса, нико други осим студената није могао да види било шта од података који су се објављивали. Услед отварања ове мреже и за кориснике широм света и услед редизајнирања саме странице, Facebook је корисницима омогућио да сами прилагоде опције шта ће делити са ким одредивши им да њихове објављене податке не може видети нико, могу видети само пријатељи, могу видети и пријатељи пријатеља, сви корисници ове друштвене мреже или свако ко уопште приступа ингтернету. Када је Facebook постао платформа за друштвену мрежу на којој су и различите компаније могле да остављају своје апликације, корисницима је дата могућност да се одлуче да ли желе да њихови подаци буду доступни овим компанијама или не. Сваки пут када је Facebook додавао нову опцију за садржаје које је могуће делити, приватност сваког од корисника аутоматски би била враћана на опцију јавног приступа профилу.

Проучавајући ову друштвену мрежу стиче се утисак да је тежња да што више личних података о корисницима буде доступно за преглед целокупној јавности која се креће виртуелним простором интернета, јер су приликом регистрације корисника сви подаци на минималној опцији заштите приватности док корисник сам не постави одређене границе. Корисници могу да сами подесе опције своје приватности на овој друштвеној мрежи и да на тај начин себи осигурају неколико различитих степена заштите своје приватности.

---

[143] About Spokeo, http://www.spokeo.com/blog/about, претражено 12. 08. 2012. године
[144] "The evolution of privacy on Facebook", http://mattmckeon.com/facebook-privacy/, претражено 17. 02. 2014. године

Корисник који да само приступи овој друштвеној мрежи мора да упише своје основне демографске информације,[145] а када жели да креира налог мора да наведе своје име, е-маил адресу, датум рођења, пол, док су пожељни али не обавезни и подаци о адреси становања, занимању и радном месту или школи, фотографије, интересовања и други детаљи који се односе на личност корисника.[146] Такође, од корисника се очекује да стварају нове везе са другим корисницима, тако што ће их означити као "пријатеље", да деле своја размишљања и медијске садржаје, ажурирају своје статусе, фотографије и коментаре. Ови подаци, заједно са профилном сликом корисника, корисничким именом и лозинком постају доступни свима на интернету[147]. Грос и Акуисти (Gross & Acquisti) су, након спроведеног истраживања о начину коришћења друштвених мрежа и заштити приватности, дошли до податка да чак 82% корисника друштвене мреже Facebook открива следеће поверљиве информације о себи: датум рођења, број мобилног телефона, адресу, па чак и име свог сексуалног партнера.[148] Сама правила ове друштвене мреже су таква да подстичу кориснике да откривају што више личних података и да на тај начин сами руше своју приватност.

Корисник сам мора да по регистрацији подеси приватност свог налога. Основно подешавање налога приликом регистрације је да је сваки профил и свака објављена информација јавна, што значи да је доступна свакој особи која је корисник интернета.

Сваки пут када се корисник улогује на свој профил, када прегледа туђи профил, потражи одређену страницу или пријатеља, кликне на оглас који се налази на страници или користи било коју апликацију Facebook добија, прикупља и чува ове податке, а уколико корисник објави фотографију или видео запис, Facebook бележи и време, датум и место на коме је фотографија или видео запис настао. Подаци се прикупљају и складиште на основу

---

[145] Boyd, Danah, Hargittai, Eszter: "Facebook Privacy Settings: Who Cares?", First Monday, Volume 15, Number 8, 2010, http://firstmonday.org/article/view/3086/2589, претражено 15. 04. 2014. године

[146] Фејсбук - Политика о коришћењу података: Информације добијене од корисника, Registration information, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године

[147] Фејсбук - Политика о коришћењу података:Информације добијене од корисника, Information that is always publicly available, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године

[148] Gross, Ralph, Acquisti, Alessandro, *op.cit.,* 2005, стр. 77

„колачића" (енгл. Cookies), који представљају мале текстуалне фајлове које сваки интернет сајт складишти на рачунару корисника, како би се по потреби брзо и поново препознали, чиме је омогућено брже учитавање жељене странице. Сакупљање података је могуће без обзира како и одакле су послати на профил корисника (да ли су послати са рачунара, мобилног телефона или било ког другог уређаја са кога је могуће приступити мрежи).

Друштвена мрежа прикупља личне податке о регистрованим корисницима уз образложење да су корисници, прихватањем правила коришћења мреже дали сагласност за обраду својих података. Постоји неколико врста личних података које се на Фејсбуку сакупљају: [149]

1. Листа пријатеља (енгл. List of Friends) – у којој се налази списак свих корисника друштвене мреже коју је неки конкретан корисник прихватио и означио као "пријатеља"; у зависности од безбедоносних подешавања сваког корисничког налога, овај податак могу видети или само пријатељи корисника или може да буде јаван и доступан свима који су на интернету.
2. Личне информације о кориснику (енгл. Personal Information) – део који обухвата све информације које је корисник желео да наведе о себи, попут имена и презимена, занимања, старости, политичке и верске припадности, ствари које корисник воли, лична интересовања, чланства у различитим групама на друштвеној мрежи и сл.
3. Постови на „зиду" корисниковог профила или статуси (енгл. Wall posts) – представљају јавне поруке које је неки корисник примио од других корисника или апликација које корисни на друштвеној мрежи, могу да представљају и различите врсте обавештења; они најчешће изражавају како се корисник осећа, шта ради, шта мисли и са ким је у одређеном тренутку.
4. Поруке (енгл. Messages) – представљају приватне поруке примљене од других корисника ове друштвене мреже, слично порукама електронске поште.

[149] McCown, Frank, Nelson, L. Michael: „What happens when facebook is gone?", In Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries, стр.251-254. ACM, 2009, http://www.cs.odu.edu/~mln/pubs/jcdl09/archiving-facebook-jcdl2009.pdf, претражено 15. 02. 2015. године

5. Фотографије (енгл. Photos) – које корисник није обавезан да објављује већ их објављује по својој вољи и на њима може да означи (енгл. Tag) све особе које се налазе на њима; о овим сликама у зависности од безбедоносних подешавања корисници друштвене мреже могу да постављају коментаре. Интересантно је да корисници ове друштвене мреже уколико запамте интернет адресу на којој се налази одређена слика, могу јој приступити чак и након пар година од њеног брисања.[150]
6. Белешке (енгл. Notes) – представљају писања корисника слична блоговима који сами корисници креирају и који могу да садрже текст и фотографије, док други корисници могу да их коментаришу или деле даље.

Наведене информације које је Facebook сакупио[151] постају доступне великом кругу лица: пријатељима корисника, свим корисницима ове мреже, а уколико се ова опција не искључи биће доступне и маркетиншким партнерима са којима Facebook сарађује, оглашивачима који купују рекламни простор, као и ауторима видео игара и различитих апликација. Оснивачи ове мреже су одмах и објаснили сврху коришћења личних података корисника: ради сигурности производа и услуга мреже, заштите права интелектуалне својине мреже и његових корисника, дељења локалних догађаја и услуга са осталим корисницима, мерења и бољег разумевања ефекта које рекламни простор изазива код корисника давања препорука за налажење могућих пријатеља или дељења заједничких слика, за решавање техничких проблема и начина побољшања саме услуге. [152]

На основи свих сакупљених података, Facebook корисницима преко опције “Friend Finder” нуди опцију да им сугерише које особе могу да познају. Коришћење ове опције је прилично спорно са становишта приватности корисника, јер сама друштвена мрежа обрадом личних података сужава круг људи које корисник може да познаје или са којима се дружи, без обзира на то да ли су они регистровани на друштвеној мрежи или не. Након што обради

[150] ФБ чува обрисане фотографије, http://www.b92.net/tehnopolis/vesti.php?nav_id=465257&fs=1, претражено 07. 08. 2012. године
[151] Фејсбук - Политика о коришћењу података: Информације добијене од корисника, How we use the information we recieve, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године
[152] *Ibid.*

објављене личне податке корисника, Facebook у име корисника шаље позиве да се могући познаници придруже друштвеној мрежи или да већ регистровани корисници постану пријатељи са корисником у чије име се шаље позив. Сагласност корисника се тек тражи након ових обављених радњи, а манифестује се тако што ће корисник одређено лице прихватити као пријатеља или ће се лице које није корисник придружити друштвеној мрежи.

Како би Facebook и даље био бесплатан за кориснике, оснивачи ове друштвене мреже „морају“ да „деле“ личне контакте корисника различитим маркетиншким компанијама како би им оне посредством интернета слале рекламни материјал.[153] У полиси о коришћењу услуга наведено је да је корисник и даље власник свих информација, да је у могућности да забрани мрежи коришћење личних информација и података или да захтева да му се име не спомиње како би идентификација била спречена. Интересантно је да већина корисника мреже и не зна за ове могућности као ни за своја права, јер највећи број корисника ретко улази у подешавања налога и не поставља личне захтеве за реализацију ових могућности. Сакупљање података о корисницима ради дељења у рекламне сврхе врши се и уз помоћ „колачића“ (енгл. Cookies) и дугмета „Свиђа ми се“ (енгл. Like button). У зависности од тога које рекламне садржаје корисник прегледава, врши се групација о сврставање корисника друштвене мреже у посебне групе, на основу њихових интересовања и на тај начин се корисник касније затрпава нежељеним рекламама. На овај начин се, уз помоћ „колачића“, прави детаљно профилисање корисника ове друштвене мреже које није у складу са принципима заштите података. Уз помоћ дугмета „Свиђа ми се“ корисници Facebook мреже се аутоматски разврставају према својим афинитетима, а прикупљени подаци се симају и складиште, али и прослеђују компанијама за чији су садржај корисници показали интересовање.

Када би неки корисник хтео да деактивира свој налог, политика мреже му то не дозвољава да одједном учини. Налог се најпре „ставља на чекање” и за то време није видљив другим корисницима друштвене мреже. Све информације

[153] Рекламирање прилагођено понашању корисника (енгл. *“Behavioural Advertising“)* представља посебну врсту рекламирања на интернету којом се посматра кретање корисника на интернету и који се садржају претражују како би им се приказао одређени рекламни материјал уз помоћ реклама (тзв.банера). *Видети*: Дилигенски, Андреј, Прља, Драган: „Фејсбук и право“, Институт за упоредно право, Београд, 2014.година, стр. 10

које су биле објављене приликом деактивирања налога се не бришу, чак ни након деактивирања налога. За деактивацију налога потребно је око месец дана, док неке информације могу да остану у резервним копијама и евиденцијама до 90 дана.

Интересантан је податак да је ова друштвена мрежа користила незнање корисника и њихове личне податке чинила доступним без њихове сагласности. Још 2007. године Facebook је почео да користи тзв. Бикон програм (Beacon program) који је имао за задатак да пријављује интернет активности корисника свим његовим „пријатељима" и рекламним агенцијама, што је разбеснело милионе корисника ове друштвене мреже.[154] На тај начин, свака куповина коју би преко интернета неки Facebook корисник обавио или услуга коју је неко користио била би смештена у ажурирање активности (енгл. News Feed) и доступна на увид свим интернет пријатељима тог корисника. Корисник при том није ни свестан да је у секунди цело интернет друштво упознато са његовом активности, нити да под подешавањима која се односе на приватност корисник ову опцију не може никако да трајно искључи или бар привремено блокира. Разлог за коришћење овог програма од стране друштвене мреже био је економске природе: одређени корисник наизглед „препоручује" особама са којима је у контакту преко друштвене мреже одређене услуге и производе и на тај начин „рекламира" одређене компаније. Facebook је тек 2009. године у потпуности престао са коришћењем овог програма после бројних критика Електронског информационом центра за заштиту приватности (Electronic Privacy Information Center – EPIC).[155]

Познат је случај да је група EPIC поднела жалбу пред Федералном трговинском комисијом САД због софтвера за аутоматско препознавање лица које Facebook користи приликом употребе опције "tag".[156] Од Федералне трговинске комисије САД било је затражено да детаљно испита и истражи легитимност ове опције аутоматског препознавања лица јер не постоји претходно дата сагласност корисника за примену овакве радње, као и да захтева

[154] Фејсбук - Политика о коришћењу података:Информације добијене од корисника, Deleting and deacrivating your account, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године
[155] Spinello, Richard, *op.cit.,* 2011., стр. 43
[156] Прља, Драган, Дилигенски , Андреј, *op.cit.*, 2012, стр. 202

строжије стандарде за заштиту приватности. Facebook политика непоштовања приватности је 2009. године покренула бројне акције како би се заштитила приватност корисника ове друштвене мреже, на тај начин што ова друштвена мрежа не би смела да у јавност прослеђује личне податке попут корисничког имена, слике и пола корисника. Због активности EPIC и јавне критике која је расла из дана у дан, Facebook је променио своју политику приватности најпре 2010. године, омогућавајући корисницима да подешавањима свог корисничког налога утичу на доступност и видљивост личних података, а затим и 2014. године када је укинуто правило да су све почетне опције нових чланова подешене на јавну видљивост података већ ће подаци корисника бити од момента приступања мрежи бити видљиви у потпуности само њиховим пријатељима.[157] Ово ново правило примењује се и на фотографије и на прве две фотографије које представљају кориснички профил.

Упркос напретку у чувању приватности које Facebook пласира и даље постоји неколико „слабих тачака“ које угрожавају приватност личних података корисника ове друштвене мреже. На пример, приликом претраге одређеног имена преко Google претраживача, прва опција која се добија као резултат претраге је комплетан Facebook налог, уколико он постоји. Један од проблема на који је већ сугерисано од стране EPIC (EPIC 2011) је и могућност заштите података попут адресе и телефонског броја корисника, који су сада, уколико су унети у кориснички профил, доступни свима.[158]

Канадска невладина организација која се бави политиком Интернета и јавним интересом (Canadian Internet Policy and Public Interest Clinic – CIPPIC)[159] упутила је Канцеларији повереника за приватност информација Канаде (Office of the Privacy Commissioner – OPC)[160] притужбе како је на више начина извршена повреда приватности корисника друштвене мреже Facebook: неовлашћеним прикупљањем различитих података о личности, неовлашћено

[157] 24 сата, http://www.24sata.rs/specijal/it/vest/veca-privatnost-profile-novih-korisnika-i-cover-slike-videce-samo-prijatelji/137514.phtml , претражено 26. 05. 2014. године
[158] *Ibid.*
[159] Canadian Internet Policy and Public Interest Clinic – CIPPIC, https://cippic.ca/, претражено 14. 06. 2015. године
[160] Office of the Privacy Commissioner – OPC, https://www.priv.gc.ca/index_e.ASP, претражено 14. 06. 2015. године

давање личних података корисника трећим лицима у сврху рекламирања и сл.).[161]

Facebook почев од јануара 2015. године уводи одређена нова правила када је у питању приватност личних података корисника ове друштвене мреже који се објављују и који су видљиви широком кругу корисника. У домену заштите приватности корисника,[162] Facebook се потрудио да детаљно појасни како сам корисник види свој профил, како тај профил виде други корисници и како корисници могу међусобно да комуницирају. Овим изменама је само побољшан начин заштите корисника у односу на друге кориснике, јер је могуће одредити које ће информације бити коме доступне и приказане. Такође, ове новине дозвољавају и да се ограничи број корисника који могу објављивати своје постове на нечијем профилу као и контролисано обележавање људи на фотографијама које се објављују, чиме се донекле спречавају подругљиви постови и насиље које настаје на овај начин.[163] Ипак, на овај начин је кориснику ове друштвене мреже само појашњено шта може сам да учини како би од других корисника покушао да сачува своју приватност, али још увек није решен проблем како сама друштвена мрежа и у којој мери сме да располаже личним подацима које јој корисници, саглашавајући се са правилима коришћења, остављају „на чување“.

Најпознатији сигурносни пропуст на овој друштвеној мрежи[164] везан је за учитавање фотографија на кориснички профил, јер том приликом корисник мора да у свој рачунар учита ActiveX контролу уз коју је био „прикачен” и злонамерни програм због кога је нападач био у могућности да добије приступ подацима из корисниковог рачунара. На овој друштвеној мрежи више пута се догодило да су нападачи на непознат начин успели да отуђе корисничка имена и лозинке одређених корисника, па тако угрозе приватност свих података који се налазе на њиховим профилима.

Највећи број судских спорова који су покренути и вођени против друштвене мреже Facebook односе се на сакупљање података уз помоћ

[161] *Видети:* Томић, Наташа, Петровић, Далибор, *op.cit.*, 2009., стр. 99
[162] Facebook, https://www.facebook.com/about/basics, претражено 29. 11. 2014. године
[163] Facebook, https://www.facebook.com/about/basics/how-others-interact-with-you/, претражено 29. 11. 2014. године
[164] Сигурносни ризици друштвених мрежа, Хрватска академска и истраживачка мрежа, www.cert.hr, претражено 17. 03. 2015. године

„колачића" и дугмета „Свиђа ми се". Један од најпознатијих случајева је свакако случај Макса Шремса, који је затражио од друштвене мреже Facebook да му достави све податке које има сакупљене о њему.[165] За период од 3 године коришћења друштвене мреже, Facebook је сакупио 1.222 странице А4 формата личних података.[166] Највише пажње је привукла чињеница да су информације које је Макс Шремс обрисао са друштвене мреже (попут обележавањима на фотографијама, обрисаних порука, обрисаних пријатеља, промењених имена корисника и сл.) остале и даље у Facebook архивама.

Никола – Ник Чубриловић, Србин који живи у Аустралији, открио је да Facebook не брише „колачиће" који са друштвене мреже шаљу податке на рачунар корисника и обрнуто, чиме прикупља информације о имену корисника, лозинкама, сајтовима које посећује, и на тај начин врши тешку повреду приватности својих корисника.[167] Он је тврдио да када се корисници одјаве са Facebook мреже, мрежа и даље прати њихово кретање по сајтовима који имају дугме „Свиђа ми се" и на овај начин злоупотребљавају податке.

Коришћењем дугмета „Свиђа ми се" нису повређена само права појединаца, већ и различитих компанија, државних институција па чак и локалних самоуправа. На веб сајту града Хамбурга (www.hamburg.de) постављено је „Свиђа ми се" дугме. Град Хамбург је, сумњајући у допуштеност оваквог начина прикупљања података, захтевао мишљење од Facebook компаније у вези са начином коришћења ове функције. Facebook је одговорио да се обрада података заиста врши, као и да се сакупљени подаци бришу након три месеца од њиховог сакупљања. Како Град није био задовољан одговором који је добио, администратори званичне презентације Града су са своје странице уклонили дугме „Свиђа ми се".[168] Слично су поступиле и власти немачке покрајине Шлезвиг-Холштајн, које су са друштвене мреже Facebook уклониле и дугме „Свиђа ми се" и страну за обожаваоце коју су имали на овој друштрвеној мрежи.[169]

---

[165] Прља, Драган, Дилигенски , Андреј, *op.cit.*, 2012, стр. 193
[166] europe-v-facebook.org, наведено код *Ibid.*
[167] Курир- дневна новина од 30. 09. 2011. године : „Ексклузивно: Србин који је разбио Фејсбук", http://www.kurir.rs/ekskluzivno-srbin-koji-je-razbio-fejsbuk-clanak-113719, претражено 14. 08. 2012. године
[168] *Наведено код:* Прља, Драган, Дилигенски , Андреј, *op.cit.*, 2014, стр. 14
[169] *Ibid.*

2.3.2. Twitter

Када корисник креира или реконструише Twitter налог, обавезан је да остави неке податке о себи: име, корисничко име, лозинку и електронску адресу. Сервери аутоматски евидентирају све податке (тзв. дневник података) креиране од стране корисника.[170] Самим учлањењем на друштвену мрежу, корисник даје дозволу мрежи да прикупља податке о њему, складишти их, манипулише њима, проследи их даље у одређеним сучајевима. Дневник података може да садржи информације као што су ИП адреса, тип претраживача, посећене странице, оператер мобилне телефоније корисника, најчешћи претраживани термини, интеракција са сајтом, апликацијама и рекламама. Twitter прикупља личне податке о својим корисницима, приватне и јавне поруке, јавне твитове или број корисника који су кликнули на одређену везу, и све ове податке може да дели са трећим лицима.[171]

Ова друштвена мрежа прикупља информације о регистрованим корисницима преко различитих интернет сајтова којима приступају корисници, апликација које користе, послатих твитова, обавештења и коришћених услуга. Самим моментом регистровања и приступања мрежи, корисник је дао сагласност да се његови лични подаци сакупљају, складиште и обрађују, али и да се под одређеним условима ови подаци и деле са неким другим компанијама. Могуће је такође да се подаци о корисницима поделе и са другим друштвеним мрежама, уколико исти корисник има отворен и регистрован налог и на некој другој друштвеној мрежи. Оваквим могућностима које ова друштвена мрежа нуди потврђује се намена мреже – глобална размена информација.[172] Корисницима је остављен избор да сами прилагоде приватност информација које су објављене на профилу.

Што се тиче „трговине" прикупљеним подацима од корисника, Twitter задржава право да прода све сакупљене информације ако дође до промене

---

[170] Твитер - Политика приватности - Скупљање,коришћење и измена корисничких података, https://twitter.com/privacy, претражено 04. 08. 2012. године

[171] *Видети:* Rushe, Dominic: „Icelandic MP Fights US Demand for Her Twitter Account Details", *The Guardian*, January 8, 2011, http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages, претражено 04. 08. 2012. године

[172] Самчовић, Андреја: „Безбедност друштвених мрежа са освртом на Twitter", INFOTEH-JAHORINA Vol. 12, 2013., стр. 861, http://infoteh.etf.unssa.rs.ba/zbornik/2013/radovi/RSS-5/RSS-5-9.pdf, претражено 06. 08. 2015. године

власника мреже. Када је налог на овој друштвеној мрежи деактивиран, он се не брише 30 дана. Тек након истека овог периода почиње процес брисања налога, што може да потраје и до недељу дана.[173] Политика приватности ове друштвене мреже је јасна када могуће откривати податке које је корисник оставио на мрежи: у случају сарадње са полицијом или владиним телима, у случају откривања превара или заштите безбедности неке особе, нечијих права или имовине мрежа је дужна да открије тражене податке одређеног корисника.[174]

До сада је било више сигурносних пропуста на друштвеној мрежи Twitter али су забележени и случајеви грубог кршења права на приватност.

Интересантан пример злоупотребе права на приватност догодио се јануара 2011. године, када је влада Сједињених Америчких Држава уручила овој друштвеној мрежи судски налог за откривање информација о неким корисницима који су били умешани у случајеве Викиликса (WikiLeaks). Интересантан је случај Бригите Јорнсдотр (Birgitta Jonsdottir), посланице у Исландском парламенту и некадашњег волонтера Викиликса, која тренутно води судски спор са америчким правосудним системом због покушаја да се искористе њене приватне поруке које је слала и примала преко друштвене мреже Twitter почев од 1. новембра 2009.године. Јорнсдотр је изјавила како је свесна да се овде не ради само о њеним информацијама, већ да је ово упозорење свима који су сарађивали са Викиликсом. Њу, као посланицу државног парламента од јавног коришћења и објављивања приватних порука штити посланички имунитет, али шта ће се десити са обичним људима који се из неког разлога нађу у сличној ситуацији? [175] Twitter је реаговао опозивањем судског налога, залажући се за идеју да би корисници интернета требало да буду обавештени и да им се пружи прилика да одбране своја уставна права пред судом пре него што буду компромитована.

Један од најпознатијих сигурносних пропуста на овој друштвеној мрежи је пропуст везан за дозвољавање извршавања произвољног програмског кода на

---

[173] Твитер - Политика приватности - Скупљање, коришћење и измена корисничких података, https://twitter.com/privacy, претражено 04. 08. 2012. године
[174] Ibid.
[175] Government Requests For Twitter Users' Personal Information Raise Serious Constitutional Concerns, Says ACLU, ACLU – American Civil Liberty Union, 2011, http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu, претражено 12. 08. 2012. године

нечијем профилу, што је искористио црв StalkDaily, који се ширио мрежом самим прегледавањем профила корисника.[176] Још једно од опасних угрожавања безбедности личних података о корисницима догодило се када је хакер под надимком „Hacker Croll“ успео да уђе у сандуче електронске поште једног од администратора ове друштвене мреже и да украде корисничко име и лозинку за целокупну друштвену мрежу, чиме је довео у опасност приватност милиона корисника мреже.[177]

2.3.3. LinkedIn

Као и приликом регистрације на Facebook или Twitter, приликом регистрације на LinkedIn информације о корисницима обухватају име, е-адресу, занимање и послодавца, земљу корисника и лозинку. Податке је могуће прикупити и када их корисник изричито не даје већ приликом прегледа и коришћења веб страница са исте ИП адресе, при чему је могуће добити и ИП адресу корисника, тип коришћених претраживача, оперативни систем који се користи и адресе свих посећиваних сајтова у којима су уграђене технологије LinkedIn платформе.

Интересантна је одредба да прикупљене податке LinkedIn не може продавати, изнајмити или делити трећим лицима без пристанка корисника, осим уколико је то неопходно партнерима LinkedIn у пружању услуга[178]. LinkedIn се ограђује од неовлашћеног коришћења личних података на следећи начин: „Личне информације корисника биће безбедне у складу са индустријским стандардима и технологијама. Пошто интернет није околина која је 100% сигурна, не можемо да гарантујемо или обезбедимо сигурност било које информације коју поставите на LinkedIn. Не постоји гаранција да информацијама неће бити приступано, да неће бити копиране, мењане, подељене са другима или уништене”.[179] LinkedIn чува податке све док је кориснички налог активан.

---

[176] “Сигурносни ризици друштвених мрежа”, Хрватска академска и истраживачка мрежа, www.cert.hr, претражено 17.03.2015.године
[177] *Ibid.*
[178] LinkedIn - Политика приватности, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, претражено 04. 08. 2012. године
[179] *Ibid.*

Подаци о регистрованим корисницима или информације које су објављивали корисници могу бити у следећим случајевима подељени са трећим лицима тек након добијања изричите сагласности: (1) уколико су битни за вођење судског поступка, издавања судског налога или изрицање било какве правне санкције; (2) због поштовања Уговора о условима коришћења услуга мреже; (3) ако неки други корисник пријави да је дошло до кршења правила понашања на мрежи; (4) ако је у интересу заштите нечијих права, имовине или личне сигурности.

Сигурносни пропусти на овој друштвеној мрежи манифестују се најчешће преко нежељених порука, јер корисници веома често примају поруке од администратора мреже или осталих корисника.[180]

[180] „Сигурносни ризици друштвених мрежа", Хрватска академска и истраживачка мрежа, www.cert.hr, претражено 17. 03. 2015. године

2.4. Интернет права и принципи за заштиту људских права

Динамична коалиција за интернет права и принципе (Internet Rights and Principles Dynamic Coalition - IRP)[181] представља мрежу коју чине појединци и организације из целог света делујућу уједињено у циљу да очувају и заштите људска права у виртуелној средини. Рад ове коалиције се базира на раду Интернет форума Уједињених нација (UN Internet Governance Forum), који окупља владе земаља чланица, пословне партнере и организације цивилног друштва како би се расправљало о свим заједничким проблемима и питањима који задиру у домен интернет права и управљања.[182] Коалиција се до сада бавила применом досадашњих принципа очувања људских права у интернет окружењу, као и изградњи свести, разумевања и заједничке платформе за мобилизацију око права и принципа за интернет. Како би сви корисници интернета поштовали и штитили људска права на интернету, Коалиција је заузела став да се морају предузети одређени кораци како би се осигурало да Интернет функционише и еволвира на начине који поштују људска права до максималних размера.

Како би помогли да се оствари визија Интернета као средства за остваривање људских права, Коалиција је усвојила 10 права и принципа:[183]

(1) Универзалност и једнакост – сви људи су рођени слободни и једнаки, у достојанству и са правима која се морају поштовати и остваривати у Интернет окружењу;

(2) Права и социјална правда – Интернет је простор за промоцију, заштиту и остваривање људских права као и за унапређење социјалне правде. Обавеза свих је да поштују људска права других у виртуелном окружењу;

(3) Приступ интернету – сви људи имају једнака права на приступ и употребу сигурног и отвореног Интернета;

---

[181] Internet Rights and Principles Dynamic Coalition (IRP): Internet rights & Principles Charter - Internet rights & Principes, http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet-English_4thedition.pdf, претражено 06. 08. 2015. године

[182] Internet Governance Forum, http://www.intgovforum.org/cms, претражено 28. 08. 2015. године.

[183] Internet Rights and Principles Dynamic Coalition (IRP): Internet rights & Principles Charter - Internet rights & Principes, http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet-English_4thedition.pdf, претражено 06. 08. 2015. године

(4) Изражавање и удруживање – свако има право да слободно тражи, прима и дели информације на Интернету, без цензуре или других уплитања. Такође, свако има право да се слободно удружује путем Интернета у циљу постизања друштвених, културних или сличних циљева;

(5) Приватност и заштита података – свако има право на приватност у Интернет окружењу. То подразумева и слободу од надгледања, право на коришћење енкрипције и право на анонимност. Свако има право на заштиту података, укључујући контролу над личним подацима, чување, обрађивање, располагање и објављивање истих;

(6) Живот, слобода и сигурност – У Интернет окружењу морају да се поштују, заштите и остварују право на живот, слободу и сигурност. Ова права не смеју да се крше или користе како би се прекршила нека друга права у Интернет окружењу;

(7) Различитост – на Интернету мора да се промовише културни и језички диверзитет, а да се подстичу техничке и политичке иновације у циљу подршке плурализму;

(8) Једнакост на мрежи – свако треба да има једнак или отворен приступ садржајима на Интернету, без дискриминаторског фаворизовања, филтерисања или контроле коришћења Интернета у комерцијалне, политичке или друге сврхе;

(9) Стандарди и регулација – структура Интернета, комуникацијски системи и формати докумената и података морају да буду засновани на отвореним стандардима који осигуравају пуну интероперабилност, укљученост и једнаке прилике за све;

(10) Управљање – људска права и социјална правда морају да буду правне и нормативне основе на којима ће Интернет да функционише и да буде уређен. Ово треба да се одвија на транспарентан и мултилатералан начин, да буде засновано на принципима отворености, језичког учешћа свих и одговорности.

Сви ови принципи су детаљно разрађени у **Повељи људских права и принципа на Интернету,**[184] која представља заједнички стандард који мора да се достигне. Сваки појединац и сваки орган управљања друштвом мора да ради на промоцији поштовања ових права и слобода, као и да предузима све неопходне мере да обезбеди њихово препознавање. Такође, сваки корисник Интернета има дужност и одговорност да мора да поштује права других корисника Повељом се гарантују: *право на приступ интернету*, а посебно квалитет пружене услуге, слобода избора оперативног система и програма који се користе, дигитализацију, једнакост и неутралност интернет мрежа; *право на недискриминацију приликом омогућавања, коришћења и управљања интернет приступом*, које подразумева једнакост приступа, присутност маргинализованих група и подржавање родне једнакости; *право на слободан и сигуран Интернет,* у оквиру кога се подразумева заштита од свих облика криминалитета као и сигурност Интернета; *право на развој кроз Интернет* које делује у циљу смањења сиромаштва, модернизацију људског развоја и одрживи развој уопште; *слобода изражавања и доступних информација на Интернету*, у оквиру које се подразумева слобода изражавања протеста преко интернета, слобода од цензуре, право на информације, слобода медија и непостојање говора мржње на Интернету; *право на верско опредељење и изражавање преко Интернета; слобода организовања и удруживања преко Интернета; право на приватност на Интернету,* које подразумева доношење националних прописа који се односе на приватност, развијање политика приватности и могућности њиховог подешавања на Интернету, постојање стандарда поверљивости и интегритета ИТ система, заштита виртуелне персоналности, право на анонимност и коришћење енкрипције, непостојањее надгледања Интернет комуникације, немогућност ширења гласина и клевета преко Интернета; *право на заштиту дигиталних података* које подразумева заштиту личних података, обавезу сакупљања података, постојање минимума стандарда за коришћење личних података и надгледање Интернета од стране независних органа за заштиту података.

[184] Internet Rights and Principles Dynamic Coalition (IRP): Internet rights & Principles Charter - Internet rights & Principes, http://internetrightsandprinciples.org/wpcharter, претражено 06. 08. 2015. године

Повељом се такође гарантују: *право на едукацију за коришћење Интернета*, које се реализује кроз образовање путем Интернета и едукацију о поштовању људских права при коришћењу Интернета; *право на културу и приступ знању преко Интернета* је право које подразумева право на учешће у културном животу друштва, различитост језика и култура, право на коришћење матерњег језика, непостојање забрана у области културе и приступа знању преко Интернета, доступност бесплатних софтвера и отворених стандарда; *права деце на Интернету*, од којих су посебно препозната право на добробит од коришћења Интернета, право детета да не буде искоришћавано и узнемиравано насилним сликама преко Интернета, право да се дечији глас чује, поступање у најбољем интересу детета; *права особа са инвалидитетом на Интернету*, која подразумевају право на приступ Интернету и право да приуште себи Интернет; *право на рад и Интернет*, при чему се мисли на поштовање права радника, Интернет и радно окружење, као и на рад преко Интернета; *право да се учествује у одлучивању о питањима од јавног значаја преко Интернета;право на заштиту потрошача преко Интернета; право на здравствени и социјални систем заштите преко Интернета,* које обухвата и доступност здравствених служби преко Интернета; *право на правни лек и на фер суђење*; *право на одговарајући друштвени и међународни поредак на Интернету*, које подразумева поштовање људских права, вишејезичност и различитост на Интернету као и ефективно учествовање креирању глобалне политике преко Интернета.

Циљ Повеље је, поред осталог, стварање почетне тачке дијалога и сарадње између различитих интересних група, правни оквир за стварање норми на локалном, националном и глобалном нивоу које ће се бавити Интернет управљањем, као и стварање одговарајуће политике и механизама лобирања за владе, предузећа и групе цивилног друштва које су посвећене развоју основних принципа Интернета.

3. Безбедносни ризици на друштвеним мрежама и препоруке за њихово смањивање

Убрзани развој технологије омогућио је све бржу обраду података и ефикасно функционисање као и доступност бројних информација, истовремено обезбеђујући појединцу да као део огромне базе података остане „анониман". Чувени магазин The New Yorker је још 1993. године почео да објављује стрип који је поручивао да „на интернету, нико не зна да си пас"[185] и да је на интернету до те мере тешко открити нечији идентитет да су могућности злоупотребе небројене. У циљу борбе против свих видова компјутерског криминалитета, било је једино могуће контролисати приступ компјутерском систему аутоматски, 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.

Друштвене мреже се могу злоупотребљавати на разне начине, а криминалитет који се реализује на овај начин може имати облик било ког од традиционалних видова криминалитета. Забринутост великог броја корисника интернета изазива чињеница да се информације које се тичу њих самих аутоматски генеришу, прикупљају, складиште, међусобно повезују и користе у различите сврхе, укључујући комерцијалне, па и незаконите.[186]

Подацима о индивидуама који се неовлашћено прибављају злоупотребом информационих система може се на разне начине манипулисати. Откривањем великог броја личних података корисници заправо свесно се одричу дела своје приватности јер се на овај начин прави једна богата колекција личних података о корисницима. Поред тога, постављање фотографија може да омогући идентификацију корисника помоћу програмских алата за препознавање лица, али и место на коме се корисник на тој фотографији налази. Још једна од

[185] Steiner, 1993, наведено код Hargittai, Eszter: "Whose Space? Differences Among Users and Non-Users of Social Network Sites", Journal of Computer-Mediated Communication, volume 13, issue 1, стр. 276-297, октобар 2007, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00396.x/full, претражено 13. 04. 2013. године

[186] Спасић, Видоје: „Онлајн безбедност", Зборник Правног факултета у Нишу, Ниш: Правни факултет, Центар за публикације, 2010. - бр. 56 (2010), стр. 78

потенцијалних опасности налази се у чињеници да на појединим друштвеним мрежама није могуће обрисати све податке које садржи кориснички профил, већ је могуће само деактивирати профил чиме подаци и даље остају похрањени негде у виртуелном простору.

У Европи број корисника друштвених мрежа који су пријавили да су били жртва напада на приватност на некој од друштвених мрежа је са 6% (2009. година), најпре повећан на 12% (2010. година) а затим на 15% (2011. година).[187] У САД овај број је са 8% (2009. година) порастао на 18% (2011. година).[188]

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 већину неовлашћених приступа.

Међутим, примери указују и на другу страну напретка. Управо овакав вид „улажења у траг" извршиоцима различитих облика сајбер криминалитета довео је до све чешћих глобалних напада 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.

Интернет корисници могу да заштите своју приватност преко контролисаног откривања личних информација. Објављивање „постова" и личних информација на интернету може бити штетно за приватност појединца јер су информације (блогови, слике и интернет стране) које су једном објављене на интернету трајне. Угрожавање података (безбедности) може да буде разноврсно, али се најчешће, зависно од утицаја потенцијалних нападача на ток информација, карактерише као *активно* (промена садржаја информација или њиховог тока, као и модификација мрежних пакета, производња неовлашћених мрежних пакета или прекид информационог тока) и *пасивно* (које подразумева

[187] Cybercrime on social networks continues to climb, http://www.net-security.org/secworld.php?id=11464, претражено 04. 10. 2013. године
[188] *Ibid.*

све облике утицаја на ток информација, без активних измена у самом току, нпр. прислушкивање, надгледање и сл).[189]

Поставља се питање до које је мере за функционисање једног модерног друштва потребно и оправдано прикупљање личних података, као и колики је обим права осталих корисника друштвених мрежа приликом коришћења и располагања туђим личним подацима. 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. Према правилима коришћења најпопуларнијих друштвених мрежа, коришћење личних података дозвољено је само регистрованим корисницима.

Интересантно је да је децембра 2013. године осам најутицајнијих технолошких компанија на свету (Google, Apple, Facebook, AOL, Twitter, Microsoft, LinkedIn и Yahoo) заједнички упутило захтев председнику САД и америчком Конгресу да престану са надзором и неовлашћеним праћењем корисника друштвених мрежа, као и да уведу строгу контролу активности тајне службе.[190] Ови гиганти информационих технологија, који су међусобно једни другима најоштрији конкуренти, били су принуђени на овај корак након што је Едвард Сноуден открио да америчке власти имају директан приступ њиховим серверима захваљујући договору са провајдерима, чиме константно надгледају грађане и њихове активности. Twitter је коришћен како би се, на основу поштанског броја места из кога се шаљу поруке (тј. „твитује") и презимена корисника, добила адреса стана, број телефона и електронска пошта тог корисника; Facebook је коришћен за праћење конекција корисника, почев од новембра 2010.године када су промењена правила надзора и када је држава добила дозволу да контролише грађане, а Google је коришћен за надзор коресподенције која се водила између корисника што је обухватало дужину трајања позива преко мреже, серијски број мобилног уређаја као и потенцијалну локацију учесника у разговору. На основу свих података до којих су дошле, ове

[189] Спасић, Видоје*, op.cit.,* 2010, стр. 80

[190] Блиц – дневна новина од 10.12.2013.године, www.blic.rs, дневна новина „Блиц" од 10. 12. 2013. године, претражено 10. 12. 2013. године

компаније су председнику САД и америчком Конгресу упутиле следеће захтеве: ограничити овлашћења влада за прикупљање информација о корисницима и свести их у законске оквире, владина овлашћења треба да контролишу независни судови, а све важне пресуде треба да се објаве и изложе суду јавности, транспарентност налаже да владе дозволе компанијама да објаве број и природу захтева за приступ информацијама, владе не смеју да ограничавају које компаније или појединци имају право на легалан приступ информацијама и владе морају да ускладе законе о прикупљању информација.[191]

Приватност на друштвеним мрежама зависи и од степена контроле коју корисник друштвене мреже има над приступом и употребом личних података. Углавном сви сајтови којима се приступа на различите друштвене мреже захтевају од корисника да прихвати полису о условима коришћења (енгл.Terms of acceptance, Terms of use) пре него што му допусте да користи њихове услуге. Интересантно је да управо та полиса о условима коришћења често садржи клаузуле којима је дозвољено операторима друштвених мрежа не само да складиште податке о корисницима, већ и да их деле трећим лицима, најчешће маркетиншким компанијама.[192] Грешка највећег броја корисника је што ове полисе прихватају без претходног читања, јер су оне за корисника неразумљиве и преобимне, а често постоје само на енглеском језику па је њихово разумевање за просечног корисника прилично тешко.

Решење које би смањило могућност злоупотребе права на приватност на интернету, а посебно на друштвеним мрежама, мора да се заснива на три различита нивоа – решавање друштвених проблема услед којих долази до злоупотребе права на приватност, превазилажење техничких проблема услед чијег постојања је неовлашћеним лицима омогућено да дођу до туђих личних података и стварањем адекватног правног оквира и механизама за откривање, спречавање и санкционисање дела која се изврше. За решавање друштвених проблема који резултују последицом повреде права на приватност су од кључног значаја породица и околина у којој корисник проводи време (школа,

[191] *Ibid.*
[192] Bangeman, Eric: "2010. Report: Facebook caught sharing secret data with advisers", http://arstechnica.com/tech-policy/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers/, претражено 04. 10. 2013. године

посао, градска или рурална средина).[193] Политика сваке од друштвених мрежа је да води рачуна о техничким могућностима које би злоупотребе података онемогућиле или свеле на најмању могућу меру.[194] Друштвена мрежа MySpace нпр.је имала софтвер који је омогућавао да се „препознају" деца која имају мање од 14 година и „забрањивао" им је да се прикључе овој друштвеној мрежи.[195] Адекватним правним нормирањем на наднационалном нивоу било би олакшано сазнавање за повреде права на приватност као и санкционисање учинилаца ових дела.

ЕУ је 2004. године формирала Европску агенцију за безбедност мрежа и информационих система (ENISA),[196] а затим почетком 2007. усвојила Стратегију за безбедно информационо друштво у Европи,[197] чији је циљ био да се препозна дијалог, партнерски однос и оспособљавање кључних актера, побољшају безбедности мрежа и информација, ојача ENISA и подрже напори држава чланица за постизање синергије.[198] Као потенцијалне претње сигурности друштвених мрежа, ENISA је у свом документу број 1[199] све уочене претње поделила у 4 категорије:

Прва категорија обухвата **претње приватности корисника**, у које спадају ***стварање базе личних података корисника (тзв. „дигиталних досијеа"),*** јер се сви подаци са друштвених мрежа могу учитати на било чији рачунар и тако учитани чувати; ***сакупљање пратећих података о активностима корисника*****,** као нпр. подаци о трајању боравка на мрежи, профили корисника који су посећивали, послате поруке; ***програми за препознавање лица на фотографијама корисника*****,** јер фотографија представља

---

[193] Barnes, Susan, *op.cit.,* 2006.
[194] Duffy, Michael: "A dad's encounter with the vortex of Facebook," http://www.time.com/time/magazine/article/0,9171,1174704,00.html, претражено 23. 01. 2015. године
[195] State wants MySpace to raise minimum age, Reuters, 2006, http://www.rapidnewswire.com/5036-myspace-0245.htm, претражено 29. 12. 2013. године
[196] Видети European Union Agency for Network and Information Security, http://www.enisa.europa.eu/
[197] Стратегија за безбедно информационо друштво у Европи –Strategy for a Secure Information Society in Europe "Dialogue, partnership, and empowerment", http://ec.europa.eu/information_society/doc/com2006251.pdf , претражено 21. 11. 2014. године
[198] Резолуција Европског Савета бр. 2007/C 68/ –European Council Resolution 2007/C 68/01, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007G0324(01)&from=EN, претражено 21. 11. 2014. године
[199] ENISA Position Paper No.1: Security Issues and Recommendations for Online Social Networks, 2007, http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks , претражено 19. 03. 2015. године

бинарни идентификатор корисника; ***препознавање простора/места са фотографије; могућност повезивања слика и података из целе мреже***, јер све друштвене мреже дозвољавају корисницима да означавају људе и места на фотографијама што може да доведе до бесконачног укрштања података и њихове размене без знања и воље корисника; ***немогућност да се у потпуности избрише кориснички налог***, јер чак и ако корисник успе да избрише све податке које је објављивао, неће моћи да обрише коментаре које су њему писали други или оне које је он постављао на корисничке налоге других људи;

Другу категорију чине **претње друштвеним мрежама и безбедности информација**, у које спадају ***слање нежељених порука*** (тзв. спамовање); ***слање злонамерних програма*** (вируси и црви); ***могућност размене података између друштвених мрежа без знања корисника***;

Трећа категорија су **претње по идентитет**, у које спадају ***опасност од интернет превара (фишинга)***, јер су друштвене мреже веома осетљиве на различите злонамерне програме којима је могуће изазвати да се овакви линкови који преусмеравају на сајтове за преварне радње аутоматски корисницима отварају; ***брзо ширење информација***, иако многе друштвене мреже видљивост података ограничавају само на кориснике означене као "пријатељи", нове конекције се лако склапају па се тако и подаци о корисницима брзо шире; ***могућност преузимања нечијег идентитета***, јер је могуће регистровати кориснички налог на било чије име а интернет омогућава да се свако сакрије иза анонимности;

Четврту категорију чине **друштвене претње**, у које спадају: ***прогањање преко друштвене мреже***, које се манифестује претећим понашањем где починилац више пута контактира жртву електронским путевима комуникације, попут електронске поште, причаоница или форума; ***малтретирање и узнемиравање***, које може да се манифестује и дељењем приватних садржаја без знања корисника; ***корпоративна шпијунажа***, која се манифестује тако што се пропусти друштвених мрежа користе за убацивање злонамерних програма којима се руши корпоративна инсфраструктура њихових информационих технологија.

У истом документу дате су и одређене **препоруке**, на који је начин се може значајно смањити могућност злоупотребе друштвених мрежа:[200]

1. **препоруке које се односе на владине регулаторне политике:** охрабрити подизање свести и организовање едукативних кампања; ревидирање правне регулативе у овој области; повећање транспарентности руковања подацима који се налазе на друштвеним мрежама; забранити коришћење друштвених мрежа по школама;

2. **препоруке интернет провајдерима**: промовисати јачу проверу идентитета приликом коришћења друштвених мрежа и појачати контролу приступа; спровести одговарајуће мере како би се спречила корпоративна шпијунажа; повећати могућности за пријављивање злоупотребе података на друштвеним мрежама; омогућити да почетна подешавања корисничких профила буду подешена у циљу заштите приватности личних података које су корисници објавили;

3. **техничке препоруке**: омогућити да оператери могу да у потпуности обришу са друштвене мреже податке корисника који то желе; подстицати употребу само проверених и безбедоносно доказаних техничких могућности; осмислити аутоматске филтере за злонамерне програме који се шире преко друштвених мрежа и омогућавају крађу личних података од корисника; учинити обавезним добијање сагласности од корисника друштвене мреже за свако означавање на фотографијама; увести рестриктивно учитавање личних података са друштвених мрежа; обратити посебну пажњу на резултате који се добијају коришћењем различитих претраживача, јер многи корисници друштвених мрежа нису свесни колико се личних података пронађе претрагом њиховог имена преко претраживача; израдити одговарајуће програме којима би било могуће елиминисати намерно затрпавање поште нежељеним порукама; преточити у правну регулативу све примере добре праксе којима је могуће спречити преваре на интернету;

4. **препоруке у области истраживања и стандардизације**: омогућити да се не открива идентитет особа на фотографијама већ да све особе буду анонимне, осим ако не постоји њихов пристанак на објаву фотографије;

---

[200] *Ibid.*

промовисати мобилне друштвене мреже; спровести што више истраживања која би појаснила спону између стварног и виртуелног света, злоупотребе које се јављају на друштвеним мрежама као и могућу већу заступљеност мобилних друштвених мрежа.

Међународна радна група за заштиту података у телекомуникацијама (тзв. Берлинска група, International Working Group on Data Protection in Telecommunications)[201] објавила је 2008. године извештај и водич о заштити приватности, који садржи битне смернице за провајдере, администраторе сервиса за друштвено умрежавање и кориснике друштвених мрежа, које су познате под називом „Римски меморандум“.[202] Овај документ истиче ризике по приватност и безбедност корисника друштвених мрежа, при чему су као највеће претње препознате:

1. Чињеница да се на Интернету се ништа не заборавља – подаци који се објаве остају на Интернету буквално заувек, јер чак и када их неко обрише, постоји могућност да их је нека трећа особа већ запамтила, а постоје и друштвене мреже које не бришу у потпуности профиле својих корисника;
2. стварање лажне слике „заједнице” – многе друштвене мреже наглашавају да се поштује приватност корисника и тајност објављених података тако што објављене податке могу да виде само контакти корисника („пријатељи”), што није у потпуности тачно;
3. појам „бесплатног” на Интернету – ништа заправо није бесплатно, јер корисник све плаћа кроз секундарну употребу његових личних података, које друштвене мреже и/или пружаоци услуга прослеђују другим компанијама (нпр. маркетинг агенцијама);
4. сакупљање података о кретању на Интернету и њихово дељење са другим корисницима и трећим лицима, које врше пружаоци услуга друштвеног умрежавања;

[201] International Working Group on Data Protection in Telecommunications, http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt, претражено 12. 09. 2015. године

[202] Report and Guidance on Privacy in Social Network Services - ”Rome Memorandum” - 43rd meeting, 3-4 March 2008, Rome (Italy), http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf, претражено 12. 09. 2015. године

5. потреба да се рефинансирају услуге и додатно заради могу да повећају сакупљање, обраду и коришћење података о корисницима;
6. обелодањивање више личних података него што је корисник имао намеру да обелодани – нпр.на основу објављене фотографије могуће је утврдити место на коме се корисник налази, друштво у коме се креће и сл.;
7. злоупотреба личних података објављених на профилу од стране трећих лица, која зависи од подешеног нивоа заштите приватности сваког корисничког профила и техничких безбедоносних услова којима свака од друштвених мрежа располаже;
8. ризик од крађе идентитета и „хаковања" корисничких профила;
9. коришћење несигурне инфраструктуре;
10. постојање безбедоносних проблема код самих пружаоца Интернет услуга и неуједначеност техничких могућности различитих друштвених мрежа.

Препоруке је радна група сврстала у 3 групе, а односе се на субјекте који креирају правне оквире (регулаторна тела), оне које пружају услуге друштвеног умрежавања (нпр. сервиси за друштвено умрежавање, интернет провајдери) као и за оне који користе услуге друштвеног умрежавања (кориснике):

(1) Препоруке које се односе на регулаторна тела: дозволити корисницима употребу псеудонима уместо правих имена; апеловати на сервисе за друштвена умрежавања да буду искрени и јасни када су у питању личне информације неопходне за основно коришћење друштвене мреже као и неопходност изричите сагласности власника податка за прослеђивање података; обавеза обавештавања корисника о покушајима крађе идентитета како би успели да побољшају своја безбедоносна подешавања; ревидирати правне прописе који се односе на право објављивања личних података на друштвене мреже; повећати интегрисаност питања која се тичу права на приватност у образовни систем;

(2) Препоруке које се односе на пружаоце услуга друштвеног умрежавања: пружаоци услуга морају да као приоритет имају очување сигурности и приватности објављених личних података својих корисника; давање транспарентних и отворених информација корисницима о обради и коришћењу личних података; омогућити

креирање профила под псеудонимом; одржавање обећања која су дата корисницима; аутоматска подешавања која штите безбедност и приватност корисника; побољшање контроле над подацима са корисничких профила и то од стране самих корисника; увести одговарајуће механизме за решавање притужби корисника друштвених мрежа; побољшати и одржавати сигурност информационог система; унапредити мере против илегалних активности попут слања спам порука и крађе идентитета; понудити енкриптоване конекције за одржавање профила (попут безбедоносног логовања); поштовање стандарда који се односе на приватност у свим земљама где пружају своје услуге;

(3) Препоруке које се односе на кориснике друштвених мрежа: корисници морају да буду пажљивији и да ажљиво размисле пре него што објаве неки лични податак; да пажљиво размисле да ли ће на профилу да напишу своје право име или да користе псеудоним; да поштују приватност других корисника друштвених мрежа и да не објављују туђе личне податке и фотографије без изричито добијене сагласности; да буду информисани о свим битним питањима која се тичу безбедности и заштите приватности на друштвеним мрежама; да користе подешавања која у највећој могућој мери штите приватност; да користе различите лозинке за приступ различитим налозима; да контролишу начине како пружаоци услуга чувају објављене личне податке, као и да посебно обрате пажњу на активности деце на Интернету а посебно на друштвеним мрежама.

ГЛАВА II

ЗЛОУПОТРЕБА ДРУШТВЕНИХ МРЕЖА КАО ОБЛИК КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

1. Појам, појавни облици и остале феноменолошке карактеристике компјутерског криминалитета

Компјутери и компјутерска технологија као савремена средства комуникације могу бити како предмет злоупотреба које се односе на угрожавање приватности корисника, доступност и/или поузданост рачунарских мрежа и телекомуникационих система, тако и средство за извршење традиционалних кривичних дела. Што је виши степен развијености одређеног друштва, веће су могућности за појаву и постојање најразноврснијих облика ове врсте криминалитета, начини извршења су разноврснији и софистицираније, а учиниоци су компетентнији и бројнији. Комуникација на социјалним мрежама и уопште дигитална комуникација доводи до креирања потпуно новог жаргонског језика, кога неки аутори (Prensky, M., 2001)[203] називају „дигитални језик“ или „језик дигиталних урођеника“. Основни елементи тог језика су скраћенице и ознаке за осећања и користећи знакове који постоје на тастатури, учесници у компјутерској комуникацији стварају визуелне изразе осећања. Скраћенице су неизоставни део свих четова, а настају због тога да се текстуални разговор по брзини што више приближи говорном.

Компјутерски криминалитет подразумева и активно и пасивно коришћење компјутера, па чак и чување доказа о извршеном кривичном делу у рачунару или у електронској форми,[204] а жртве и могуће жртве су сва физичка и

[203] Prensky, Marc: “Digital Natives, Digital Immigrants”, On the Horizon vol. 9 no. 5., 2001., http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf, претражено 03. 07. 2015. године

[204] Report and Guidance on Privacy in Social Network Services - ”Rome Memorandum” - 43rd meeting, 3-4 March 2008, Rome (Italy), http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf, претражено 12. 09. 2015. године

правна лица која се служе рачунарима и базама података или зависе од њихове употребе.[205] Рачунар може да се јави као:

- објекат извршења кривичног дела – радња извршења кривичног дела подразумева уништење рачунара, података или програма који се налазе у рачунару или рачунарском систему, као и уништење пратеће рачунарске опреме или извора струје и напајања помоћу којих они функционишу;

- субјекат извршења кривичног дела – рачунар може бити место или окружење и коме ће се извршити кривично дело, као када се нпр. било каква врста преваре која се изврши променом података који се налазе у рачунару или рачунарском систему;

- средство извршења кривичног дела – неке врсте кривичних дела или начини извршења кривичних дела су веома комплексни и захтевају активну или пасивну употребу рачунара као средство извршења, као што је активно скенирање телефонских кодова како би се неовлашћено продрло у систем телефоније или пасивна симулација књиговодствене главне књиге како би се до краја реализовало кривично дело проневере;

- „оружје“ или средство којим се неко застрашује или обмањује – лажно представљање непостојећих организација, које преко интернета продају своје услуге које су фиктивне и на тај начин се врше интернет преваре.

Као што нема потпуне сагласности у дефнисању компјутерског криминалитета, тако нема ни сагласности у називу ове врсте криминалитета. У употреби су различити термини и називи: компјутерски криминалитет, криминалитет везан за компјутере, интернет криминал, мрежни криминал, дигитални и електронски криминал, рачунарски, информациони, високотехнолошки, сајбер криминалитет-cybercrime,[206] e-crime, hi-tech,

---

[205] *Ibid.*

[206] Термин „сајбер простор“ први је употребио Вилијам Џибсон (William Gibson) у научнофантастичној новели Neuromanser 1984. – цит. према: Радновић, Бранислав, Илић, Милена, Радовић, Немања: „Економски сајбер криминал у Србији – аспект заштите интернет потошача”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., с. 129., http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године. Термин *Cyber space* је требало да прикаже нематеријални простор незамисливе комплексности у коме рачунарски подаци путују као делићи светлости. Данас се под сајбер простором подразумева врста „заједнице“ сачињене од мреже компјутера у којој се елементи традиционалног друштва налазе у облику бајтова и битова, или простор који креирају компјјутерске мреже, односно глобална информациона инфрестуктура кроз коју се

electronic crime, криминалитет, ИТ криминалитет. У раду ће бити коришћена два термина компјутерски и високотехнолошки криминалитет с обзиром да су ови термини најчешће користе у међународним и националним документима посвећеним овом облику криминалног понашања и да је у нашем законодавству у употреби термин „високотехнолошки криминал“. У криминолошкој литератури се користи термин компјутерски криминалитет[207] како би се истакла повезаност криминалитета са употребом компјутера, компјутерских система и мрежа, али и других система (интернета, друштвених мрежа) који се користе уз помоћ компјутера. Компјутерски криминалитет се у правној литератури такође сликовито назива и „криминал сивих шешира“.[208]

Постоји велики број различитих дефиниција компјутерског криминалитета, али је у готово свим дефиницијама наглашена посебност и специфичност кривичних дела која припадају компјутерском криминалитету, као и поседовање знања или употреба одређених вештина из области компјутерских технологија.[209]

Према једној дефиницији, компјутерски криминалитет представља такав облик криминалног понашања код кога се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривично-правном смислу релевантна последица. Компјутерски криминалитет представља такође противправну повреду имовине код које се рачунарски подаци с предумишљајем мењају - манипулација рачунара, разарају - рачунарска саботажа, или се користе заједно са хардвером - крађа времена.[210]

врши масовна комуникација и у којој истовремено постоје виртуелно и реално. Цит. према Жунић Павловић, Весна, Ковачевић Лепојевић, Марина: „Интерперсонално насиље у „cyber“ простору”, Истраживања у специјалној педагогији, факултет за специјалну едукацију и рехабилитацију, Београд, 2009, стр. 227.

[207] Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна, Костић, Миомира: “Криминологија”, 5. измењено и допуњено издање, Ниш: Правни факултет, Центар за публикације, 2012, стр. 178.

[208] *Наведено код*: Спасић, Видоје: „Актуелна питања у области сајбер криминала“, Билтен судске праксе Врховног суда Србије, Београд: Intermex, 2006. - бр. 1 (2006), стр. 107

[209] Schjolberg, Stein: „The History of Global Harmonization on Cybercrime legislation - The Road to Geneva“, децембар 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, претражено 20. 11. 2013. године

[210] APIS Security consalting, Компјутерски криминалитет, http://www.apisgroup.org/sec.html?ид=29, претражено 20. 11. 2013. године и Николић, Слађан: „Случај економског бироа КОНЕКО-аларм за узбуну”, APIS Security Consulting, http://www.apisgroup.org/sec.html?id=26, претражено 08. 06. 2012. године.

Према мишљењу неких аутора, компјутерски криминалитет је немогуће дефинисати јединственим појмом због велике феноменолошке разноврсности и због тога је прихватљивије одредити компјутерски криминалитет као општу форму испољавања различитих облика криминалне делатности,[211] то је криминалитет који је управљен против безбедности информационих (компјутерских, рачунарских) система у целини или у њеном појединим делу, на различите начине и различитим средствима у намери да се себи или другом прибави каква корист или да се другоме нанесе каква штета.[212] Овај вид криминалне активности обухвата кривична дела код којих се компјутер појављује као средство (оруђе), предмет или објекат напада за чије је вршење или покушај неопходно извесно знање из рачунарства или информатике.[213]

Поједини аутори[214] сматрају да приликом дефинисања појма компјутерског криминалитета треба поћи од дефинисања објекта заштите: заједнички заштитни објекат кривичних дела која могу да се карактеришу као компјутерски криминалитет је безбедност рачунарских података, при чему се под појмом рачунарских података подразумевају подаци који се уносе или користе ради несметаног рада рачунара, подаци који се уносе ради електронске обраде или који се преносе рачунарским мрежама.

Хронолошки посматрано, прво је у Сједињеним Америчким Државама 1979. године Национални правни институт САД донео Практикум о компјутерском криминалитету,[215] у коме је дефинисан компјутерски криминалитет, да би касније и међународне организације, које су се бавиле овим питањем, одредиле шта се подразумева под појмом компјутерски криминалитет.

---

[211] Parker, Don: "Fighting computer crime", New York, 1983.

[212] Јовашевић, Драган, Хашимбеговић, Тарик: "Кривичноправна заштита безбедности рачунарских података", http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-08.pdf, претражено 12. 03. 2014. године

[213] Бого Брвар: „Појавне облике злорабе рачулника", наведено код Јовашевић, Драган, Хашимбеговић, Тарик: „Кривичноправна заштита безбедности рачунарских података", http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-08.pdf, претражено 12. 03. 2014. године

[214] Тањевић, Наташа: „Компјутерски криминал − правна заштита на националном нивоу", Безбедност - Часопис Министарства унутрашњих послова Републике Србије, број 1-2/2009, стр. 154.

[215] The Computer Crime: Criminal Justice Resource Manual, US Department of Justice/ National Institute of Justice/Office of Justice Programs, уредник Donn B. Parker, 1979 - друго издање из 1989. године доступно на https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf, претражено 29. 11. 2014. године

У Практикуму о компјутерском криминалитету, компјутерски криминалитет дефинисан је у најширем смислу као сваки злочин који се деси у оквиру неког компјутерског система, али и као врста криминалитета белог оковратника извршеног у оквиру неког компјутерског система, при чему се компјутер користи као средство извршења овог пословног кривичног дела.[216] Према тексту Практикума, ова врста кривичних дела може у себи да садржи и висок степен агресије и насиља, који су усмерени на уништење компјутера, компјутерског система или њиховог садржаја, и да на тај начин угрозе људске животе (нпр. ако је реч о нападу компјутерских система по болницама, где се прате животне функције пацијената). [217]

Поједини међународни документи из области високотехнолошког криминалитета, који предвиђају кривична дела и механизме којим се ова дела могу спречити, такође дефинишу појам компјутерског криминалитета.

Препорука Организације за економску сарадњу и развој из 1986. године компјутерски криминалитет дефинише као свако противправно, неетичко и недозвољено понашање које се односи на аутоматску обраду и пренос података.[218]

У Препоруци Савета Европе из 1989. године под компјутерским криминалитетом се подразумева тачно одређен број кривичних дела која су овом Препоруком предложена на усвајање националним законодавствима,[219] док Препорука из 1995. године дефинише кривична дела повезана са информационим технологијама као кривична дела код којих истражни органи приликом вршења истражних радњи морају да поседују информација које се

[216] *Ibid.*
[217] *Ibid.*
[218] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986), наведено код Schjolberg, Stein, Hubbard, M. Amanda: „Harmonizing National Legal Approaches on Cybercrime“, стр. 3, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity , Document: CYB/04, 2005., http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf, претражено 29. 11. 2014. године
[219] Препорука Савета Европе о криминалитету везаном за рачунаре бр. 9 (Council of Europe Computer-related crime Recommendation No. R (89) 9), 1989, http://www.oas.org/juridico/english/89-9&final%20Report.pdf, претражено 07. 11. 2014. године и 29. 11. 2014. године

обрађују или преносе компјутерским системима или електронским системима за обраду података.[220]

На Десетом конгресу Уједињених нација за превенцију криминалитета и третман делинквената у Бечу 2000. године,[221] дефинисан је компјутерски криминалитет (*cybercrime*) као општи појам који обухвата кривична дела која се врше посредством компјутерског система или мреже, у компјутерском систему или мрежи или против компјутерског система или мреже, а обухвата било који криминалитет извршен електронским путем или извршен у делу или у целости у електронском окружењу. У пленарном делу посвећеном компјутерском криминалитету, констатовано је да је могуће препознати две врсте компјутерског криминалитета:[222]

(1) компјутерски криминалитет у ужем смислу, који подразумева свако незаконито понашање усмерено на електронске операције сигурности компјутерских система и података који се у њима обрађују (где спадају дела која се односе на неауторизовани приступ компјутерском систему или мрежи кршењем мера сигурности; оштећење компјутерских података или програма; компјутерске саботаже; неовлашћено пресретање комуникација од и у компјутерским системима и мрежама; компјутерска шпијунажа) ,

(2) компјутерски криминалитет у ширем смислу, који подразумева свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и такав криминалитет какво је незаконито поседовање, нуђење и дистрибуирање информација преко компјутерских система и мрежа (попут компјутерских фалсификата; компјутерске крађе; техничке манипулације уређајима или електронским компонентама уређаја; злоупотребе система

---

[220] Препорука Савета Европе бр. 95 о заштити појединаца у поступку обраде личних података и њиховог слободног преношења - Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, усвојена 11. 09. 1995. године, http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp, претражено 07. 11. 2014. и 29. 11. 2014. године

[221] United Nations Office on Drugs and Crime, Tenth UN Congress on the Prevention of Crime and Treatment of Offenders ”Crime and Justice: Meeting the Challenges of the Twenty-first Century”, http://www.uncjin.org/Documents/congr10/4r3e.pdf, претражено 12. 12. 2014. године и http://www.unodc.org/congress/en/previous/previous-10.html, претражено 12. 08. 2015. године

[222] *Наведено код* Никић, Срђан: “Најчешће методе напада cyber криминалаца и како се одбранити”, http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf, претражено 25. 10. 2014. године

плаћања као што су манипулације и крађе електронских кредитних картица или коришћење лажних шифри у незаконитим финансијским активностима).

У складу са Препоруком Савета Европе[223] из 1989. године и листом OECD[224] из 1985. године приликом дефинисања компјутерског криминалитета наводе се и други појавни облици његовог испољавања: неауторизовани приступ компјутерском систему или мрежи кршењем мера сигурности (хакеровање), оштећење компјутерских података или програма, компјутерске саботаже, неовлашћено пресретање комуникација од и у компјутерским системима и мрежама и компјутерска шпијунажа.

Конвенција Савета Европе о високотехнолошком криминалу бр. 185 из 2001. године[225] класификује компјутерски криминалит у четири групе зависно од учињених кривичних дела на: кривична дела против поверљивости, интегритета и доступности компјутерских података и система, кривична дела везана за компјутере, кривична дела везана за садржаје и кривична дела дела везана за кршење ауторских и сродних права.

За компјутерски криминалитет специфична је чињеница да је потребно релативно кратко време за стицање знања неопходног за извршавање кривичних дела из ове области, као и да су потребни су мали материјални и људски ресурси у односу на штету или противправну добит која се може остварити и без физичког присуства на месту извршења дела.

Облици испољавања компјутерског криминалитета су различити. Једна од основних криминолошких подела је подела на (1) традиционални компјутерски криминалитет и (2) савремене облике компјутерског криминалитета који су се развили због злоупотреба компјутера и компјутерских мрежа.[226] Традиционални компјутерски криминалитет најчешће обухвата кривична дела која су уз помоћ рачунара извршена против имовине (нпр. кривична дела крађе, проневере, утаје, уцене и сл.), док савремени облици компјутерског криминалитета обухватају само она кривична дела која могу да

[223] Препорука Савета Европе бр. (95) 13 (Council of Europe Recommendation No. R (95) 13), *op.cit.*
[224] The United States Department of Justice, http://www.justice.gov/criminal/cybercrime/intl.html, претражено 16. 04. 2014. године
[225] Конвенција Савета Европе о високотехнолошком криминалу бр. 185 (Convention on Cybercrime CETS No. 185), 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, и http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG претражено 07. 11. 2014. године.
[226] Тањевић, Наташа, *op.cit.,* 2009, стр. 157

изврше употребом рачунара и злоупотребом рачунарских мрежа без обзира на то да ли је мотив за њихово извршење стицање материјалне користи (нпр. интернет прогањање, сајбер тероризам и сл.).[227]

Појавни облици компјутерског криминалитета могу такође да буду: противправно коришћење услуга и неовлашћено прибављање информација, компјутерске крађе, компјутерске преваре, компјутерске саботаже, компјутерски тероризам, криминалитет везан за компјутерске мреже и сл.

Зависно од типа извршених кривичних дела, компјутерски криминалитет може бити:

а) политички (компјутерска шпијунажа, хакинг, компјутерска саботажа, компјутерски тероризам, компјутерско ратовање),

б) економски (компјутерске преваре, хакинг, крађа интернет услуга и времена, пиратерија софтвера, микрочипова и база података, компјутерска индустријска шпијунажа, преварене интернет аукције - неиспоручивање производа, лажна презентација производа, лажна процена, надограђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта, вишеструке личности),

ц) производња и дистрибуција недозвољених и штетних садржаја (дечија порнографија, педофилија, верске секте, ширење расистичких, нацистичких и сличних идеја и ставова, злоупотреба жена и деце),

д) манипулација забрањеним производима, супстанцама и робама (дрогом, људским органима, оружјем),

е) повреде приватности на интернету (надгледање електронске поште, спам, прислушкивање и снимање „причаоница", праћење конференцијских веза).

Немачки теоретичар Сибер (Sieber),[228] који се бави искључиво проблемима компјутерског криминалитета, сматра да се проблем компјутерског криминалитета појавио први пут када је угрожена приватност корисника интернета[229] и да се компјутерски криминалитет може класификовати на

[227] *Ibid.*
[228] Sieber, Ulrich: „Legal Aspects of Computer-related crime in the Information society- COMCRIME Study", The European Comission, 1998, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, претражено 04. 12. 2014. године
[229] *Ibid.*

криминалитет повреде приватности, на компјутерски економски криминалитет (компјутерски хакинг, компјутерски шпијунажу, софтверску пиратерију, изнуде вршене коришћењем компјутера, компјутерске преваре), криминалитет противзаконитог и штетног садржаја компјутерских података и остала слична дела извршена употребом рачунара.[230]

Злоупотреба компјутера је у време њиховог конструисања и постепеног усавршавања била практично немогућа у већој мери јер је њихово коришћење подразумевало специјалну едукацију коју је пролазио релативно узан круг информатичких стручњака јер компјутери у то време нису били у масовној употреби. Брз развој компјутерске технологије, стварање веома једноставних начина њихове употребе, као и производња и масовно коришћење персоналних компјутера, довели су до стварања веома повољних услова за коришћење рачунара у вршењу кривичних дела. Свакодневна употреба компјутера од стране широких слојева становништва, уз либералан приступ глобалним комуникацијским и информатичким мрежама, довели су до тога да компјутерски криминалитет из сфере футуризма постане опасан и известан вид криминалитета данашњице.

Криминалитет који се реализује помоћу компјутера може да има облик било ког од традиционалних видова криминалитета, као што су крађе, утаје, проневере, док се подаци који се неовлашћено прибављају злоупотребом информационих система могу на различите начине користити за стицање противправне користи. У односу на штету или противправну корист коју овај вид криминалитета може да нанесе друштву или до које може да доведе, материјални и људски ресурси који се улажу су минимални, време извршења је веома кратко што додатно отежава откривање и доказивање дела, а веома често извршилац се уопште физички не налази на месту извршења дела.

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

[230] *Ibid.*

таквим информацијама (компјутерска саботажа), компјутерски тероризам.[231] Актери наведених недозвољених активности користе услуге интернета и друштвених мрежа у свим фазама криминалне активности: за планирање, припремање, врбовање жртве, обезбеђење средстава, реализацију и прибављање користи, знајући да је могућност откривања њиховог идентитета минимална. Криминалне активности које се испољавају преко друштвених мрежа у суштини представљају прилагођене облике испољавања компјутерског криминалитета. Ефикасна превенција, откривање и покретање поступака против извршилаца кривичних дела додатно је отежана транснационалним карактером ове врсте криминалитета.

Интересантна је класификација понашања на интернету која се могу окарактерисати као девијантно понашање или дела компјутерског криминалитета коју даје Дебра Литлџон Шиндер (Debra Littlejohn Shinder) на: насилна и потенцијално насилна дела, деструктивна понашања и на ненасилна понашања на интернету. У *насилна и потенцијално насилна понашања* на интернету убрајају се интернет (сајбер) тероризам, увреда и претња преко интернета, интернет прогањање и дечија порнографија; у *деструктивна понашања* спадају дела приликом чијег извршења се уништравају или оштећују рачунарске мреже или подаци (хаковање, брисање података или програма, уношење вируса и штетних програма, сајбер вандализам и сл.), а у *ненасилна понашања на интернету* спадају неовлашћени упад у базе података, интернет крађа, интернет превара, интернет проституција, коцкање преко интернета и сл.[232]

2. Обележја извршилаца кривичних дела компјутерског криминалитета – „хакера”

Појавом Интернета као глобалне компјутерске комуникационе мреже и снажног утицаја који интернет има на развој модерног друштва, појавила се и

[231] Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна, Костић, Миомира, *op.cit.,* 2012.
[232] Littlejohn Shinder, Debra: “Scene of the Cybercrime: Computer Forensics Handbook”, 2002., стр. 19, http://www.dvara.net/hk/Syngress%20Scene%20of%20the%20CyberCrime.pdf, претражено 24. 10. 2015. године

нова врста извршилаца кривичног дела – „хакери“ - који за свој субјекат и објекат деловања имају интернет окружење, примењујући своје стечено знање које је по правилу знатно изнад знања којег имају органи откривања и гоњења.

Јединствени профил учиниоца кривичног дела компјутерског криминалитета не постоји, али се сви они означавају заједничким називом – хакер.

У периоду шездесетих и седамдесетих година XX века, под појмом хакер је подразумевана особа, компјутерска „мудрица”, која поседује знања о компјутерима, способности и жељу за истраживањем и унапређивањем компјутерских система. Значење овог појма било је позитивно јер су хакерски напади тада имали случајни и добронамерни карактер и настајали су као резултат личног усавршавања хакерских вештина у циљу истраживања, забаве или такмичења. Осамдесетих година прошлог века хакинг битно мења своју садржину, актере, циљеве и последице и постаје претња сваком компјутерском систему, појединцима, организацијама, као и државама. Најопштија дефиниција је да хакинг представља упадање у компјутерске системе тајно и без овлашћења.

Према субјекту, хакинг може да се дефинише и као активност хакера.[233] Учиниоци оваквог дела нису директно мотивисани ни остварењем користи ни проузроковањем штетних последица, већ једноставно траже задовољство у неовлашћеном „упаду” и узимању информација из неког добро обезбеђеног информационог система. Они користе своје рачунарско знање да би упадали у туђе добро чуване информатичке системе. Хакер је особа која детаљно испитује програмске системе и који тежи да максимално прошири своје знање у овом домену, као и особа која на илегални начин упада у компјутерске системе. [234]

Већина дефиниција хакинга своди се на две активности хакера: истраживање и неовлашћено коришћење компјутерског система и покушај неовлашћеног приступа компјутерском систему, док се хакер дефинише као особа која поседује знања, способности и жељу за потпуним истраживањем система. Дороти Денинг (Dorothy Denning) сматра да је хакер особа која

[233] Galley, Patrick: “Computer terrorism: what are the risks?”, Science, Technology and Society Swiss Federal Institute of Technology, 1996, http://www.home.ch/~spaw1165/infosec/sts_en/, претражено 14. 02. 2014. године
[234] *Ibid.*

провађује у компјутерске системе и бесплатно их користи [235] а Томас Норден (Thomas Nourten) под хакерима подразумева вандале који неовлашћено добијају приступ компјутерским системима и уништавају податке и програме који се налазе на њима. [236]

Једна од дефиниција хакинга је да хакинг представља „процес у коме нека особа спроводи нелегалан упад у компјутерски или комуникациони систем и тамо чита податке, оставља поруке, стартује програме, брише или исправља програме и информације".[237] Хакинг је такав приступ компјутерском или комуникационом систему за који не постоји дозвола његовог власника. Осим тога, хакинг се дефинише и као „неовлашћени упад у компјутерске или телекомуникационе системе и неовлашћено коришћење компјутерских или телекомуникационих ресурса (читање, копирање, измена, брисање, убацивање података и програма или електронско пресретање података у њиховој трансмисији) у циљу незаконите манипулације резултатима наведених активности (лична употреба, пренос употребе на друга лица, продаја, уцена, тероризам и слично)".[238] Управо ова последња дефиниција, по нашем мишљењу, најбоље описује криминалну радњу којом се крши право на приватност корисника интернета и друштвене мреже.

Поједини аутори, попут Фредерика Коена (Frederick B. Cohen) указивали су на неколико најчешћих мотивација услед којих долази до вршења оваквих кривичних дела.[239] Зарада новца се ретко појављује као мотив, много чешћи мотив је друштвено доказивање (поготово код млађих извршилаца) или освета према некоме рушењем његовог угледа у друштву, јавног компромитовања, манипулацијом истинитих података или уништавањем његових података.

---

[235] Denning, Dorothy, Drake, Frank:"A Dialog on Hacking and Security", edicija: Computers under attack: intruders, worms, and viruses, Association for Computing Machinery Publications, New York, 1990, стр. 421-439
[236] Nourten, Thomas:"Vandalism or Prank?", edicija: Computers under attack: intruders, worms, and viruses, Association for Computing Machinery Publications, New York, 1990, стр. 522-523
[237] Дракулић, Мирјана: „Основи Компјутерског права", Друштво операционих истраживача Југославије - ДОПИС, Београд, 1996.
[238] *Ibid.*
[239] *Ibid.*

Свакако најпознатија хакерска група на свету су Анонимуси (Anonimys). Јануара 2015. године изречена је казна новинару Берету Брауну, портпаролу Анонимуса, којом је Браун осуђен на затворску казну у трајању од 63 месеци и новчану казну у износу од 890.000 долара, колико ће морати да исплати компанији Стратфор, коју су Анонимуси хаковали а Браун је објављивао линкове за фајлове које су хакери украли од Стратфора. Као посебну меру суд је изрекао меру надзора електронских комуникација које Браун води, чак и када он буде изашао на слободу. Брауна је ФБИ ухапсио 2012. године, суђење му је трајало укупно 31 месец, колико је он већ и провео у затвору. У почетку је оптужница против њега била знатно дужа и обухватала је и кривична дела крађе идентитета и поседовање бројева украдених кредитних картица. Оптужница је касније ревидирана, а Браун је априла 2014. године споразумно признао кривицу по три тачке оптужнице, за кривично дело преношења претње у међудржавној трговини, ометање извршења претреса и саучесништво после неовлашћеног приступа заштићеном рачунару. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Novinar-portparol-Anonimusa-osudjen-na-pet-godina-zatvora.html, претражено 26. 01. 2015. године)

Новембра 2013. године непознати хакер је извршио упад на информациони систем Агенције за промоцију извоза и страних улагања Владе Србије (СИЕПА), одакле је проследио око 300 мејлова који пружају увид у рад једне државне агенције, садрже назнаке постојања корупције и несавесног поступања у руковођењу овом агенцијом као и наводне проневере, корупцију, непотизам и расипање новца грађана Србије. Након детаљног испитивања садржаја прослеђене електронске поште, тадашњи директор ове Агенције је поднео оставку, Агенција за борбу против корупције је потврдила да „из садржине дописа примљених електронском поштом, произлази сумња да су извршена кривична дела за која се гони по службеној дужности" и да су примљени материјал проследили Апелационом јавном тужилаштву у Београду на даљу надлежност и поступање. Предмет испитивања посебно су биле околности које се односе на несавесно поступање СИЕПА у вези са ненаплативим банкарским гаранцијама у вредности од преко два милиона евра, јавне набавке, организација и опремање промотивних сајмова у иностранству као и одлуке о додели бесповратних средстава фаворизованим инвеститорима. (Балканист, http://balkanist.net/bcs/siepa-leaks/, претражено 19. 12. 2013. године)

Марта 2012. године, полиција је у Панчеву ухапсила хакера Г. В. (19), који је био познат по коришћењу псеудонима „John the Ripper" и „SunTzu" за кога је постојала основана сумња да је за неовлашћено приступање серверима државних органа и служби примао новац. У оптужбеном предлогу наведено је да је Г. В. одговоран за 28 хакерских акција које су у оптужном предлогу квалификоване као кривична дела рачунарска саботажа, прављење и уношење компјутерских вируса, неовлашћени приступ заштићеном рачунару и прављење и давање средстава за извршење кривичних дела против безбедности рачунарских података. Месец дана касније, априла 2012. године, припадници Службе за борбу против организованог криминала ухапсили су Б.С. (28), који се сумњичи да је са свог рачунара изменио приступне и сигурносне параметре на Фејсбук профилу једног јавног предузећа и преко електронске поште претио директору предузећа да му неће вратити приступне шифре и да ће профил остати под његовом контролом, уколико му не исплати 2.000 евра.

(Вечерње новости – дневна новина од 11. 04. 2012. године, http://www.novosti.rs/vesti/naslovna/aktuelno.291.html:375140-Tuzilastvo-Haker-primao-novac-za-obaranje-sajtova, претражено 06. 08. 2012. године)

Новембра 2014. године суд у Данској је осудио једног од оснивача сајта Pirate Bay Готфрида Варга на три и по године затвора због хаковања. Варг је проглашен кривим због хаковања ИТ компаније CSC у Данској чиме је извршио кривично дело неовлашћеног приступа стотинама хиљада бројева социјалног осигурања, полицијских досијеа и судских докумената. Казна коју је одредио суд је мања од оне коју је тражило тужилаштво које је захтевало да Варг буде осуђен на пет година затвора, што је такође мање од максималне прописане казне за хаковање која у Данској износи шест година. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Zbog-hakovanja-suosnivac-Pirate-Bay-osudjen-na-3-5-godine-zatvora.html, претражено 26. 01. 2015. године)

Познат је и случај деветнаестогодишњег канађанина Стивена Артура Солис-Рејеса, који је априла 2014. године оптужен је да је хаковао сајт канадске пореске агенције и да је том приликом украо 900 бројева социјалног осигурања тако што је у систем унео злонамерни програм назван Heartbleed bugg. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Prvo-hapsenje-zbog-Heartbleed-baga.html, претражено 26. 01. 2015. године)

Казна од 11 година затвора на коју је октобра 2014. године осуђен естонац Сергеј Николајевич Тшуриков (25), вођа хакерске групе која је 2008. године за 12 сати украла 9,4 милиона долара са банкомата, једна је од најстрожијих казни која је изречена неком хакеру у САД. Тшуриков је изручен властима САД због тога што су он и седам његових помагача упали у мрежу RBS WorldPay, амерички огранак Royal Bank of Scotland са седиштем у Атланти и компромитовали енкрипцију система за обраду картица. Када су успели да пробију енкрипцију система за обраду картица, хакерска група је подигла лимите компромитованих налога а затим су помоћу фалсификованих дебитних картица подигли 9,4 милиона долара са више од 2.100 банкомата у најмање 280 градова широм света, укључујући и градове у САД, Русији, Украјини, Естонији, Италији, Хонг Конгу, Јапану и Канади. Осим Тшурикова, оптужени су и Виктор Плешчук (28) из Русије и Олег Ковелин из Молдавије, затим особа која је у оптужници означена као „Хакер 3", као и још четворица помагача из Естоније. Виктор Плешчук је као један од вођа ове криминалне групе осуђен на условну казну у трајању од 4 године, а казна му је ублажена пошто је признао кривицу и пристао да тужилаштву пружи информације о осталима који су учествовали у нападу. Поред условне казне досуђена му је и обавеза да врати 8,9 милиона долара компанији RBS WorldPay. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Vodja-grupe-koja-je-za-12-sati-ukrala-9-miliona-dolara-sa-bankomata-osudjen-na-11-godina-zatvora.html, претражено 26. 01. 2015. године)

Априла 2011. године у Београду интернет презентација некадашњег окружног тужилаштва за борбу против високотехнолошког криминала сатима је била полигон за вежбање будућих хакера, до којих су многи били малолетни. Сајту се приступало уз помоћ основног корисничког имена и шифре. Непозната особа приметила је да се администраторском делу сајта приступа школским примером корисничког имена и шифре, па је ту информацију пренела другим људима. Друштвеном мрежом Фејсбук информација о незаштићеном сајту проширила се великом брзином, па су одмах осванула бројне приватне поруке и више фотографија са порнографским садржајем, а интернет презентација који промовише борбу против високотехнолошког криминала послужила је и за приватне разговоре посетилаца. Особа која је информацију објавила била је потписана преудонимом Џон Трбосек (John the Ripper). (Блам тужилаштва за сајбер криминал, http://www.samo-opusteno.info/forum/tehnologija/blam-tuzilastva-za-sajber-kriminal/, претражено 06. 08. 2012. године)

3. Злоупотреба друштвених мрежа као девијантно понашање

3.1. Појам злоупотребе друштвених мрежа и облици испољавања

Глобалне друштвене мреже допринеле су даљем развијању компјутерског криминалитета, у оквиру кога се компјутерске мреже користе као циљ напада (нападају се сервиси, функције, садржаји који се налазе на мрежи), средство или алат (on line продаја сексуалних услуга, људских органа, жена и деце за проституцију, 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).[240] Највећи број друшвено неприхватљивих и недозвољених понашања у оквиру компјутерског криминалитета и нелегалног коришћења друштвених мрежа је предвиђен у закону као кривично дело.

Међутим, постоје такви облици злоупотребе друштвених мрежа који нису инкриминисани, али су свакако друштвено неприхватљиви и девијантни. Уколико се прихвати шире криминолошко социолошко дефинисање криминалитета, ова понашања се могу сматрати криминалним. У том смислу и за потребе овог рада, *злоупотреба друштвених мрежа се може дефинисати као девијантно понашање које се састоји у нелегалном коришћењу друштвених мрежа противно правилима о заштити приватности, протоколима о електронској комуникацији, препорукама и утврђеним правилима која постоје на друштвеним мрежама,*[241] *чиме се друштву и појединцима корисницима друштвених мрежа, али и онима који то нису, наноси материјална и нематеријална штета.*

---

[240] *Ibid.*

[241] У оквиру виртуелних заједница установљена су одређена правила која је потребно поштовати и која подразумевају забрану вулгарног изражавања, расну, верску, полну и друге врсте дискриминације, вређање осталих учесника виртуелног простора, „преплављивање“ екрана порукама и сл. За поштовање ових правила старају се две врсте контролора: супервизори, који су запослени у систему и „полицајци“, волонтери из редова корисника. Осим ових системских правила, постоје и неписана правила која успостављају сами корисници и која се међусобно разликују . *Видети више код:* Симовић, Владимир: „Социјални и правни контекст рачунарства”, Висока школа струковних студија за информационе технологије, Београд, 2010, стр. 57.

Због отвореног приступа личним подацима корисника, често долази до велике злоупотребе коришћењем ових 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, као и идентификационе информације које се односе на посетиоца одређене интернет странице. Према мишљењу Стива Рамбама, приватног детектива за област заштите интернет приватности, велики број експерата из области компјутерске безбедности и приватности верује да приватност не постоји: „Приватност је мртва – преболите то“. [242]

Интересантан пример могуће злоупотребе друштвене мреже за извршење неког другог кривичног дела представља објављивање података 2010. године на интернет порталу www.PleaseRobMe.com, где је приказан преглед свих профила корисника друштвене мреже Twitter који су отишли на одмор, на викенд или на посао и оставили свој дом празан. Циљ оснивача овог сајта био је да покаже корисницима сајтова за друштвено умрежавање како њихов дом може лако бити опљачкан због информација које пласирају преко друштвене мреже, да упозоре људе на последице које могу да имају информације које остављају на Интернету, а не да ти корисници буду опљачкани.[243] Пошто су све информације најчешће јавне и садрже кућну адресу корисника друштвене мреже, заинтересована лица лако могу да одреде које су куће и станови празни. Оснивачи сајта наводе да је за прикупљање података о корисницима било довољно обавити проверу њиховог статуса који су сами корисници навели,

[242] Стив Рамбам - Приватност је мртва – преболите то, Google video, http://www.documentary24.com/privacy-is-dead-get-over-it--317/, претражено 08. 08. 2012. године
[243] Please Rob Me, http://pleaserobme.com/, претражено 10. 09. 2012. године

додајући да су се служили и подацима са сајта www.Foursqure.com, који омогућава да се појединци прате у стопу на карти Google maps. Било је довољно унети име града и псеудоним одређене особе на Твитеру да би се добио приступ последњим порукама које је та особа оставила, што омогућава да се сазна где се она налази.

Најопаснији вид злоупотребе друштвених мрежа је интернет или дигитално насиље, које се може појавити у различитим облицима. Путем друштвених мрежа насилници могу приступити жртви у било које време и са било ког места, жртва може да постане стална мета виктимизације. Број особа које су укључене у насилне инциденте путем друштвених мрежа веома је тешко контролисати, а њихов идентитет је немогуће открити. Анонимност охрабрује насилнике и појачава несигурност код жртве. Жртве интернет насиља су најчешће младе особе активне на друштвеним мрежама. Интернет насиље (engl. Cyber bullying),[244] се дефинише као свака комуникацијска активност рачунарском технологијом која се састоји у претњи, узнемиравању, омаловажавању, застрашивању или другом начину угрожавања и наношења штете појединцу. [245]

Постоје различити облици ове врсте насиља: (1) слање узнемиравајућих порука путем мобилне мреже, e-maila или опције ћаскања (engl.Chat); (2) (крађа или неовлашћена промена лозинке (engl. Password) за e-mail или налога (engl. Account) на некој од друштвених мрежа (нпр. Facebook, My Space, Twitter и сл.); (3) крађа или неовлашћена промена „надимка" (енгл. Nick, Nickname) на опцији ћаскања; (4) објављивање приватних података или неистина о некоме, коришћењем опција ћаскања, на приватним интернет страницама или на блогу; (5) слање узнемиравајућих порука преко CMC, MMC или e-mail порука; (6) постављање увредљивих интернет анкета о некоме; (7) постављање слика жртава и писање увредљивих коментара; (8) слање вируса и штетних програма (engl. Malware) на интернет налог или страницу на друштвену мрежу, чиме се уништава тј. „хакује" нечији профил на друштвеној мрежи или уништавају подаци у рачунару услед деловања послатог вируса; (9) слање увредљивих,

[244] Cyberbullying Research Center, http://cyberbullying.us/cyberbullying_glossary.pdf, претражено 11. 03. 2014. године.
[245] Kids Health, http://kidshealth.org/parent/positive/talk/cyberbullying.html, претражено 10. 09. 2012. године.

порнографских или нежељених садржаја; (10) 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 и скривен иза свог „надимка", што је један од разлога зашто се овакви извршиоци кривичних дела осећају моћни.

Поједини аутори, као што су Delmonico и Griffin Elizabeth[246], као и Diamanduros, Downs и Jenkins [247] сматрају да се могу препознати поједини знаци који указују на постојање интернет насиља код млађе популације корисника Интернета: појава депресије или анксиозности уколико је онемогућен приступ интернету, промена понашања након добијања електронске поруке, одсуство из школе, повлачење и удаљавање од пријатеља и породице, жртвовање слободног времена и реалних активности како би се што више времена проводило пред компјутером у виртуелним комуникацијама, држање у тајности свих активности на интернету (нагло гашење компјутера када је неко у близини, брисање посећиваних страница и сл.).

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. С обзиром на масовност корисника и њихову хетерогеност у смислу припадности различитим националним, верским, регионалним, локалним, полним, образовним, сексуалним, мањинским групама, преко друштвених мрежа се све чешће испољавају различити облици електронског насиља кроз говор мржње (претње, понижавања, малтретирања, деградирања и сл.).

---

[246] Delmonico David, Griffin Elizabeth: „Cybersex and the e-teen: what marriage and family therapists should know", Journal of Marital Family Therapy, volume 34, number 4, 2008; стр. 431-444. http://www.researchgate.net/publication/23481408_Cybersex_and_the_E-teen_what_marriage_and_family_therapists_should_know, претражено 05. 11. 2014. године.

[247] Diamanduros Terry, Downs Elizabeth, Jenkins J. Stephen: "The role of school psychologists in the assessment, prevention, and intervention of cyberbullying", Psychology in School Publications., 2008; volume 45, number 8, стр. 693-704.

Поред крађе идентитета и разних облика превара које се испољавају на друштвеним мрежама, говора мржње, вршњачког насиља усмереног ка млађим корисницима друштвених мрежа, треба поменути још три облика испољавања компјутерског криминалитета преко друштвених мрежа, то су пиратерија, порнографија и педофилија и тероризам. Пиратерија је веома распрострањена на друштвеним мрежама пре свега због одређених апликацијских могућности и непостојања техничких ограничења у погледу дистрибуције пиратског садржаја. Иако је пиратерија изричито забрањена, друштвене мреже су веома погодне за дељење пиратизованог музичког, филмског, видео или сличног садржаја што значајно угрожава ауторска права. Друштвене мреже су такође веома погодне за брзо и масовно ширење порнографског материјала и педофилије јер се веома лако проналазе, идентификују и врбују жртве - корисници друштвених мрежа. Посебно је друштвено опасан сајбер тероризам, односно тероризам који се у потпуности или парцијално реализује на интернету или коришћењем могућности интернета. Друштвене мреже се користе за комуникацију међу терористима због заштићености комуникације, пропагирање терористичких ставова, проналажење истомишљеника и повезивање са њима.[248]

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

Поред наведених понашања која су већ дуги низ година проучавана, једно од новијих злоупотреба друштвених мрежа је употреба говора мржње на друштвеним мрежама и на интернету уопште. Како би се овакво деловање политичких, верских, националних и навијачких група на интернету свело на минимум, у Србији је фебруара 2014. године основан Национални комитет за

[248] Позната је улога Фејсбука и Твитера у догађајима познатим под називом „арапско пролеће“, због чега се револуције изазване у делу арапских држава називају Фејсбук односно Твитер револуцијама. *Видети детаљније:* Миладиновић, Александар, Петричевић, Витомир: „Криминогени аспект друштвених мрежа“, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30. 03. 2012. година, с. 266., http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

борбу против говора мржње на интернету[249] при Министарству омладине и спорта Републике Србије.

Постоје и аутори који појавне облике насиља и злоупотребе права на приватност у виртуелном свету класификују и у односу на пол,[250] па тако сматрају да виктимизација жена на друштвеним мрежама зависи од степена патријархалне идеологије у једном друштву, друштвених улога полова, утицаја медија, заштите права жена и сл. Насилници могу да буду и мушкарци и жене, а напади који се дешавају могу да буду сексуалне и несексуалне природе. Као неки од основних облика насиља и повреде приватности које жене могу да доживе на друштвеним мрежама наводе се: изражавање мржње, ширење лажи, прогањање, монтажа фотографија, стварање лажних корисничких профила, хаковање корисничког профила, злостављање, виртуелно силовање, забрана да јавно искаже своје мишљење, вршњачко насиље и називање погрдним именима, наставак породичног насиља, претње и уцене.[251]

3.1.1. Крађа и злоупотреба идентитета

а) Појам. Идентитет је скуп својстава везаних за појединца, који га карактеришу и по којим се тај појединац разликује од других особа.[252] Поред правних својстава (променљива својства: лично име и презиме, држављанство, брачни статус...), фактичких својстава (непроменљива својства: датум и место рођења, матични број...) и физичких својстава (пол, изглед...), постоје и виртуелна својства једне личности, попут лозинке, корисничког имена, пин кода и сл.[253]

Крађа идентитета се састоји у неовлашћеном коришћењу личних података (датум рођења, тренутно пребивалиште, број телефона, занимање,

---

[249] Блиц – дневна новина од 11. 02. 2014. године, www.blic.rs, дневна новина "Блиц" од 11. 02. 2014. године, претражено 11. 02. 2014. године

[250] Halder, Debarati, Jaishankar, Karuppannan: "Cyber Socializing and Victimization of Women", ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 5-26

[251] *Ibid.*, стр.12

[252] Милићевић, Слободанка, Вујовић, Срђан: "Проблем савремене доби: облици крађе и злоупотребе идентитета и мјере превенције", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., с. 303, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[253] *Ibid.*

пријатељи, личне слике) који су постали јавно доступни.[254] Она подразумева злоупотребу личних података који се налазе у виртуелном простору, најчешће ради стицања финанасијске добити. [255] Крађа идентитета на интернету представља облик преваре којом се од корисника рачунара путем лажне поруке електронске поште или веб-сајта сазнају лични и финансијски подаци. Приликом крађе идентитета неко лице се лажно представља као друго лице у намери прибављања противправне имовинске користи или друге личне користи.[256] Крађа идентитета почиње са присвајањем личних података о неком лицу, које се врши без знања и пристанка тог лица, путем обмањивања, крађе или преваре, а наставља се употребом прикупљених података за извршење кривичних дела која су у највећем броју случајева везана за стицање противправне имовинске користи лицима која злоупотребљавају украдени идентитет.[257]

Крађа идентитета представља преузимање „улоге" неког лица на Интернету, у циљу стицања неке материјалне или друге користи.[258] То је најдрастичнији атак на приватност личности, који претпоставља претходно извршење неког другог кривичног дела (преваре, упада у туђ рачунар или рачунарски систем, постављање вируса или другог штетног софтвера).[259]

Одређивањем појма крађе идентитета бавиле су се и најутицајније међународне организације, које су покушавале да их кроз своје стратешке документе дефинишу и регулишу. На 12. Конгресу УН у вези с превенцијом

---

[254] Gross, Ralph, Acquisti, Alessandro, *op.cit.,* 2005., стр. 80

[255] Roberts, Lynne: „Cyber-Victimisation in Australia:Extent, Impact on Individuals and Responses", http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan036070.pdf, претражено 01. 12. 2014. године

[256] Teri Bidwell: "Hack Proofing Your Identity in the Information Age", Syngress Publishing, Inc, 2002, стр. 3., *наведено код* Ивановић, Звонимир, Уљанов, Сергеј, Урошевић, Владимир: „Анализа феномена крађе идентитета", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на високотехнолошки криминал, Лакташи 28-30.03.2012., с. 149, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[257] Милошевић, Милан, Урошевић, Владимир: "Крађа идентитета злоупотребом информационих технологија", Безбедност у постмодерном амбијенту, Зборник радова књига VI, Центар за стратешка истраживања националне безбедности, Београд, 2009., стр. 53 - 64, наведено код Ивановић, Звонимир, Уљанов, Сергеј, Урошевић, Владимир, *op.cit.,* 2012, стр. 149

[258] Прља, Драган, Рељановић, Марио: "Високотехнолошки криминал – упоредна искуства", Страни правни живот бр. 3/09, Београд, стр. 169, http://www.comparativelaw.info/spz20093.pdf, претражено 15. 09. 2015. године

[259] *Ibid.*

криминала и кривичног правосуђа који је одржан 2010.године крађа идентитета је дефинисана као злоупотреба личних података другог лица са намером вршења преваре.[260] OECD (ОЕБС) предвиђа да крађа идентитета постоји када једно лице прибавља, пребацује, поседује или користи личне податке физичког или правног лица на недозвољен начин, у намери да изврши превару или почини неко друго кривично дело.[261] Како би преузели нечији идентитет и дошли до личних података о некој особи, извршиоци користе различите методе: слање и активирање злонамерних програма, слање електронских порука обмањујуће садржине, упућивање на лажне интернет сајтове који обмањују посетиоца како би оставио уписане своје личне податке и сл. Када се на један од оваквих начина дође до нечијих личних података, они могу бити злоупотребљени на различите начине од којих су најчешћи злоупотреба банковних рачуна, отварање лажних рачуна, бесправно коришћење одређених државних сервиса, служби и докумената, преваре у вези здравственог осигурања и сл.[262]

Савет Европе је 2007. године припремио платформу за израду јединствене, универзалне легислативе која се односи на крађу идентитета, а која је дефинисана као „крађа или преузимање постојећег идентитета (идентификационих обележја лица или значајног дела истих) са или без пристанка лица чија су и без обзира да ли је власник жив или је преминуо". Крађа идентитета се састоји их три манифестациона облика: начин извршења дела (*modus operandi),* мета напада и мотивација извршиоца дела. Као најчешћи *начини извршења дела* наводе се: физички метод (крађа делова рачунара, физичко противправно одузимање носилаца података), физичка крађа поште, коришћење интернет претраживача и система за дељење датотека, напади хакера као и напади методима социјалног инжењеринга. Најчешћа *мета напада* су подаци о идентификационим бројевима (нпр. јединствени матични број грађана, ЛБО број и сл), бројеви личних докумената (број личне карте, пасоша,

[260] 12. конгрес УН у вези с превенцијом криминала и кривичног правосуђа (12th UN Congress on Crime Prevention and Criminal Justice), 12 – 19. 04. 2010, стр. 6, https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf, претражено 12. 08. 2015. године
[261] OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, Ministerial background report: DSTI/CP (2007)3/FINAL, стр. 3, http://www.oecd.org/sti/40644196.pdf, претражено 10. 11. 2015. године
[262] *Ibid.*, стр. 4

кредитне или плоатне картице), корисничка имена и шифре на различитим интернет налозима. *Мотивација* за извршење дела је различита: она је начешће усмерена ка стицању материјалне добити, прикривање нечијег правог идентитета или као припремна радња за извршење неког другог кривичног дела.[263]

б) Законска регулатива крађе идентитета. Мали број земаља је донео кривичне законе којима се конкретно регулише и санкционише крађа идентитета као кривичног дела, док највећи број земаља понашања која представљају крађу идентитета третира и санкционише као дела незаконитог приступа подацима, преваре, фалсификовање, непоштовање ауторских права и сл. или као дело које претходи извршењу неког другог кривичног дела.

Као кривично дело *per se*, крађа идентитета је прописана Законом о крађи идентитета Сједињених Америчких Држава и подразумева подразумева сваки акт лица које свесно трансферује или неовлашћено користи било које име или број, који се може користити самостално или у спрези са неком другом информацијом, како би идентификовао одређену особу, у намери да изврши, помогне у извршењу или наведе на неку незакониту активност која представља кршење федералног закона, или представља кривично дело према неком закону државе чланице.[264] Канада је 2007. године крађу идентитета прописала и санкционисала као посебно кривично дело, јер до тада су слични случајеви били процесуирани и санкционисани као кривична дела лажног представљања и фалсификовања.[265]

Једина европска држава која је крађу идентитета предвидела као посебно кривично дело је Велика Британија, одређујући крађу идентитета као вид преваре која може да буде извршена на интернету и то на један од следећих начина: лажним представљањем, путем намерног пређуткивања и прикривања

[263] Cybercrime Convention Comitee – T-CY Guidance Note #4, Identity theft and phishing in relation to fraud, Council of Europe, 2013, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7096, претражено 20. 09. 2015. године

[264] Identity Theft Assumption and Deterrence Act - the Identity Theft Act; U.S. Public Law 105-318, https://www.ftc.gov/node/119459, претражено 12. 08. 2015. године

[265] Canadian Department of Justice, http://canada.justice.gc.ca/en/news/nr/2007/doc_32178.html, претражено 15. 08. 2015. године

чињеница или злоупотребом положаја.[266] Француска је 2005. године покушала да у свој кривичноправни систем уведе крађу идентитета као кривично дело, али је већ 2006. године овај предлог повучен из процедуре уз објашњење да је овакво понашање обухваћено инкриминисањем других кривичних дела.[267]

У важећем кривичном законодавству Србије није посебно предвиђено кривично дело крађе идентитета коришћењем интернета и друштвених мрежа. Највеће базе података о грађанима имају Министарство унутрашњих послова (евиденција о личним картама), Републички фонд за здравствено осигурање (подаци из здравствених картона, фактуре о издатим лековима и лекарским интеренцијама), Фонд пензијског и инвалоидског осигурања (евиденција пензионих осигураника), велике банке (поред исцрпне базе података о својим клијентима, имају и посебно осетљиве здравствене податке које прикупљају приликом одлучивања о кредитним захтевима) и велика је опасност за злоупотребу ових података и повреду приватности уколико се они открију. Највећи ризик за крађу идентитета постоји уколико се сазна јединствен матични број грађана, јер на основу њега може да се „уђе“ у базу података. Процењује се да у Србији постоји велики број људи којима на адресу стижу рачуни за разна дуговања или пријаве за утају пореза у вези са пословањем предузећа чији су „власници“ иако за њих први пут чују. На туђе име се отварају фирме, подижу кредити, купује роба и сл. Уколико дође до крађе идентитета, примењују се одредбе Кривичног законика које се односе на рачунарску превару (чл. 301), превару (чл. 208), фалсификовање и злоупотребу платних картица (чл. 255 ст. 4), неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга (чл. 233).

в) Појавни облици. Извршиоци крађе идентитета постижу свој циљ најчешће коришћењем друштвених мрежа како би са туђег рачунара прикупили лозинке, корисничка имена и бројеве кредитних картица које корисник користи на рачунару. Сваки рачунар прикупља информације о кориснику рачунара које он у току коришћења различитих програма и услуга уноси и складишти их у

[266] Видети: The UK Fraud Act 2006, http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf, претражено 12. 08. 2015. године и Out-Law news: „Phishing kits banned by new Fraud Act“, http://www.out-law.com/page-7469, претражено 12. 08. 2015. године

[267] OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, *op.cit.* ,2007, стр. 16.

датотекама скривеним на хард диску. Фајлови, који се на рачунару налазе сакривени, као што су „кеш“ (енгл. Cache), „историја претраживача“ (енгл. History) и други „привремени интернет фајлови“ (енгл. Temporary internet files) се могу користити како би се реконструисале интернет навике корисника. Управо ове датотеке складиште информације попут корисничких имена и лозинки, имена, адресе, бројеве кредитних картица.

Неки од начина на који је могуће извршити крађу идентитета су: **хаковање** (енгл. Hacking), **фишинг** (енг. Phishing), **фарминг** (енгл. Pharming), **спуфинг** (неауторизован приступ некој интернет локацији како би се дошло до других важних података, енгл. Spoofing), **скиминг** (превара платним или кредитним картицама у смислу меморисања информација са магнетних трака платних и кредитних картица који се затим рекодирају ради прављења фалсификоване картице, енгл. Skimming), **скам** (врсте превара и трикова који се шаљу путем електронске поште, најчешће у виду лажних лутрија, фишинг порука, нигеријских превара и сл. (енгл. Scam)), преусмеравање слања података, лажни формулари који се попуњавају на интернету, лажна логовања у која се уносе поверљиве шифре за улазак на различите профиле.[268] Ипак, најчешћи облик крађе идентитета и поверљивих информација путем електронске поште – тзв. фишинг.

Крађа идентитета путем електронске поште **(фишинг, енг. phishing)** састоји се у слању е-маил поруке кориснику у којој се наводи да поруку шаље легитимно правно лице или овлашћена особа тражећи личне податке и приватне информације. Наводи у поруци су лажни, а уколико прималац напише податке који се траже, они ће касније бити искоришћени за крађу идентитета. На тај начин се прибављају заштићене информације од корисника (корисничко име, лозинка, број кредитне картице), да би дошло до „преузимања“ идентитета корисника у неком облику електронске комуникације. Е-пошта усмерава корисника да посети веб сајт где се тражи да се лични подаци (лозинке и кредитне картице, социјално осигурање, бројеви банковних рачуна) које легитимна организација већ има, ажурирају. Веб сајт је, међутим, лажан и

[268] Paget, Francois: „Identity theft”, McAfee Avert Labs technical white paper No 1.’, 2007, http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf, претражено 01. 12. 2014. године

подешен само за крађу информација корисника.[269] Различити су начини на који се може извршити оваква злоупотреба,[270] а шема социјалног инжењеринга[271] се састоји из три фазе извршења: у *првој фази*, извршилац потенцијалној жртви шаље електронску поруку за коју се чини да је послата у име банке коју жртва користи или у име неке друге организације која би жртви могла да буде блиска а која може да захтева одређене личне податке; *друга фаза* почиње када жртва прочита електронску поруку, одговори на њу или буде прослеђен на одговарајући лажни интернет сајт пошиљаоца поруке остављајући своје личне податке и *трећа фаза* која подразумева прослеђивање података о жртви директно извршиоцу, који добијене податке користи како би извршио још неко противправно дело, а најчешће кривично дело преваре.[272]

„Фишинг технике“ могу да буду: крађа идентитета путем злонамерног софтвера (тзв. фарминг) и циљани „фишинг“.[273]

Крађа идентитета путем злонамерног софтвера **(фарминг, енгл. pharming)** представља посебан облик „фишинга“ приликом чијег извршења хакер покушава да преусмери електронску комуникацију и размену података са легитимне веб странице на потпуно другачију интернет адресу. Овај начин злоупотребе се најчешће врши променом фајлова на компјутеру корисника - жртве или искоришћавањем недостатака на серверу који се користи. Ради се о софистицираније врсти „фишинга“ јер у овом случају корисник ни не треба да

---

[269] All About Phishing, http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp, претражено 07. 09. 2012. године

[270] Електронска порука обично садржи неке од наведених елемената: поље „from“ изгледа као да је од легитимне компаније поменуте у е-поруци. Е-порука уобичајено садржи лого и слике које су узете са сајта компаније која је поменута у лажној е-поруци. Е-порука уобичајено садржи линк преко кога је неопходно унети личне податке власника е-маила. Обично ће у е-поруци бити наведена последица неактивирања линка из поруке, на пример “Ваш налог ће бити суспендован или затворен”. Оваква електронска пошта може да садржи и лого који није исти као лого компаније, грешке у спеловању, појављивање знака „%“ праћеног бројевима или „@“ знацима унутар хиперлинка, насумична имена или е-мејл адресе у телу текста или заглављу е-поруке. *Ibid.*

[271] Социјални инжењеринг представља методу довођења жртве у ситуацију да одаје одређене поверљиве податке особама које нису овлашћене да их знају, то је оригинално смишљен “фишинг” напад уз примену обмањујућих или лажних и прикривених електронских писама и “хакованих” веб сајтова компанија и банака који је осмишљен у циљу да особа којој је порука упућена ода одређене идентификационе информације и своје личне податке. *Видети*: Прља, Драган, Ивановић, Звонимир, Рељановић, Марио, op.cit., 2011, стр. 116

[272] OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, op.cit., 2007, стр. 17

[273] OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, op.cit., 2007, стр. 16

одговара на мејл да би тзв.“фармери“ могли да дођу до његових података. Само отварањем овакве електронске поруке у рачунар се учитава вирус или „тројанац“ (енгл. Malware) и „ки генератор“ (енгл. Key generator), који краде информације корисника - лозинке, корисничка имена и бројеве кредитних картица које користе на рачунару.[274] Након добијања података, могуће је креирати лажне идентификације, фалсификовати документа, чекове или кредитне картице.

Циљани „фишинг” **(„фишинг копљем”, усмерени фишинг, енгл. Spear fishing)** се за разлику од „уобичајеног” фишинга не врши слањем масовних електронских порука већ се жртве добро изаберу у складу са неким склоностима или навикама, па је самим тим и много прецизнији. Ова врста „фишинга” је усмерена на тачно одређене групе интернет корисника или чак на конкретне појединце.

Августа 2011. године у Бијелом Пољу дванаестогодишњу девојчицу је силовао М. К. (20). Девојчицу је контактирао, упознао и намамио преко Фејсбука, при чему се лажно представио као петнаестогодишњак, успео да договори сусрет у близини девојчицине куће, сачекао је, запретио пиштољем и силовао. (Вијести online, http://www.vijesti.me/vijesti/u-bijelom-polju-silovana-djevojcica-napasnik-je-namamio-preko-fejsbuka-clanak-34026/, претражено 10. 08. 2012. године)

У Нишу августа 2012. године Р.С. је убио другу супругу и своју ћерку из првог брака, а затим извршио самоубиство. Супругу је упознао лажно се представљајући као радник у БИА преко друштвене мреже Фејсбук јој је понудио брак, а њеног оца је убедио да му да свој пиштољ којим је извршио убиства под изговором да ће да га ослободи плаћања пореза. (Портал Нишке вести, http://www.niskevesti.info/hronika/vesti/krvni-delikti/578-preko-qfejsbukaq-do-velike-tragedije , претражено дана 16.08.2012. године и Блиц – дневна новина од 23.08.2012.године,http://www.blic.rs/Vesti/Hronika/338974/Ubica-iz-Nisa-spremao-i-trece-vencanje, претражено 23. 08. 2012. године)

[274]How to Defend Yourself Against Identity Theft, http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp, претражено 17. 09. 2012. године

Британац Јан Вуд успео је да од својих комшија из истог стамбеног блока у коме је живео украде у периоду од 2010. до 2012. године укупно 35.000 фунти тако што је присвајао њихов идентитет, сакупљајући податке које су остављали по различитим друштвеним мрежама. Наиме, проучавајући личне податке својих комшија које су остављали на друштвеним мрежама, Вуд је на њихово име аплицирао код различитих банака за добијање кредитних картица. Такође, користио је и телефонско и електронско банковно пословање како би узимао новац са рачуна својих комшија са којима је контактирао преко друштвених мрежа. Оператере је молио да му ресетују шифру за улазак на рачун пошто не може да је се сети, а како је познавао већину личних података, попут датума рођења, девојачког презимена корисника, корисничког имена на друштвеној мрежи и сл. лако је могао да прође аутентификацију. Вуд је до те мере постао сигуран у своју тактику да је почео да директно пребацује новац са рачуна својих комшија на свој рачун, па је тако на крају и откривен. За извршено кривично осуђен је на казну затвора у трајању од 15 месеци. (Find Law UK, http://blogs.findlaw.co.uk/solicitor/2011/08/computer-crime-hacker-uses-facebook-to-steal-35k-from-neighbours.html, претражено 26. 01. 2015. године)

Један полицијски инспектор се на друштвеним мрежама представио као четрнаестогодишња девојчица како би открио педофиле који су се појављивали на мрежи. (McGrath, Michael, Casey, Eoghan, 2002.). Тако је ступио у контакт са Чарлсом Вајтом (49) који му се јавио на ћаскању преко друштвеног сервиса АОЛ. Наредна два и по месеца, Вајт је покушавао да задобије поверење „жртве“ за коју је мислио да је четрнаестогодишња девојчица, најпре је то чинио преко ћаскаоница, затим је почео да шаље своје слике, да се поставља заштитнички и заводљиво. После извесног времена, Вајт је од „жртве“ затражио да му пошаље пар гаћица и да се са њим и уживо нађе. У међувремену је почео да "жртви" шаље дечију порнографију, чиме је заправо омогућио инспектору да га открије. Приликом хапшења код Вајта су нађене слике сексуалног односа са девојчицом из комшилука. Вајт је проглашен кривим за сексуалну експлоатацију малолетног лица, поседовање и дистрибуцију дечије порнографије, илегално прелажење државне границе ради противзаконитог сексуалног односа са малолетним лицем и незаконито поседовање оружја, и осуђен на 10 година затвора. (U.S. v. White, Case No. IP99-CR-0005-01-M/F (S.D. Ind.1999), http://www.casebriefs.com/blog/law/criminal-procedure/criminal-procedure-keyed-to-israel/arrest-search-and-seizure/united-states-v-white/, претражено 12. 09. 2014. године)

Румун Лаурентиу Кристиан Буска (26) осуђен је марта 2013. године на затворску казну у трајању од 5 година због фишинг превара (облика крађе идентитета) чије су жртве клијенти америчких компанија и финансијских институција. Буска је, заједно са својим саучесницима, слао поруке путем електронске поште у име компанија PayPal, eBay, Comerica Bank, Regions Bank, LaSalle Bank, Well Fargo, Citibank, Capital One, Bank of America i JP Morgan Chase, којим је клијенте ових компанија обавештавао да постоји проблем са њиховим рачуном и да треба да посете сајт на коме треба да оставе своје личне податке, укључујући и податке као што су бројеви платних картица, датум истека картице, ПИН-ови, имена, адресе, бројеви телефона, и бројеви социјалног осигурања. Тако прикупљене информације, преваранти су касније користили за приступ рачунима и извлачење новца и то најчешће са банкомата у Румунији. Претпоставља се да је Буска, у периоду од 2004. до 2006. године, на овај начин украо 10 000 бројева дебитних или кредитних картица, а поред њега још 18 држављана Румуније оптужено је за саучесништво у овом случају. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Pet-godina-zatvora-zbog-fising-prevara.html, претражено 26. 01. 2015. године)

Педофилија и сексуално насиље често почиње најпре контактом преко интернета или друштвене мреже када се извршиоци представљају као деца или тинејџери како би намамили малолетне жртве да им најпре верују, па затим и да се са њима виде. Ричард Ромеро (35), који је најпре задобио поверење једног тинејџера представљајући се као петнаестогодишњак. (McGrath, Michael, Casey, Eoghan, *op.cit.,* 2002.), био је осуђен за отмицу, превођење малолетног лица преко државне границе са намером да га укључи у противправну сексуалну активност и за ометање правде јер је покушао да уништи доказе својих кривичних дела. (U.S. v. Romero, 189 F.3d. 576 (7th Cir. 1999), http://openjurist.org/189/f3d/576/united-states-of-america-v-richard-romero, претражено 12. 09. 2014. године)

Адвокатску стручну јавност је забринула чињеница да се на интернету појављује све већи број лажних адвокатских фирми које нуде своје услуге тако што сакупљају податке о финансијском пословању потенцијалних „клијената“. Ове лажне адвокатске фирме користе биографије и профиле „правих“ адвоката и адвокатских канцеларија, покушавајући да на овај начин улију поверење „клијентима“ које покушавају да преваре. На пример, лажна презентација непостојеће адвокатске куће Carter Legal Associates је за партнера у фирми навела име Едварда Скота (Edward Scott QC), адвоката који заиста постоји и који је веома поштован у струци када је реч о заступањима и одбрани у кривичној и прекршајној материји (Neil, Martha: „Fake law firm websites using real lawyers' profiles are increasing, bar group says“, ABA Journal – Law Practice Management, http://www.abajournal.com/news/article/fake_law_firm_websites_using_real_lawyers_profiles_are_fishing_for_financia, претражено 23. 02. 2015. године).

Најекстремнији забележени случај крађе идентитета је свакако случај белоруса Димитрија Насковеца (26), који је признао да је руководио веб сајтом CallService.biz који је нуди услуге крађе идентитета онима који су касније звали банке представљајући се као да су легитимни власници банковних налога и тврдећи да су они у ствари жртве крађе идентитета. CallService.biz се рекламирао податком да је преко њега обављено 5400 оваквих позива банкама. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/38-godina-zatvora-zbog-kradje-identiteta.html, претражено 26. 01. 2015. године)

Случај Меган Мајер, који се догодио у Мисурију (САД), има елементе и лажног представљања и вршњачког насиља. Тринаестогодишња девојчица Меган извршила је самоубиство након што јој је њен шеснаестогодишњи "пријатељ" са друштвене мреже MySpace, кога она никада није упознала нити срела, рекао да ће "свет бити много боље место уколико она нестане са њега". Заправо, тај шеснаестогодишњи дечак није ни постојао, већ је то била особа која се крила иза лажног профила измишљеног дечака. Лажни профил је направила Лори Дру, мајка девојчице која је са Меган ишла у исто одељење и хтела да се освети Меган због свађе која је у току истраге била оптужена за компјутерску превару због прављења лажног профила на друштвеној мрежи, слања увредљивих порука и изнуђивања поверљивих информација од малолетног лица, али и за кршење правила понашања на друштвеној мрежи MySpace. (Више о случају Меган Мајер на интернет страни Megan Meier Foundation,http://www.meganmeierfoundation.org/megans-story.html,претражено 03.01.2015.године, а видети и Decision of Defendant’s F.R.CRIM. 29(c) Motion, Case UNITED STATES of America, Plaintiff, v. Lori DREW, Defendant. No. CR 08–0582–GW. | Aug. 28, 2009., http://stanford.edu/~jmayer/law696/week1/United%20States%20v.%20Drew.pdf, претражено 03. 01. 2015. године)

Први забележени пример који је узбуркао јавност у Србији и отворио бројне расправе о регулисаности компјутерског криминалитета, сигурности компјутерских система и реаговања судских и полицијских органа при квалификовању дела и вођењу самог поступка је случај „КОНЕКО". Београдски "Економски биро-КОНЕКО", једна од најзначајнијих саветодавних фирми и партнер Министарства за привреду и приватизацију и Агенције за приватизацију, опљачкан је у ноћи између 26. и 27. децембра 2002. године, када су се непознати извршиоци попели кроз необезбеђени улаз зграде, попели на трећи спрат, развалили улазну браву и са шест (од укупно десет) компјутера скинули и однели хард дискове са свим подацима који су се на њима налазили. Након само неколико дана, у ноћи између 10. и 11. јануара 2003. године КОНЕКО је поново био мета напада, приликом чега је однето нешто техничких уређаја и велики број компакт-дискова на којима је био снимљен део важне документације о предузећима чија се вредност процењивала у овом Бироу. На хард дисковима и компакт-дисковима који су украдени налазила се процена вредности комплетног капитала више стотина српских предузећа које су се припремала за приватизацију. Биро је ове податке прикупљао и обрађивао са званичном лиценцом Министарства за привреду и приватизацију. Свако ко је у датом моменту поседовао ове податке имао је стартну предност у односу на конкуренцију, на аукцијама или тендерима који су били расписани за предузећа у процесу приватизације. Управо је та чињеница отворила бројне могућности за злоупотребу, пошто процена вредности капитала проедставља пословну тајну сваке фирме. (Случај КОНЕКО је наведен у чланку Николић Слађана "Случај економског бироа КОНЕКО-аларм за узбуну", APIS Security Consulting, http://www.apisgroup.org/sec.html?id=26, претражено 08. 06. 2012. године)

Један од последњих забележених случајева крађе личних поверљивих података догодио се у периоду децембар 2014 - јануар 2015. године, када су петорица младих српских хакера неовлашћено ушли у државне системе са личним подацима свих грађана Србије. Наиме, хакери су послали електронску поруку једној од најчитанијих дневних новина у Србији у којој је писало да су дошли у посед матичних бројева, адреса и бројева телефона великог броја грађана Србије и као доказ у поруци доставили и осам табела са личним подацима неколицине грађана Београда, Новог Београда, Чачка, Сремских Карловаца, Новог Сада, Аранђеловца и Јагодине. (Блиц – дневна новина од 12.12.2014.године, http://www.blic.rs/Vesti/Drustvo/518714/KAKO-SU-HAKERI-DOSLI-DO-NASIH-PODATAKA-Upali-u-spiskove-partija, претражено 12. 12. 2014. године).

У свом обраћању, као мотиве оваквог поступка хакери су навели да „народ треба да види колико је његова приватност у овој земљи угрожена, да виде како је могуће да се дође до свих података о свакоме али и да држава види и после више упозорења схвати да је заштита система у коме се чувају подаци слаба". (Блиц – дневна новина од 11.12.2014.године, http://www.blic.rs/Vesti/Drustvo/518514/DRZIMO-SRBIJU-U-SACI-Hakeri-tvrde-da-su-ukrali-JMBG-gotovo-svih-gradjana, претражено 11. 12. 2014. године). Неколико дана касније, у истим дневним новинама објављена је вест да су због организовања хакерских напада на заштићене мреже ухапшена два дечака од 16 година, чланови хакерске групе "Српски хакери", који су неовлашћено приступили заштићеном рачунару и скинули податке које су доставили редакцији дневних новина, уз напомену која је наведена у објављеном тексту да су сви подаци о грађанима који су на списковима били достављени заправо лажни. Против њих је поднета кривична пријава због сумње да су на наведен начин дошли у посед базе чланства једне политичке партије и проследили је медијима. Прегледом рачунарске опреме која је припадала двојици момака пронађени су злонамерни програми који служе за крађу података, текстуални фајлови на којима се налазе корисничка имена и шифре електронских налога за које постоји сумња да припадају грађанима Србије као и подаци о више платних картица у електронском облику. Двојици осумњичених је одређен притвор у трајању до 30 дана, а рачунарска опрема која је служила за извршење овог кривичног дела је одузета. (Блиц – дневна новина од 14. 01. 2015. године, http://www.blic.rs/Vesti/Hronika/526500/SAZNAJEMO-Uhapseni-tinejdzeri-koji-su-objavljivali-zasticene-podatke, претражено 14. 01. 2015. године)

Дејвид Реј Камез (22) осуђен је маја 2014. године на 20 година затвора, плаћање накнаде штете у износу од 20 милиона долара и на три године служења казне под надзором због оптужбе да је био члан криминалне организације која је руководила трговином украденим личним подацима корисника друштвених мрежа. Камез се 2008. године придужио форуму Carder.su, који је у јулу 2011. године имао око 5500 чланова. Током 2009. и 2010. године он је од агента ФБИ који је био убачен на овај форум куповао лажне возачке дозволе а продавао фалсификоване кредитне картице које су му послате из Пакистана. Приликом претерса Камезовог дома у Фениксу, пронађен је и велики број фалсификованих кредитних картица и опреме за њихову израду, фалсификовани новац и личне карте, док је у Камезовом рачунару приликом претреса пронађен софтвер за кодирање кредитних картица као и украдени подаци жртава крађе идентитета. (Član foruma Carder.su osuđen na 20 godina zatvora, http://www.informacija.rs/Sajber-hronika/Clan-foruma-Carder-su-osudjen-na-20-godina-zatvora.html , претражено 26. 01. 2015. године)

г) Облици заштите. Крађа идентитета путем коришћења интернета разликује се од крађе идентитета без коришћења интернета (одузимање новчаника са новцем и кредитним картицама).[275] Крађа идентитета путем интернета може имати значајне последице јер већина жртава крађе идентитета на интернету уопште одмах не препознаје да је нешто украдено од њих док се не појаве финансијски губици или кад се приватне и поверљиве информације корисника искористе за добијање лажних докумената (документ са туђим подацима и фотографијом извршиоца).[276] Због тога жртва треба одмах када посумња да постоји крађа идентитета да обавести банку у којој има рачуне или финансијску институцију која врши трансакцију.[277]

Како корисник не би постао жртва крађе идентитета, неопходно је да: никада не даје број кредитне картице преко телефона осим ако је корисник тај који је звао и сигуран је у поузданост саговорника; сваког месеца проверава стање на рачуну и да о свим стварима које му се чине чудним одмах обавести

[275] Internet Identity Theft, http://articles.winferno.com/computer-fraud/internet-identity-theft, претражено 17. 09. 2012. године

[276] Beal, Vangie: "How to Defend Yourself Against Identity Theft", http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp, претражено 17. 09. 2012. године

[277] Иако не постоје прецизни подаци колика је учесталост вршења овог кривичног дела, нека америчка истраживања су дошла до податка да је у протеклих пет година један од осам америчких грађана/грађанки био жртва интернет крађе идентитета. *Цит. према:* Internet Identity Theft, http://articles.winferno.com/computer-fraud/internet-identity-theft, претражено 17. 09. 2012. године

банку; уколико уочи, банци и полицији пријави све неауторизиване финансијске трансакције.[278]

Корисници друштвених мрежа морају себе да заштите од могуће крађе или злоупотребе идентитета и на тај начин што ће пажљиво бирати своје пријатеље и контакте. Интересантно истраживање спровела је сигурносна фирма Sophos[279] у циљу приказивања недостатака друштвених мрежа, могућности њихове злоупотребе као и неопрезности самих корисника. Наиме, направљена су два лажна профила на друштвеној мрежи Facebook: први профил је регистрован на име Daisy Feletin старе 25 година који је за профилну слику имао лик гумене паткице, а други профил био је регистрован на име Dinette Stonily старе око 50 година, а за профилну слику је имао лик мачке која се игра. Истраживање је било усмерено на кориснике друштвене мреже Facebook који су из Аустралије, а са сваког од лажних профила послато је по 100 захтева за пријатељство различитим људима. На захтеве за пријатељство који су послати позитивно је одговорило 87 контактираних особа, а интересантно је да је захтев за пријатељство послало још 5 особа које нису биле непосредно контактиране већ их је привукао један од ова два фиктивна профила. Интересантно је колико се личних података разменило на овакав начин: преко 87% је учинило доступним адресу своје електронске поште, а телефонски број је фиктивној "пријатељици" дало 23% млађе и 7% старије популације. Личне ствари о себи и члановима своје породице причало је 46% млађих корисника и 31% старијих, док је 89% млађих и 57% старијих написало у комуникацији свој пун датум рођења.

OECD је указао на неке од главних проблема са којима се све државе сређу приликом решавања проблема крађе идентитета: непостојање јединствене дефиниције овог дела, нерегулисаност крађе идентитета као кривичног дела *per se* у националним законодавствима, побољшање сарадње са приватним сектором, непостојање оквирних статистичких података о обиму и структури извршења овог дела, непостојање програма помоћи жртвама и одговарајућих

[278] The FBI – Common Fraud Schemes: Internet Fraud, http://www.fbi.gov/scams-safety/fraud/internet_fraud , претражено 03. 05. 2013. године

[279] Sophos, http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/, претражено 19. 12. 2012. године

правних лекова, недовољна едукација корисника друштвених мрежа на који све начин може да дође до крађе идентитета. [280]

3.1.2. Прогањање преко интернета (сајбер прогањање, ухођење, енгл. cyber stalking)

а) Појам прогањања и интернет прогањања. Понашања попут прогањања и сексуалног узнемиравања увек су се у стварном животу везивали искључиво за близак физички контакт насилника и жртве: жртва се прогони „из близине", а прогонитељи желе да их жртва види и буде свесна њиховог присуства.[281] Међутим, на Интернету, близина добија ново значење јер у виртуелном свету корисници имају илузију близине иако су физички удаљени.

Осећај реалне, физичке близине насилника и жртве је поткрепљен чињеницом да друштвене мреже у профилима својих корисника најчешће садрже информације о локацији боравка, распореду активности и месту последњег логовања корисника,[282] што потенцијалном уходитељу помаже да одреди физичку локацију корисника. Прогањање и сексуално узнемиравање путем интернета представљају велики, у Србији још увек правно нерегулисан проблем, који у потпуности релативизирају питање близине.

Појам прогањања путем интернета (сајбер прогањање, енгл. cyber stalking) још увек није потпуно прецизно одређен и усаглашен у теоријским и истраживачким радовима. Шире дефиниције сајбер прогањања се односе на прогањање путем свих средстава информационе и комуникационе технологије, не само путем интернета. Прогањање представља нежељену и злонамерну комуникацију, оштећење туђе имовине и физички или сексуални напад на неку особу, који је интензиван и нежељен и изазива страх.[283]

Осим тога, приликом одређивања појма интернет прогањања, постоји велики број схватања која настоје да утврде разлику између класичног прогањања и сајбер прогањања. Између интернет прогонитеља и „стварних" прогонитеља постоје бројне сличности и разлике. Слично правим

---

[280] OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, *op.cit.,* 2007, стр.5

[281] Gilbert, Pamela: "On Sex, Cyberspace, and Being Stalked*",* Women and Performance 9, No.1, 1996, стр. 125-149

[282] Gross, Ralph, Acquisti, Alessandro, *op.cit.,* 2005., стр. 78

[283] Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking, Women's Aid Federation of England, 2014, www.womensaid.org.uk, претражено 08. 01. 2015. године

прогонитељима, cyber 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 online активности. Жртва постаје несигурна, уплашена, застрашена и не сагледава начин на који може да утиче на престанак узнемиравања и прогањања.

Као и у случају стварног, физичког прогањања, и прогањање преко интернета може да често буде увод за испољавање агресивног понашања које води у физичко насиље. [284]

Сличности између физичког прогањања и прогањања преко интернета	Разлике између физичког прогањања и прогањања преко интернета
Прогонитеља најчешће мотивише велика жеља да има контролу и моћ над жртвом.	За разлику од физичког прогањања, прогонитељ и жртва не морају да се физички и географски налазе близу.
У већини случајева, прогонитељ и жртва се познају или је чак реч о некадашњим партнерима, док код прогањања преко интернета прогонитељ можда никада није ни видео своју жртву нити зна било шта о њој.	Невидљивост и анонимност која је карактеристична за виртуелни простор, а посебно за комуникацију преко друштвених мрежа, охрабрује насилнике да узнемиравају и застрашују жртву.
Највећи број жртава прогонитеља је женског пола. Највећи број прогонитеља је мушког пола.	У виртуелном свету моралне баријере које нас оптерећују у свакодневном животу су смањене, интернет прогонитељ може да извегне суочавање „очи у очи“ са жртвом.

Једна од најуочљивијих сличности обе врсте преступника је да желе да имају моћ, контролу и утицај над жртвом.[285] Често се прогањање у виртуелном свету сматра релативно безопасним, али, уколико се на овакво понашање не обрати пажња и не пријави надлежним органима, постоји опасност да дође до физичког контакта насилника и жртве.

Очигледан начин разграничења традиционалног дела прогањања од интернет прогањања је чињеница да се интернет прогонитељи ослањају углавном на интернет као средство електронске комуникације како би малтретирали, претили и застрашивали своје жртве које су одабрали. Највећи

[284] Benschop, Albert, *op.cit.,* 2003.
[285] Reno, 1999, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.184

број понашања интернет прогонитеља може да се окарактерише као свесно испланирано, склоно понављању, веома досадно и упорно понашање.[286] Разлика између прогањања и интернет прогањања је и географска удаљеност између прогонитеља и жртве. У случајевима традиционалног прогањања, жртва и насилник углавном живе или раде једно близу другога, док интернет прогонитељ може своју жртву да злоставља и из суседне куће, али и из далеке земље.[287] Код прогањања путем интернета ретко кад постоји било какав физички контакт, па је то један од разлога што полиција не придаје велику пажњу пријављивању оваквог понашања и не реагује на жртвине пријаве.[288]

Прогањање путем коришћења интернет мреже дефинише се као упорно и циљано злостављање појединца путем електронских начина комуникације[289] или као употреба нових технологија у циљу прогањања неке особе.[290] Овакво понашање може да буде само „виртуелно“ и ограничено само на online комуникациони простор, али се може пренети из „виртуелног“ у „стварни“ свет и тада представљати увод у најопасније облике виктимизације. Постоје и аутори који сматрају да је сајбер прогањање заправо наставак физичког прогањања.[291]

Појам „прогањања” осамдесетих година XX века користио се за означавање „трајнијег облика злостављања према истој особи наметањем комуникације или контакта које та особа не жели”.[292] Овако дефинисано, прогањање обухвата понављање извесних радњи које трају дуже време, попут: честих телефонских позива упућених жртви, слање жртви писама или поклона различите садржине, праћење и посматрање жртве, прелазак и боравак у простору који је у власништву жртве, ступање у контакт са породицом жртве, са њеним пријатељима или сарадницима.[293]

---

[286] Hutton & Haantz 2003, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.184.
[287] Reno, 1999, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.184.
[288] *Ibid.*, стр.185.
[289] Yar, Majid: “Cybercrime and society”, SAGE Publications, Lonodon, 2006., стр.122 и Yar, Majid: “The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory”, European Journal of Criminology, October 2005 vol. 2 no. 4, стр. 407-427, http://www.sagepub.in/upm-data/27202_6.pdf, претражено 28. 08. 2015. године
[290] Clough, Jonathan: “Principles of Cybercrime”, Cambridge University Press, 2010, стр. 366.
[291] Petherick, Wayne :”Cyberstalking: Obsessional pursuit and the digital criminal”, 2001, http://www.crimelibrary.com/criminology/cyberstalking/index.html, претражено 14. 11. 2014. године
[292] Mullen et. al. 2001: 9, наведено код Yar, Majid, *op.cit.,* 2006, стр.123
[293] McGuire, Brian, Wraith, Anita: “Legal and psychological aspects of stalking: A review”, Journal of Forensic Psychiatry, volume 11 no.2, 2000, стр. 317.

Прогањање представља више пута поновљен начин понашања којим једна особа другој намеће нежељену комуникацију или сусрете, што има за последицу испољавање жртвиног страха да није безбедна[294] односно „више пута поновљено коришћење интернета, електронске поште или неког другог електронског начина комуникације у циљу нервирања, застрашивања, претњи или злостављања одређене особе“.[295]

И други аутори повезују сајбер прогањење са настанком психолошких последица код жртве. У овим дефиницијама се истиче да употреба интернета, електронске поште, било ког другог облика електронске комуникације може да доведе до застрашивања, злостављања и осећања страха код једне или код више жртава и да се мења од наизглед безопасних до потенцијално веома опасних порука.[296]

Једну од првих и најширих дефиниција прогањања путем интернета дао је Пол Боциј (Paul Bocij) наводећи да интернет прогањање представља скуп понашања којима индивидуа, група људи или организација користи информационе и комуникационе технологије како би злостављала другу индивидуу, групу људи или организацију.[297] Овакво понашење може да обухвата између осталог, претње и лажне оптужбе, крађу идентитета, крађу података, оштећење података и опреме, неовлашћено коришћење видео надзора и контроле, облик агресије, коришћење одређене информације и сл. којом се некој особи наноси емоционални бол и несигурност.

Према другој дефиницији појам инернет прогањања у највећој мери се односи на употребу интернета, електронске поште, било ког облика електронске комуникације којом се ствара криминални ниво застрашивања, злостављања и осећања страха код једне или код више жртава. Овакво понашање може да

[294] Purcell, Pathe, Mullen, 2004, стр.157 наведено код Clough, Jonathan, *op.cit.,* 2010, стр. 365.
[295] D'Ovidio, Robert, Doyle, James: "Cyberstalking: Understanding the Investigative Hurdles", FBI Law Enforcement Bulletin, volume 72 no.3, 2003, стр. 10 – 17, https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=199743, претражено 24. 03. 2015. године
[296] Petrocelli, 2005; Reno, 1999, наведено код Pittaro, L. Michael: "Cyber stalking: An Analysis of Online Harassment and Intimidation", International Journal of Cyber Criminology, Vol 1 Issue 2, 2007, стр. 181, http://www.cybercrimejournal.com/pittaroijccvol1is2.htm, претражено 10. 05. 2014. године
[297] Bocij, Paul: "Cyberstalking: harrasment in the Internet age and how to protect your family", Praeger Publications, 2004, стр. 10

варира од безопасних али досадних порука па до потенцијално опасних и смртоносних сусрета прогонитеља и жртве. [298]

Организација за интернет сигурност „Интернет анђели“ (енгл. CyberAngels)[299] прогањање путем интернета дефинише као коришћење интернета, електронске поште или неког другог облика електронске комуникације у циљу претњи, праћења и злостављања неке особе. Основна обележја овако испољеног понашања су: доминира осећање злобе, постоји намера, понавља се извршење, проузрокује се осећај узнемирености и несигурности, испољава се опсесивност, освета, малтретирање, претње и прогањање не престаје упркос захтевима жртве.[300]

Приликом дефинисања појма сајбер прогањања, аутори посвећују пажњу начину и средствима којима се врши злостављање појединца, док мотиви због којих се то чини нису обухваћени дефиницијама. Разлог за овакав приступ свакако је мноштво и различитост мотива сајбер прогањања. Интернет прогањање не мора да буде мотивисано сексуалном опсесијом према жртви. Оно може да буде мотивисано постојањем нетрпељивости између прогонитеља и жртве или агресијом, која је настала као последица неједнакости моћи и угледа у друштву, чешће него материјалним добитима или сексуалним опсесијама.[301] Интернет прогањање је, као и прогањање уопште, вођено осећањима беса, моћи, контроле, које су пробуђене чињењима или нечињенима жртве.

б) Појавни облици и врсте интернет прогањања. Прогањање путем интернета може да се изврши на два начина: (1) *у потпуности преко интернета* – прогањање које се дешава само коришћењем интернета и друштвених мрежа, нема личних контаката осим оних који се односе на виртуелни свет, може да се врши слањем електронских порука, комуникацијом у причаоницама и преко блогова, друштвених мрежа или интернет страница; (2) *мешовити тип прогањања* – прогањање почиње најпре преко интернета и као такво траје

[298] *Ibid.*, стр. 14.
[299] Cyber Angels, http://www.cyberangels.org/ , претражено 01. 11. 2012. године и 01. 03. 2013. године
[300] Ова организација дневно добија до 500 пријава о постојању виктимизације интернет прогањањем, од којих 65-100 пријава буде основано и засновано на закону. За територију САД, то значи да ова организација забележи између 24.000 – 36.500 случајева интернет прогањања годишње. *Ibid.*
[301] Mustaine, Tewksbury, 1999, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.181

неколико недеља, након чега почиње да се дешава и у „реалном“ свету (нпр. прогонитељ покушава да оствари лични контакт са жртвом), контакт може да се одржава и електронски, коришћењем интернета али је могуће такође и обрнуто: да прогонитељ жртву из „реалног“ окружења почне да прати у виртуелном свету.[302]

Најчешћи појавни облици интернет прогањања су:

1. *нежељена комуникација жртве са прогонитељем* – слање нежељених електронских порука путем електронске поште, причаоница, форума па чак и мобилних телефона представља окосницу интернет прогањања и његов најчешћи вид. Прогонитељ остаје анониман јер може да користи анонимне интернет адресе и адресе електронске поште, а лакоћа и брзина интернет комуникације омогућава прогонитељу да жртву засипа нежељеним порукама.

2. *објављивање / чињење доступним личних података о жртви* – велики број информација се свакодневно добровољно пласира на интернет преко различитих друштвених мрежа. Лакоћа којом је могуће објављивати личне податке о себи на интернету је плодно тло за активности прогонитеља којима је циљ да понизе или застраше своје жртве.

3. *напад на компјутер жртве* – прогонитељ, који је технички образован, путем злонамерног програма добија приступ рачунару жртве у циљу уништавања података, застрашивања или шпијунирања активности и кретања жртве. На овај начин, прогонитељ са сигурне удаљености може да контролише приступ информацијама, активностима, да брише и мења податке које жртва има у рачунару.

4. *сталан надзор над активностима жртве / стављање жртве под присмотру* – надзор над жртвом је незаобилазан вид прогањања који је постао све заступљенији бројним техничким достигнућима. Сврха надзора може да буде двојака. Прво, надзор може да се спроводи у циљу прикупљања личних података о жртви, о људима са којима контактира, о свакодневном кретању. Друго, сврха надзора може да буде и буквално праћење кретања жртве,

[302] Sheridan P. Lorraine, Grant,T.: "Is cyberstalking different?", Psychology, Crime & Law, volume 13 no. 6, 2007, стр. 627-640, http://www.tandfonline.com/doi/full/10.1080/10683160701340528, претражено 02. 03. 2013. године

директним праћењем или праћењем и снимањем различитим дигиталним уређајима.[303]

Остали појавни облици интернет прогањања су: узнемиравање у причаоницама, објава непријатељског садржаја, ширење злобних неистина и трачева, електронска саботажа нпр. слање вируса и сл., јавно омаловажавање некога у виртуелном простору, претећи телефонски позиви преко интернета (skype), слање отворених претњи.[304]

Врсте прогањања преко интернета могу се разликовати према понашањима прогонитеља: наручивање ствари преко интернета на име друге особе као и давање електронске адресе те особе различитим сајтовима и рекламним порталима; крађа идентитета који нека особа има у виртуелном свету како би се о тој особи ширили неистине; слање нетачних података о некој особи у групе за ћаскање и/или оформљене групе које су повезане заједничким интересовањима а све у циљу да се нека особа понизи а да се други корисници охрабре да малтретирају и вређају одређену особу; откривање локације на којој се нека особа налази или објављивање слике неке особе на порнографске интернет портале; неовлашћено приступање банковним рачунима, претплатама, телефонским рачунима и листинзима неке особе или било којим другим личним подацима који су доступни преко интернета; прављење интернет стране посвећене некој особи, без њеног знања и дозволе; приступање, надгледање и манипулација рачунаром неке особе док се она налази на интернету; праћење неке особе кроз незаконито снимање, надгледање или коришћењем било којих других начина праћења. [305]

Понашање прогонитеља критеријум је и за друге класификације интернет прогањања. Тако се интернет прогањање може разврстати на следеће облике: [306]

(1) Учестале претње - претње могу да буду упућене одређеној особи (жртви), њеним члановима породице, колегама или пријатељима коришћењем

---

[303] Clough, Jonathan, *op.cit.,* 2010, стр. 375.

[304] Pettinari, Dave: "Cyberstalking investigation and prevention", http://www.crime-research.org/library/Cyberstalking.htm, претражено 03. 08. 2014. године

[305] Hensler-McGinnis, Nancy Felicity: "Cyberstalking victimization: impact and coping responses in a national University sample", 2008, http://drum.lib.umd.edu/bitstream/1903/8206/1/umi-umd-5402.pdf, стр. 14, претражено 12. 12. 2014. године

[306] Bocij, Paul, *op.cit.,* 2004, стр. 13

електронских начина комуникације (електронска пошта, друштвене мреже, причаонице, факс или чак и СМС).

(2) Пласирање неистина о жртви – многи прогонитељи покушавају да наруше углед жртве и да јој напакосте пласирајући различите неистине, користећи електронску пошту да дође до жртвиних пријатеља, рођака, колега... Понекад прогонитељи пласирају неистине и кроз мреже различитих интернет интересних група, на интернет портале и сл.

(3) Узнемиравање жртве – прогонитељи могу својим жртвама да шаљу електронске поруке или „ћаскања“ са различитим увредљивим или порнографским садржајем, како би је узнемиравали.

(4) Напад на електронске податке и компјутерску опрему жртве - средство напада прогонитеља могу да буду и електронски подаци жртве или компјутерска опрема коју жртва има, слањем злонамерног софтвера или рачунарског вируса.

(5) Прикупљање различитих личних података о жртви – лични подаци се могу прикупљати на различите начине: противправним „упадом“ у компјутер жртве, кроз разговоре са пријатељима, рођацима и колегама жртве, па чак и унајмљивањем приватних детектива који би пратили жртву.

(6) Крађа идентитета жртве и/или лажно представљање жртвиним именом – прогонитељ може у „причаоницама“ да користи име жртве док комуницира са другим људима и док шаље поруке другима. Циљ оваквог поступања је омаловажавање жртве или вршење преваре.

(7) Вршење утицаја на друге да малтретирају жртву – понекад и трећа лица могу индиректно да злостављају жртву. Прогонитељ може да објави оглас или рекламу сексуалног садржаја са бројем телефона жртве. Неке жртве су пријављивале да су примиле стотине позива и електронских порука на овај начин.

(8) Наручивање и куповина у жртвино име – могуће је да прогонитељ наручује скупоцене ствари на жртвино име, тако да жртва има проблем да ове ствари плати или врати ономе од кога су наручене. Било је случајева да прогонитељи наручују предмете који би осрамотили и компромитовали жртву (нпр. сексуална помагала, која се жртви достављају на радно место).

(9) Физички сустрет са жртвом – неки прогонитељи који не познају лично жртву, већ са њом комуницирају само путем интернета, могу да одлуче да

организују сусрет са жртвом или да је без њеног знања прате приликом обављања дневних активности. Овакво понашање се често манифестује као педофилија.

(10) Физички напад на жртву – овакви случајеви су ретки, али је могуће да прогонитељ поред прогањања путем интернета и физички нападне жртву.

в) Типологија интернет прогонитеља. Интернет прогонитељ је особа која користи интернет као оружје или средство за праћење, узнемиравање, слање претњи и стварање страха и стрепње код жртве, користећи софистициране тактике.[307] Слично прогонитељима из реалног живота, интернет прогонитељи покушавају да надгледају активности своје жртве, пронађу што више података о њој, контактирају особе са којима је жртва блиска, да на незаконит начин читају пошту своје жртве и прате њене интернет активности. Жртва постаје несигурна, уплашена, застрашена и не сагледава начин на који може да утиче на престанак узнемиравања и прогањања. Срж моћи сваког прогонитеља је поседовање знања о жртви. Могућност да је застраши и контролише зависи од броја информација које прогонитељ поседује и до којих може да дође.[308]

Виртуелни прогонитељи своје жртве у највећој мери проналазе посећујући форуме и причаонице. Када остваре први контакт, потрудиће се да се жртви представе као да су јој прави пријатељи или ће једноставно у својој перцепцији створити такву слику о њиховом односу. Другим речима, прогонитељ заиста верује да између њега и жртве постоји јака и присна веза, иако је жртва наивно само куртоазно одговорила на питања која јој је прогонитељ поставио приликом „сусрета“ у причаоници или на форуму.[309]

Форуми су најпогоднија места где насилник може да објављује своје злобна мишљење и коментаре, личне податке о жртви или да износи различите неистине о њој. Поједини аутори наводе основна обележја овако испољеног понашања, наглашавајући да код прогонитеља доминира осећање злобе, да постоји намера за такво понашање, да се извршење понавља, испољава се опсесивност, освета, малтретирање, а претње и прогањање не престаје упркос

[307] Pittaro, L. Michael, *op.cit.,* 2007.
[308] McGrath, Michael, Casey, Eoghan., 2002, стр. 89.
[309] Stephens 1995, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.184

захтевима жртве.[310] Овакво понашање код жртве проузрокује константно осећање узнемирености и несигурности.

На Интернету постоје различити сајтови који се у потпуности баве сајбер прогањањем. Тако нпр. неки од њих[311] покушавају да објасне који су заправо мотиви којима се воде интернет прогонитељи и да ова врста виртуелног прогањања није ништа безазленија од физичког прогањања. Десет најчешћих ралога за понашање прогонитеља су: завист прогонитеља према жртви, опсесија прогонитеља жртвом, прогонитељ мисли да је недодирљив и непобедив јер нико "не види" шта он ради, тренутно је незапослен и потребно му је нешто да му окупира пажњу и одагна мисли са другог проблема који има, жели да застраши жртву и да је доведе у инфериоран положај у односу на себе, има сумануте мисли које немају додир са реалношћу, жели да жртву потчини пред другима, жели да жртву обрука и доведе у непријатне ситуације пред другим људима, има проблем који не може сам да реши, превише је радознао, а та радозналост ствара фрустрацију због које уходи жртву и прети јој.[312]

Смањењем демотивационих фактора попут стида и страха од одбацивања, интернет може да охрабри појединце да се укључе у дијалог и да учине нека дела која би у „реалној" комуникацији ретко кад учинили. Прогонитељ који би у директном контакту био суздржан да започне комуникацију са потенцијалном жртвом, у интернет окружењу реагује без оклевања и жртви учестало шаље претеће или узнемирујуће поруке. Недостатак инхибиције може да прогонитеља „натера" да се у виртуелној комуникацији лажно представља: није ретка појава да прогонитељ преузме идентитет неког пријатеља или рођака жртве како би сазнао што више информација, или да се чак представља жртвиним именом ширећи различите неистине.[313]

---

[310] Bocij, Paul, *op.cit.,* 2004, стр.9

[311] Quit Stalking Me – Report a Cyberstalker, http://quitstalkingme.com, претражено 02. 07. 2014. године

[312] Ten Reasons Why Someone is Stalking You Online, http://quitstalkingme.com/2011/07/28/ten-reasons-why-someone-is-stalking-you-online/, претражено 02. 07. 2014. године

[313] Ellison, Louise: "Cyberstalking: Tackling harrasment on the Internet", Crime and the internet, London: Routledge, 2001, стр. 141, http://books.google.rs/books?id=JRb9BDTlrUsC&pg=PA141&lpg=PA141&dq=Ellison+Cyberstalking:+Tackling+harrasment+on+the+Internet&source=bl&ots=K2rQ0sNGFK&sig=dtrxWvfu2e5atvbxvXtKvYehCmI&hl=sr&sa=X&ei=5A-UIu_Gc_IsgaioYG4BA&sqi=2&redir_esc=y#v=onepage&q=Ellison%20Cyberstalking%3A%20Tackling%20harrasment%20on%20the%20Internet&f=false, претражено 02. 03. 2013. године

Недостатак личног контакта прогонитеља са жртвом може да доведе до различитих пројекција прогонитеља, због чега жртва може бити изложена одбацивању, понижењу или бесу.[314] У литератури се наводи да је велики број интернет прогонитеља већ имало претходну криминалну активност, историјат насилничког понашања или поремећај понашања који директно или индиректно повећава вероватноћу да ће се особа понашати социопатски.[315] Прикупљене студије о интернет прогонитељима показале су да код њих постоји поремећај личности који може да варира од високог нивоа параноје до различитих опсесивних мисли и понашања.[316]

Постоји много типологија интернет прогонитеља. Поделе и класификације прогонитеља вршене су према различитим критеријумима зависно од схватања појединих аутора.

Једну од првих типологија поставио је Мајкл Зона (Michael A. Zona) са сарадницима[317] на основу анализе 74 случаја које је испитивала полиција у Лос Анђелесу (САД). Они су навели да на основу посматраних случајева, све интернет прогонитеље је могуће поделити на: *еротомане* – имају нестварна веровања да је жртва заљубљена у њих и да заправо жели да буде са њим; *љубавне опсесивце* – имају нереализовану жељу да са жртвом буду у емотивној вези, понашају се фанатично, најчешће се везују за прогањање познатих личности, веома често болују од схизофреније или неког другог психичког поремећаја, и *опсесивце* – у највећем броју случајева реч је о бившем партнеру жртве који жели да остане у емотивној вези са жртвом или да јој се освети за нешто.

Мекфарлејн и Боцај (McFarlane & Bocij)[318] спровели су једно од најобухватнијег истраживања о интернет прогонитељима и њиховим жртвама.

---

[314] McGrath, Michael, Casey, Eoghan: "Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace", 30. journal of the American Academy of Psychiatry and the Law 81, 2002, стр. 86, http://www.jaapl.org/content/30/1/81.full.pdf+html, претражено 02. 03. 2013. године

[315] Hutton, Haantz, 2003; Reno, 1999, наведено код Pittaro, L. Michael, *op.cit.*, 2007, стр. 184.

[316] Mullen et.al, 1999, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр. 184.

[317] Zona, A. Michael, Sharma, S. Krunal. , Lane, C. John: "A comparative study of erotomanic and obsessional subjects in a forensic sample," Journal of Forensic Sciences, volume 38, 1993, стр. 894-903.

[318] McFarlane, Leroy , Bocij, Paul: "An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers", Journal First Monday, 2005, volume 8,

Из резултата добијених истраживањем, дефинисане су четири групе интернет прогонитеља:

(1) Осветољубиви интернет прогонитељи, *осветнички тип*, већ имају криминални досије и раније су се појављивали као злостављачи. Њихови поступци могу да буду индикатор менталног поремећаја. Злонамерни су и зли, развијају бројне тактике на који начин ће злостављати жртву, најчешће затрпавајући јој електронску пошту, шаљу злонамерне програме или краду идентитет. Ова категорија извршилаца има тенденцију да застрашује, прати и малтретира жртву на коју се фокусира. Забележени су бројни случајеви коришћења различитих „тројанаца" од стране ових извршилаца, јер на овај начин они директно могу да уђу у компјутер жртве, добијајући приступ свим њеним подацима.

(2) Сталожен интернет прогонитељ, тактику прогањања базира на жељи да код жртве створи сталан осећај страха и несигурности. Он је смирен, уравнотежен, неразметљив. Његов основни циљ је да жртву држи у сталном страху и тензији, на тај начин што према жртви испољава низ „претећих" понашања.

*(3) Интимни интернет прогонитељ***,** *романтичан тип*, има за циљ да буде у присној или интимној вези са жртвом услед своје опседнутости њоме. Код ове групе извршилаца, карактеристично је да ће за своју жртву одабрати особу према којој гаје страствена осећања и наклоност, за разлику од осталих типова где је могуће да за жртву буде насумице одабрана било која индивидуа која користи интернет или друштвену мрежу. Од поступака прогањања користе се e-mailovi, web групе за дискусију, сајтови за упознавање и др. Разликују се две подгрупе прогонитеља: бивши партнери или бивши познаници/пријатељи жртве и непознате особе које желе да успоставе интимну везу са жртвом.

(4) Колективни интернет прогонитељи, постоје у случају да два или више лица злостављају једну исту жртву. У ову групу интернет прогонитеља најчешће спадају лица која су део одређених интересних група и који су обучени за рад са компјутерским мрежама, јер овакво дело подразумева

---

http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/1076/996/, претражено 02. 03. 2013. године

организованију заједничку акцију у виртуелном простору него код претходних типова интернет злостављача.

Прогонитељ увек жели да се осећа надмоћно у односу на жртву. Особа која се изабере за жртву никада није једнако јака као прогонитељ. Управо је то разлог због чега су најчешће жртве интернет прогањања нови корисници друштвених мрежа (нпр. деца) и емоционално нестабилне особе. Тјапа и Кумар (Tjapa & Kumar)[319] сматрају да постоје три категорије интернет прогонитеља:

(1) Опсесивни интернет прогонитељ – злостављач који одбија да верује да је веза коју је имао са жртвом (пријатељска, емотивна) завршена. На овај начин, прогонитељ покушава на наизглед безопасан и искрен начин да обнови или поново успостави везу са жртвом.

(2) Интернет прогонитељ у заблуди – прогонитељ који може да буде ментално болесна особа (попут схизофреничара), који верује да између њега и жртве постоје нераскидиво јаке везе које не смеју да се прекину. Он је у стању да претпоставља да га жртва лудо воли чак и ако се никада нису срели. Овакав тип прогонитеља обично подразумева усамљеника који се најчешће везује за удате жене, познате личности, докторе, учитеље и сл. и њега је најтеже ослободити се.

(3) Осветољубиви интернет прогонитељ – особа која је бесна на своју жртву, без обзира да ли разлог заиста постоји или је умишљен, нпр. незадовољни запослени или бивши партнер, који ће покушавати да се освети за ситуацију у којој он верује да је био виктимизован.

Исти аутори наводе да психологија интернет прогонитеља може да буде различита јер зависи од степена менталног здравља прогонитеља[320] па тако разликују следеће типове прогонитеља:

(1) Одбачени прогонитељ – најчешће је био у вези са жртвом (иако има случајева када је жртва члан породице или близак пријатељ) и сматра да је прекид те везе неприхватљив. Овакво понашање карактерише мешавина осећања беса и жеље за помирењем.

---

[319] Tjapa, Anju, Kumar, Raj, *op.cit.,* 2011, стр. 5
[320] *Ibid.*

(2) Прогонитељ који тражи интимност – мотив је најчешће жеља за остварењем везе а особом која га физички привлачи а не дели осећања истог интензитета као и злостављач.

(3) „Неспособни удварач” – злостављач који покушава да развије везу али не успева да испуни све друштвене задатке који му се намећу. Најчешће је реч о особама граничне интелигенције или друштвено неинтелигентне особе.

(4) Огорчени прогонитељ – прогања своје жртве како би код њих створио страх и показао жељу за ретрибуцијом за неко понижење које је доживео или мисли да је доживео.

(5) Прогонитељ предатор – прикупља информације на основу којих у својој свести ствара фантазије које служе као припрема за сексуални напад на жртву.

(6) Прогонитељ у заблуди – најчешће подразумева особу са историјом менталне болести или поремећаја (нпр. схизофренија или манична депресија), која је престала са узимањем прописане терапије и тренутно живи у свету фантазија у коме су стварност и заблуде испреплетани. Пошто сама особа не може да разлучи шта је стварност а шта није, она запада у свет фантазија и дилема, при чему се везује за одређену особу и почиње да је прогони.

(7) Прогонитељ еротоман – такође живи у свом свету и најчешће је ментални болесник који умишља да је у вези са жртвом, са којом већ има исконструисан заједнички виртуелни живот. Слични прогонитељу еротоману су тзв. „љубавни пацови” (енгл. Love rats). Они нису прогонитељи у правом смислу, већ је реч о особама које лутају интернетом у потрази са особама са којима могу да ступе у емотивну везу. Њихова одлика је да у исто време одржавају неколико паралелних емотивних веза и да је њихов основни разлог коришћења интернета управо отпочињање нових веза са новим људима.

Мулен (Mullen) је са сарадницима проучавао осуђене починиоце дела прогањања који су се налазили на лечењу у Аустралијским психијатријским болницама.[321] Зависно од мотива прогонитеља, узрока због којих је до прогањања дошло, информација о претходном односу насилника и жртве и

[321] Mullen et al. (1999), наведено код McFarlane, Leroy , Bocij, Paul, *op.cit.,* 2005

психијатријској дијагнози прогонитеља, прогонитељи су могли да се класификују у пет категорија:

(1) одбачени прогонитељ који је са жртвом био у некој врсти присније везе (партнер, члан породице, близак пријатељ), па захлађење односа или прекид постојећих односа схвата као неприхватљив; овде постоје помешана осећања жеље за осветом и жеље за помирењем;

(2) прогонитељ који тражи интимност покушава да оствари и реализује везу са особом коју жели, а чију је пажњу у потпуности погрешно протумачио;

(3) некомпетентни удварач је незадовољан јер покушава да са особом коју жели оствари контакт, али не успева да притом испоштује одређене друштвене норме; обично су нижег интелектуалног нивоа или слабијег степена социјалне интелигенције;

(4) озлојеђени прогонитељ оптерећује своје жртве константном пажњом коју жртва доживљава као застрашујућу, а пошто не добија реакцију какву жели, прогонитељ може да жртви нанесе или стави у изглед одређено зло или да је јавно понизи;

(5) прогонитељ предатор прогони своју жртву како би сакупио што више података о њој и осмислио стратегију како би могао да се припреми за сексуални напад.

Поједини аутори[322] су на основу истраживања у коме су психијатријског процени подвргли 25 правно процесуираних интернет прогонитеља закључили да сви они могу да се сврстају у две категорије: *психотични,* који имају неки од симптома схизофреније, суманутих идеја са еротоманским елементима или елементима биполарних поремећаја, и *непсихотични,* који пате од поремећаја расположења, поремећаја личности или понашања које је проузроковано коришћењем дроге или алкохола.

Ова класификација била је основа за систем који је развијен посматрањем и анализирањем места злочина, форензичким доказима, пријављеним случајевима прогањања као и интервјуима са жртвама које су биле прогањане, а који се односи на: природу односа који постоји између жртве и насилника (да ли су у ближем односу или се не познају); садржај њихове

[322] Kienlen et al. (1997) наведено код McFarlane, Leroy , Bocij, Paul, *op.cit.,* 2005

комуникације (да ли је реалан или фантазија, тј.последица суманутих идеја прогонитеља); ниво агресије коју је прогонитељ испољио према жтзви (незнатан, средњи ниво или изразита агресија); мотиве прогонитеља (заљубљеност, посесивност, бес, одмазда), казну која је одређена за прогонитеља (правно санкционисање, смештај у психијатријску установу, самоубиство и др.). [323]

Према врсти мотива који су код њих преовлађивали, могуће су различите класификације прогонитеља. Бројне студије су показале да су најчешћи мотиви који доводе до прогањања путем интернета:

(1) *Сексуално прогањање* – када се помене прогањање, у већини случајева се подразумева сексуална заинтересованост једне особе за другу. Интернет служи као рефлексија стварног живота и људске психе, а анонимна комуникација олакшава ступање у контакт и константно упознавање активности које та особа има.

(2) *Опсесија љубављу* – може да почне одмах по започињању „интернет романсе" када једна особа одбија започињање љубавне интернет везе или када једна особа не жели да прихвати крај везе. Такође, нису ретки случајеви када се „интернет романса" пренесе и у реалан живот. Прогонитељ бива опседнут особом која му емоције не узвраћа и настоји да стално, па макар и у виртуелном свету, буде у њеној околини.

(3) Освета и/или мржња – најчешћи су мотиви интернет прогањања, а могу да почну обичном расправом која ће довести до стварања осећања мржње или жеље за осветом. Када код интернет прогонитеља постоји овакав мотив, жртва није ни свесна шта је погрешно учинила чиме је изазвала овакву емоцију, а веома често не зна ни ко је у ствари особа која је прогони у виртуелном свету и да ли је познаје. Овај тип прогонитеља најчешће користи виртуелни простор како би „избацио" своја незадовољства и фрустрације, уз жељу да се други људи осећају лоше.

(4) Јак его и жеља за моћи - интернет прогањање је генерално везано за осећај моћи који прогонитељ има над жртвом, а који је настао на његовој невидљивости и могућности да се крије иза туђег или измишљеног идентитета.

---

[323] Wright et al. (1996), наведено код McFarlane, Leroy , Bocij, Paul, *op.cit.,* 2005

Ова врста прогонитеља користи ову моћ да би се хвалила међу пријатељима и да би истакла своју идеју величине, тако да су жртве особе које уопште и не познају свог прогонитеља, већ су изабране насумице од свих интернет корисника. Особе које су биле жртве интернет прогонитеља овог типа најшешће су сматрале да је њихов прогонитељ нека заиста снажна, моћна и утицајна особа, док заправо претња или узнемиравање могу да долазе од детета које то ради из забаве и није свесно последица које његова "забава" може да изазове.

Бројни аутори су покушавали да доведу у везу различите психичке болести и поремећаје са радњом прогањања.[324] У литератури се помиње тзв. Клерамболтов синдром (Clerambault's syndrome),[325] врста поремећаја понашања слична еротоманији.[326] Овај синдром се у теорији користи да би се објаснило опсесивно и компулзивно понашање особе која искрено верује да је у интимној вези са жртвом.[327] Поборници постојања Клерамболтовог синдрома закључили су да прогањање није последица менталне болести, већ више последица поремећаја понашања, најчешће параноидног поремећаја и суманутих идеја.[328] Постоје такође и прогонитељи који су "вечити усамљеници" који имају проблем са показивањем емоција и очајнички желе пажњу и љубав друге особе,[329] али се проблем јавља када жртва и њен прогонитељ не деле исте емоције или исти однос према међусобној вези.

Релативна анонимност на интернету може да проузрокује недостатак друштвених инхибиција и моралних ограничења, што ће прогонитељима омогућити да лако пронађу своје нове жртве. Немогућност да се саговорник гледа и слуша може да доведе до потпуног отуђења и ограничења друштвене комуникације. Прогонитељ може да се претвара да је нека сасвим друга особа што га ослобађа страха да ће бити откривен, оптужен и кажњен.[330]

Смањењем демотивационих фактора попут стида и страха од одбацивања, интернет може да охрабри појединце да се укључе у дијалог и да

---

[324] McFarlane, Leroy , Bocij, Paul, *op.cit.,* 2005, стр. 11.
[325] По француском психијатру Gaëtan Gatian de Clérambault
[326] Dressing, Harald, Henn, A. Fritz, Gass, Peter: "Stalking behavior - an overview of the problem and a case report of male-to-male stalking during delusional disorder", Psychopathology Vol. 35, No. 5, 2002, стр. 313
[327] *Ibid.*, стр. 314.
[328] *Ibid.*, стр. 314.
[329] Hutton & Haantz (2003) navedeno kod Pittaro, L. Michael, *op.cit.,* 2007, стр. 184.
[330] Bowker & Gray (2004) наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.181.

учине нека дела која би у „реалној" комуникацији ретко кад учинили. Прогонитељ који би у директном контакту био суздржан и оклевао да започне комуникацију са потенцијалном жртвом, у интернет окружењу реагује без оклевања и жртви учестало шаље претеће или узнемирујуће поруке. Он може у тренутку вршења самог чина прогањања да буде и у стању урачунљивости и у стању неурачунљивости, али је веома битно и да ли је извршилац „опасан по околину"[331] тј. да ли постоји високи степен вероватноће да ће извршити конкретно кривично дело према особи коју прогони.

Недостатак инхибиције може да утиче на прогонитеља да се у виртуелној комуникацији лажно представља: није ретка појава да прогонитељ преузме идентитет неког пријатеља или рођака жртве како би прикупио што више информација, или да се чак представља жртвиним именом ширећи неистине.[332] Недостатак личног контакта прогонитеља са жртвом може да доведе до различитих пројекција прогонитеља, због чега жртва може бити изложена одбацивању, понижењу или бесу.[333]

Веза између понашања прогонитеља и осећања жртве може да се прикаже на следећи начин: [334]

Модел понашања	Радње које се предузимају	Последице
Намерно и стално малтретирање, узнемиравање или застрашивање неке особе.	*Задирање некој особи у приватност:* - нежељено присуство или близина (физичка, видокруг или виртуелна). - нежељена комуникација (лична или посредна). - претње (директне или индиректне; усмене или у писаној форми). - комбинација претходно набројаних понашања.	- Озбиљна претња. - Недостатак или мањак осећања сигурности.

[331] Дракић, Драгиша: „Сукоб кривичног права и медицинске етике и психијатријске науке на примеру психијатријског вештачења", Зборник радова Правног факултета у Новом Саду, 2/2012, стр. 202, http://scindeks-clanci.ceon.rs/data/pdf/0550-2179/2012/0550-21791202193D.pdf, претражено 14.01.2016. године

[332] Ellison, Louise, *op.cit.,* 2001, стр.141.

[333] McGrath, Michael, Casey, Eoghan., 2002, стр.86.

[334] Benschop, Albert: "CyberStalking: menaced on the internet", SocioSite-Social & Behavioral Sciences Sociology & Anthropology University of Amsterdam, October, 2003, http://www.sociosite .org/cyberstalking_en.php , претражено 14. 07. 2014. године

г) Типологија жртава и последице интернет прогањања. Сваки корисник Интернета и друштвених мрежа може да постане жртва интернет прогонитеља, али ипак постоје вулнерабилније групе корисника који су у већој опасности од других. То су жене, малолетници и новији интернет корисници.[335] Статистике показују да је највећи број жртава женског пола, а прогонитеља мушког пола,[336] али забележени су и случајеви да су интернет прогонитељ и жртва истог пола.[337] У литератури постоје различити подаци о распрострањености интернет прогањања и жртвама овог облика злоупотребе друштвених мрежа. Истраживања показују да међу жртвама прогањања и интернет прогањања преовлађују особе женског пола: жртве интернет прогањања су 52% женског пола, док је код прогањања овај број је знатно већи 75-80%.[338] Око 80% интернет прогонитеља је мушког пола, колики је и проценат прогонитеља уопште.[339] Највећи проценат жртава и злостављача је узраста од 18 до 24 године. [340] Приликом посматрања родне заступљености у оквиру броја инцидената који су се десили у ранијим партнерским односима прогонитеља и жртве, можемо да закључимо да прогањање уствари представља само наставак насиља у породици и претходног злостављања. На овај начин, прогонтељ покушава да „казни" жртву или да је приволи да се предомисли и да настави окончану везу, при чему прогонитељ верује да ће жртва константно присуство схватити као доказ привржености и оданости.[341]

Интересантно је истраживање које је септембра 2013. године спровела организација за помоћ женама (Women's Aid), чији су резултати указали на повезаност насиља у породици и партнерског насиља са насиљем које се дешава преко интернета.[342] Од испитаних 307 жена жртава породичног насиља, 45% је изјавило да је поред насиља у породици за време трајања емотивне везе преживело и неки од облика насиља и преко друштвених мрежа или

---

[335] Hutton & Haantz 2003, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр.184.
[336] Pittaro, L. Michael, *op.cit.,* 2007, стр.188.
[337] *Ibid.*
[338] *Ibid.*
[339] Yar, Majid, *op.cit.,* 2006, стр. 128.
[340] Corporate Alliance to End Partner Violence - Stalking, http://www.caepv.org/getinfo/facts_stats.php?factsec=9, претражено 06. 03. 2012. године
[341] McGuire, Brian, Wraith, Anita, *op.cit.,* 2000, стр. 318.
[342] Women's Aid conference links online abuse to off-line violence against women, Women's Aid, September 2013, www.womensaid.org.uk/stalking-links, претражено 21. 03. 2015. године

електронске поште, 48% је пријавило да је доживело неку врсту злостављања преко интернета од стране бившег партнера, 38% је пријавило да је било жртва прогањања преко интернета након раскида партнерског односа, 75% је пријавило да полиција није знала како да одреагује на пријављено насиље преко интернета а 12% је чак рекло да полиција након пријављивања интернет насиља није хтела ни да реагује.[343]

Прогањање путем интернета се углавном везује за жене као жртве и за насиље које трпе од стране бившег партнера, па је тако јасна повезаност са партнерским насиљем или насиљем у породици, при чему је прогањање почело још док је веза трајала.[344] Жене које су преживеле насиље у породици су у још већем ризику да постану и жртве прогањања и насиља преко интернета јер насилници знају доста личних информација о њима и знају како и где могу да их „пресретну" и злостављају на интернету.[345] Овако гледано, прогањање и злостављање преко интернета представља само наставак реалног насиља у породици или партнерског насиља.[346]

Према истраживању, које је 2002. године спровела група адвоката заступника жртава сајбер прогањања,[347] 71% свих жртава које су пријавиле насиље су биле женског пола, а 59% њих се познавало са прогонитељем и било у некој вези са њим. За разлику од мушкараца који прогањају преко интернета, жене ређе прогањају непознате људе већ искључиво своје раније партнере или њихове партнерке.[348]

---

[343] *Ibid.*
[344] Mullen E.Paul, Pathe, Michele, Purcell, Rosemary: „Stalkers and their Victims. Cambridge University Press", 2009, https://books.google.rs/books?hl=sr&lr=&id=Kir_ypPb7IQC&oi=fnd&pg=PR11&dq=Mullen,+Pathe+and+Purcell+Stalkers+and+their+Victims&ots=HG0TrlavDC&sig=65ass5vvLW1o5aRWsaL2uW0Qlc8&redir_esc=y#v=onepage&q=Mullen%2C%20Pathe%20and%20Purcell%20Stalkers%20and%20their%20Victims&f=false, претражено 24. 11. 2014. године
[345] Perry, Jennifer: „Digital Stalking: A guide to technology risks for victims", 2012, Women's Aid, National Stalking Service and Nominet Trust, http://www.womensaid.org.uk/core/core_picker/download.asp?id=3492, претражено 17. 09. 2014. године
[346] *Ibid.*
[347] Описано код Hutton & Haantz, 2003, наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр. 184.
[348] Purcell, Pathe, Mullen, 2001 наведено код Pittaro, L. Michael, *op.cit.,* 2007, стр. 184.

Истраживање сајбер прогањања у Србији[349] показало је да су се жртве прогањања у већини случајева биле женског пола (58,4%) и да су се најчешће суочавале са „инсистирањем на нежељеној комуникацији“, „ширењем негативних коментара и гласина“, „слањем заражених фајлова“, „инфилтрирањем и надгледањем рачунарског система“ и др.[350] Ово истраживање је, поред осталог, показало да је као основно средство прогањања коришћен е-маил (62,5%), затим телефон (25%) и програми (сајтови) за социјално умрежавање и е-маил листе. [351]

Постоји податак да ако се годишње широм света пријави око 6.000.000 случајева прогањања, процена је да је око 60% свих дела почињено у виртуалној средини.[352] Такође се процењује да је нпр. у САД једна од 1,250 особа потенцијални прогонитељ као и да су једна од 12 жена и један од 45 мушкараца бар једном у животу били жртве прогањања.[353]

Статистике из јануара 2008. године показују да је током 2005 - 2006. године око 3.4 милиона људи пријавило да су биле жртве прогањања путем интернета; 50% њих је изјавило да је са прогонитељем имало најмање један нежељени контакт недељно, 11% је било злостављано 5 или више година, а једна од седам особа је морала да промени место боравка због прогањања које је трпела.[354] Према истраживањима Алијансе за окончање партнерског насиља (САД), три од четири жртве су познавале свог прогонитеља: у 22% случајева реч је о бившем партнеру жртве а у 16% о пријатељу, цимеру или суседу жртве. Само једна од десет жртава наводи да не познаје свог злостављача, што значи да су најмањем броју случајева, прогонитељи су за жртву апсолутни незнанци.[355] До закључка да је особа која врши прогањање (најчешће мушког пола) је у

[349] Истраживање је спровео Факултет за специјалну едукацију и рехабилитацију. у периоду јун – септембар 2009. године. Подаци о жртвама сајбер прогањања добијени су on line анкетом о виктимизацији 237 испитаника/испитаница.
[350] Ковачевић-Лепојевић, Марина, Лепојевић, Борко: „Жртве сајбер прогањања у Србији”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр.3, година 12, септембар 2009, стр.103
[351] *Ibid.*
[352] Tjapa, Anju, Kumar, Raj, *op.cit.,* 2011, стр. 11
[353] *Ibid.*
[354] Corporate Alliance to End Partner Violence - Stalking, http://www.caepv.org/getinfo/facts_stats.php?factsec=9, претражено 06. 03. 2012. године
[355] *Ibid.*

великом броју случајева остављени, одбијени или бивши партнер жртве, која је најчешће женског пола дошао је и Шпицберг (Spitzberg). [356]

Према интернет истраживању које је спровео Боцић[357] најчешће пријављени облик интернет прогањања је упућивање претњи и насилничко понашање у причаоницама (47,62%), упућивање претњи преко електронске поште (39,88%). Највећи број испитаника који су попунили интернет анкету је из Велике Британије (45,5%), САД (39,9%), Канаде (7,2%) и Аустралије (2,4%).

Студија спроведена међу студенкињама једног колеџа у САД показала је да од 696 пријављених инцидента прогањања 24.7% било прогањање преко електронске поште.[358] Подаци из канцеларије Окружног тужиоца округа Лос Анђелес (САД) 1999. године, када је коришћење информационих технологија било мање заступљено него данас, показују да је 20% од 600 пријављених случајева прогањања било извршено коришћењем електронске поште или дигиталних технологија.[359] Национално истраживање виктимизације прогањањем у САД указало је да само 8% жена и 2% мушкараца пријављују да су били жртве прогањања, од којих је 1% жена и 0.4% мушкараца прогањање пријавило тек након 12 месеци од првог догађаја.[360]

Подаци из Канаде показују да је 8% Канађана пријавило да су били жртве претећих или злостављачких електронских порука,[361] док је сличан проблем пријавило 12% Британаца. [362]

Полицијско одељење за истраживање компјутерског и технолошког криминалитета у Њујорку (The New York Police Department's Computer

---

[356] Spitzberg, 2002, navedno kod Yar, Majid, *op.cit.,* 2006, стр. 124
[357] Наведено код Bocij, Paul, *op.cit.,* 2004, стр.13.
[358] Fisher, B.S., Cullen, F.T. and Turner, M.G.:"Being pursued: Stalking victimization in a national study of college women", Criminology and Public Policy 257, 2002., стр..282, наведено код Clough, Jonathan, *op.cit.,* 2010, стр. 368
[359] US Attorney General, "Stalking and Domestic Violence" , navedeno kod Clough, Jonathan, *op.cit.,* 2010, стр. 368
[360] Tjaden, Patricia, Thoennes, Nancy: "Stalking in America: Findings from the National Violence Against Women Survey", Washington DC, National Institute of Justice and US Departman of Jusice, 1998, стр. 10.
[361] Kowalski, Melanie: "Cyber-Crime: Issues, data sources, and feasibility of collecting police-reported statistic", Cat no. 85-558, Canadian Centre fot Justice Statistic, 2002, стр. 15, http://www.statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf , претражено 01. 11. 2012. године
[362] Wilson, Debbie et al.:"Fraud and Technology Crimes: Findings from the 2003/04", British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources, Home Office Online Report, 2006, стр. 8, http://webarchive.nationalarchives.gov.uk/20110220105210/rds.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf , претражено 04. 11. 2012. године

Investigation and Technology Unit – CITU) свакодневно прима пријаве које се односе на компјутерски криминалитет, најчешће преваре, неовлашћене упаде у компјутерске системе, дечију порнографију и интернет прогањање. Од укупног броја пријава које је ово Одељење примило у периоду од јануара 1996. до августа 2000. године, 42,8% пријава се односило на „тешко злостављање коришћењем компјутера или интернета".[363] Злостављање путем електронске поште било је заступљено у 92% укупног броја случајева, док су остали облици злостављања обухватали злостављање у „причаоницама", различитим форумима или интернет порталима. [364]

Када се узме у обзир број корисника интернета и друштвених мрежа, јасно је да је велики број потенцијалних жртава оваквих кривичних дела. Процењује се да је у САД једна од 1,250 особа потенцијални прогонитељ, да су једна од 12 жена и један од 45 мушкараца бар једном у животу били жртве прогањања.[365]

У Европи, подаци из Британије[366] показују да је 8% жена и 6% мушкараца у Британији било жртва прогањања, што значи 1.2 милиона жена и скоро 900.000 мушкараца на годишњем нивоу.

Као што постоје различити типови интернет прогонитеља, постоје и различити типови жртава које насилници бирају.

Потенцијалне жртве прогањања путем интернета поједини аутори[367] класификују према њиховом претходном односу са прогонитељем и према околностима услед којих којих је мотив прогањања настао. На основу ових критеријума жртве прогањања се могу поделити на:

(1) бивше партнере – жртва је у овом случају најчешће женског пола коју прогања бишши момак, муж или партнер, иако су забележени и случајеви прогањања бивших партнера мушког пола од стране бивше партнерке, али у знатно мањој мери, док су забележени и случајеви прогањања међу партнерима

---

[363] Yar, Majid, *op.cit.,* 2006, стр. 128.
[364] D'Ovidio, Robert, Doyle, James, *op.cit.,* 2003, стр. 12.
[365] Tjapa, Anju, Kumar, Raj: "Cyberstalking: Crime and Challenge at the Cyberspace", International journal of Computing and Business Research, vol.2 issue 1, 2011, стр. 11, http://www.researchmanuscripts.com/PapersVol2N1Jan2011/1.pdf, претражено 02. 03. 2013. године
[366] British Crime Survey, 2003, http://www.usak.org.tr/istanbul/files/bcs25.pdf, претражено 04. 11. 2012. године.
[367] Pathé, Michele, Mullen, Paul E., Purcell, Rosemary: „Management of victims of stalking", 2001, http://apt.rcpsych.org/content/7/6/399.full, претражено 07. 06. 2014. године

истог пола. Ове жртве обично осећају претерану кривицу због лошег избора партнера која је најчешће подржана и подкрепљена од стране најближе околине или професионалаца којима се жртва обрати за помоћ. Ова категорија жртава може да претрпи најшири спектар облика насилничког понашања који траје дугачак временски период, а спадају и у категорију жртава које најчешће претрпе и физичко насиље.

(2) познанике и пријатеље – ово је категорија у којој су жртве најчешће мушког пола, а окидач за настанак прогонитељског понашања је повремени сусрет или виђење жртве и насилника. Период прогањања је релативно кратак и смањена је могућност за настанак било каквог тежег обила насиља.

(3) особе које се баве одређеном професијом, занимањима због којих често долазе у додир са људима који су ментално болесни, проблематични или превише изоловани и/или усамљени су у опасности да буду прогањане од стране потенцијалног насилника који тражи своје уточиште од других проблема (нпр. здравствени радници, адвокати и правници, просветни радници). Прекид професионалне везе која је зближила насилника и жртву може да буде повод за прогањање, које је у домену патологије огорченог или предаторског модела прогонитељског понашања.

(4) колеге и особе из пословног окружења - жртве прогањања из радног окружења су најчешће прогоњене од стране друштвено неприлагођеног колеге или сарадника, бившег колеге који више ту не ради, клијента или корисника услуга. Овај вид прогањања се најчешће јавља када у радним организацијама настану велике организационе промене или после спроведеног дисциплинског поступка против особе која је постала прогонитељ. Прогонитељ сматра да му је нешто одузето или да је ускраћен за неко право, а да је жртва крива за то или да је жртва из целе ситуације извукла неку корист. Овај вид прогањања је веома опасан јер веома често ескалира екстремним насиљем које није ограничено само на примарну жртву већ може да има утицај и на остале људе из окружења жртве.

(5) непознати људи – жртве било ког прогонитеља који се међусобно не познају. Могућност за појаву насиља у оваквом односу релативно мала, немерљиво мања од ризика који постоји када се ради о прогонитељу предатору или насиљу између некадашњих емотивних партнера. Страх и збуњеност постоје код жртве која не може да утврди ко је прогонитељ и разлог прогањања.

(6) медијски познате личности - за ову врсту жртава се најчешће везују прогонитељи који траже интимност, друштвено неприлагођени прогонитељи, озлојеђени прогонитељи и прогонитељи предатори.

(7) лажне жртве прогањања – понекад се дешава да прогонитељи оптуже своју жртву да их она прогања, најчешће као вид освете због пажње коју су желели а нису добили или да би, уколико жртва пријави прогањање, остали и даље у контакту са својом жртвом. Такође, може да се догоди и да некадашња стварна жртва прогањања услед неког безазленог контакта или сусрета са некадашњим прогонитељем поново почне да мисли да је опет жртва прогањања и узнемиравања, због ситуације у којој се налазила и преживљеног страха.

Последице прогањања за жртву могу да буде веома тешке, упркос чињеници да до физичког насиља није дошло. Страх и анксиозност су најчешће и неизоставне реакције, могу да се јаве и поремећаји сна, депресија и самоубилачке мисли. Поједина истраживања су показала да једна трећина жртава због последица прогањања потражи психолошку помоћ, једна петина почне да изостаје са радног места, док 7% жртава не буде у стању да се уопште врати на посао.[368] Жртва је такође „приморана" да свој живот прилагођава ситуацији и да чини све како би избегла прогонитеља: промени број телефона, додатно осигура простор у коме живи и борави, носи са собом средства која могу да послуже за самоодбрану, иде на курс самоодбране, промени ауто, да се пресели, промени посао, промени лични идентитет (име, презиме), чак и да се пресели у неку другу земљу.[369]

Ефекти које прогањање може да има на особу су веома комплексни и изазивају промене у понашању, психичком стању и друштвеном животу жртве. Посебно је велики ризик од губитка осећања личне сигурности, губитак посла, губитак пријатеља, несаница, промена редовних друштвених навика које жртва има.

Постоји више фактора који су препознати као узрочници који доводе до високог нивоа застрашености код жртве.[370] Прогањање није један чин насиља, већ је то чин насиља који се понавља више пута, дуже траје и непредвидљиво је.

---

[368] Tjaden, Patricia: "The crime of stalking: How big is the problem?", National Institute of Justice - Research preview, Washington DC, National Institute of Justice, 1997, стр. 2
[369] McGuire, Brian, Wraith, Anita, *op.cit.,* 2000, стр. 323
[370] Pathé, Michele, Mullen, Paul E., Purcell, Rosemary, *op.cit.,* 2001.

Овакво понашање доводи до страха и развијања осећаја неповерења, што у комбинацији има деструктивне последице за међуљудске односе које жртва има са другим људима. Осећања напуштености и немогућности да се управља својим животом су веома јака, а додатно их може појачати неправилно реаговање од стране надлежних органа када жртва смогне снаге да пријави насиље кроз које пролази.

д) Правна регулатива интернет прогањања. Прогањање путем интернета последњих година привлачи све већу пажњу јер је глобално друштво почело све више да разматра и ствара механизме за решавање проблема различитих врста злостављања и виктимизације уопште. Иако су у теорији заступљена и мишљења да интернет прогањање треба разликовати од „реалног" прогањања, највећи број држава предвиђа само кривично дело прогањања.[371]

Упркос ставу стручне јавности да интернет виктимизација представља озбиљну и све већу претњу друштву данашњице, овај проблем се и даље не сагледава као злочин и кривично дело, већ као својеврсна „друштвена конструкција"[372]. Бројне процене показују да је дело интернет прогањања све озбиљнија и учесталија претња сигурности корисника интернета са све чешћим трагичним последицама за жртве. Интернет преступници злоупотребљавају нове технологије како би стварали нове контакте и друштвене односе и на тај начин прекорачили све границе културе и морала пристојне комуникације.

Мали број држава у свету је својим законодавствима правно регулисало прогањања преко интернета као кривично дело и углавним је реч о законодавству англосаксонског права.

У Сједињеним Америчким Државама интернет прогањање је регулисано најпре националним законима у државама Калифорнија (1999. године), Тексас (2001. године) и Флорида (2003. године).[373] Данас у САД један део држава је правно регулисао питање прогањања преко интернета кроз забрану злостављања коришћењем електронске, компјутерске или e-mail комуникације (Алабама, Аризона, Конектикат, Хавај, Илиноис, Њујорк...).[374] Поједине

[371] Clough, Jonathan, *op.cit.,* 2010, стр. 369
[372] Yar, Majid, *op.cit.,* 2006, стр.133
[373] My Space, http://www.myspace.com/johnhollywoodpierce/blog/546361330, претражено 16. 01. 2015. године
[374] *Ibid.*

државе предвиделе су интернет прогањање као кривично дело (Аљаска, Флорида, Оклахома, Вајоминг, Калифорнија).[375] У држави Тексас 2001. године донет је закон којим је санкционисано прогањање путем средстава електронске комуникације (Stalking by Electronic Communications Act, 2001.), а 2012.године у оквиру посебне главе у Кривичном закону предвиђено је злостављање и прогањање путем интернета као кривично дело (Penal Code - Chapter 33, Section 33.07: An act relating to the creation of the offense of online harassment).[376] У САД поред бројних националних закона који се односе на правно регулисање интернет прогањања, 2000. године измене и допуне федералног закона који се односи на насиље према женама (Violence Against Women Act of 1994.) такође предвиђају санкционисања интернет прогањања.[377]

Кривични закон Аустралије донет 1999. године допуњен је актом којим је забрањено прогањање преко интернета (Criminal Code Stalking Amendment Act 1999),[378] У Великој Британији је 1988. године донет Закон о злонамерним комуникацијама (Malicious Communications Act), у чијим је изменама и допунама из 2003. године прогањање преко интернета прописано као кривично дело (чл. 127). [379]

У Европи је неколико земаља је прописало и санкционисало интернет прогањање као кривично дело.

Пољска је 2011. године у изменама и допунама Кривичног закона из 1997. године (чл. 190а)[380] предвидела кривично дело прогањање путем интернета. Интернет прогањање је дефинисано као забрана упорног узнемиравања неке особе коришћењем интернет или телефонских веза које

---

[375] *Ibid.*

[376] WHOA- Working to Halt Online Abuse, http://www.haltabuse.org/resources/laws/texas.shtml, претражено 16. 01. 2015. године

[377] Sacco, N. Lisa: "The Violence Against Women Act: Overview, Legislation, and Federal Funding", https://fas.org/sgp/crs/misc/R42499.pdf, претражено 16. 01. 2015. године

[378] CRIMINAL CODE (STALKING) AMENDMENT ACT 1999 - Act No. 18 of 1999, https://www.legislation.qld.gov.au/LEGISLTN/ACTS/1999/99AC018.pdf, претражено 16. 01. 2015. године

[379] Закон о злонамерним комуникацијама Велике Британије (The Malicious Communications Act), 1988. са изменама и допунама из 2003. године, http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf, претражено 14. 01. 2015. године

[380] Кривични закон Републике Пољске (Kodeks karny), 1997 са изменама и допунама из 2011. године, http://www.legislationline.org/download/action/download/id/4286/file/POLAND_CC_am2012_%20PL.pdf претражено 16. 01. 2015. године

резултује осећањем несигурности и угрожене приватности узнемираване особе. Прописана казна за основни облик овог кривичног дела је казна затвора до три године, а уколико извршење дела доведе до самоубиства узнемираване особе прописана је казна затвора до десет година. Према одредбама закона, кривично дело се не гони по службеној дужности, већ по захтеву оштећеног. [381]

Кривични закон Краљевине Шпаније из 1995. године са изменама и допунама из 2011. године (чл. 183)[382] као кривично дело прописује и санкционише једино узнемиравање лица млађих од тринаест година. Кривично дело постоји када нека особа посредством интернета, телефона или коришћењем информационих и комуникационих технологија контактира лице млађе од 13 година и понуди му да се са њим уживо нађе, а затим изврши било које кривично дело из групе дела против полне слободе.

У Кривичном законику Републике Србије дела прогањања и прогањања преко интернета нису предвиђена као посебна кривична дела. Уколико дође до ових криминалних понашања, могуће их је квалификовати у оквиру постојећег кривичног дела класичног криминалитета као што је угрожавање сигурности (чл. 138) уколико је угрожена сигурност неког лица претњом да ће се напасти живот или тело тог или њему блиског лица. Међутим, највише случајева прогањања путем интернета врши се упорним слањем узнемиравајућих порука које у себи не морају да садрже отворено изражену претњу због чега се не могу квалификовати као кривично дело угрожавање сигурности. С обзиром на распрострањеност ове појаве и на законску нерегулисност, неопходно је да се у Кривичном законику предвиди интернет прогањање као посебно кривично дело у оквиру кога би се тачно прецизирале радње извршења и санкционисало такво понашање.[383]

---

[381] Kosiński, Jerzy: „Cybercrime in Poland“, http://www.academia.edu/3878063/Cybercrime_in_Poland, претражено 16. 01. 2015. године

[382] Кривични закон Краљевине Шпаније, 1995. са изменама и допунама из 2012. године, http://www.legislationline.org/download/action/download/id/5160/file/Spain_Criminal_Code_Codigo_Penal.pdf, претражено 18. 01. 2015. године

[383] С обзиром на то да су жене најчешће жртве прогањања, организације „Аутономни женски покрет” и „Мрежа жене против насиља” затражиле су априла 2015. да се дело прогањања уведе у Кривични законик и поновиле захтев за додатну заштиту жртава партнерског и насиља у породици. У саопштењу су подсетиле да је Србија 2013. године ратификовала Конвенцију Савета Европе о спречавању и борби против насиља над женама и насиља у породици која захтева да се прогањање пропише као кривично дело. Те организације сматрају да држава треба да пропише обавезу професионалаца који поступају у случајевима партнерског и насиља у

ђ) Облици заштите од интернет прогањања. Облици заштите од интернет прогањања обухватају личне превентивне стратегије, законодавну регулативу и решења за превазилажење техничких мана друштвених мрежа. Тјапа и Кумар[384] су на основу спроведених истраживања закључили да постоји неколико универзалних метода за одбрану од интернет прогонитеља:

(1) малолетне особе које су жртве интернет прогањања морају да о насиљу које су доживеле поразговарају са родитељима или са неком одраслом особом у коју имају поверења;

(2) у случајевима када жртва зна ко је њен прогонитељ, неопходно је да му упути писмену опомену у којој ће назначити да је контакт нежељен и да жели да прекине даљу комуникацију у сваком смислу; жртва овакво упозорење треба да пошаље само један пут и да ни по коју цену након тога не комуницира са насилником;

(3) жртва мора да има сачуване све трагове комуникације са прогонитељем у електронском и штампаном облику јер све то може да буде доказ уколико је насилник упоран па жртва мора да потражи заштиту полиције или суда;

(4) о сваком облику интернет прогањања жртва треба да обавести свог интернет провајдера јер многи провајдери и сервиси имају могућност „филтрирања" тј. забране или селекције комуникације са одређеним особама или блокирање одређених садржаја;

(5) жртва може да води дневник у коме ће назначити датум сваке комуникације са прогонитељем, претње које јој се стављају у изглед, да бележи емоције које осећа због претњи и како оне утичу на свакодневни живот и односе са породицом и најближом околином, као и мере које је предузела да би спречила свог прогонитеља да настави са насиљем;

6) жртва треба да поднесе пријаву најближој полицијској станици или надлежном суду, како би видела да ли од ових органа може да обезбеди одговарајућу заштиту;

(7) без обзира на предузимање одговарајућих мера од стране државних органа, сама жртва треба да размисли о промени интернет провајдера, адресе електронске поште, броја телефона уколико је интернет повезан са њим, о коришћењу нових и сигурнијих сервиса као и о инсталирању програма који омогућавају енкрипцију садржаја или бољу заштиту приватности.

породици да процењују ризик од понављања насиља и од наступања смртне последице. *Видети:* Нови магазин од 21. 04. 2015. године, http://www.novimagazin.rs/vesti/nvo-proganjanje-treba-da-bude-krivicno-delo, претражено 22. 10. 2015. године

[384] Tjapa, Anju, Kumar, Raj, *op.cit.,* 2011, стр.8

У литератури се наводе пожељна понашања корисника интернета као облици заштите од прогањања преко интернета.[385] То су:

- веровање својим инстинктима, што значи да се на први осећај нелагодности или непријатељске комуникације излогује из сајбер простора или блокира приступ свом профилу за особу која прети или застрашује;

- процена да ли би престанку даљег узнемиравања допринело стављање до знања особи која узнемирава да се прекида сваки контакт и да ће следеће узнемиравање бити пријављено полицији/тужилаштву;

- чување целокупне документације о комуникацији са прогонитељем као доказ, при чему треба користити print screen опцију;

- чување документације о комуникацији са администраторима друштвене мреже или са представницима полиције или тужилаштва, ако пријави прогонитеља надлежним институцијама;

- блокирање или филтрирање порука које стижу од прогонитеља;

- подношење жалбе администратору друштвене мреже уколико прогонитељ ставља о њему/њој злонамерне садржаје на друге интернет странице или друштвене мреже, као и да тражење блокирања ИП адреса прогонитеља, уклањање злонамерних објава и упозоравање прогонитеља да прекине са таквим понашањем;

- саопштавање својим пријатељима и породици о прогањању.

Ово су само неки од облика заштите од прогањања путем интернета. Како је интернет у савременом друштву постао неодвојиви свакодневни део живота великог броја људи, није решење једноставно искључити компјутере: интернет корисници морају да науче како сами себе да заштите од свих врста потенцијално опасних понашања на интернету јер је досадашња пракса показала да свако ко користи интернет може да постане жртва.

Забележен је и случај апсолвента са Универзитета у Сан Дијегу, САД, који је током целе године малтретирао и преко интернета прогањао својих пет колегиница тако што им је слао стотине насилних и претећих електронских порука. (Benschop, Albert, op.cit., 2003) Интересантна је чињеница да се овај младић никада заправо није лично сусрео са женама које је малтретирао, што доказује да у случају прогањања преко интернета није потребно да постоји било каква лична веза између жртве и прогонитеља, као и да је могуће да један прогонитељ у исто време малтретира више жртава.

[385] Колико сам безбедна? – безбедоносне препоруке за жене и девојке, Аутономни женски центар, Организација за европску безбедност и сарадњу – мисија у Србији, 2015, стр. 18-22

Америчка глумица Патриша Аркет (Patricia Arquette) била је приморана да угаси свој званични Facebook профил након што је објавила да је прогањана преко налога на овој друштвеној мрежи. Цео проблем је почео када је направљен експеримент да се познате личности преко друштвене мреже зближавају и упознају са осталим корисницима, како би им показали да су исти као и сви људи. После негативног искуства које је имала са једном од корисница друштвене мреже која је почела да је прогања, глумица је свима поручила да никако не ступају у контакте са непознатим људима путем друштвених мрежа и да не прихватају захтеве за пријатељство од особа које заправо не познају. (Patricia Arquette quits Facebook after alleged cyberstalking, http://www.digitalspy.co.uk/showbiz/news/a344419/patricia-arquette-quits-facebook-after-alleged-cyberstalking.html, претражено 28. 10. 2011. године)

Интересантан је случај који се 1999. године догодио у Сједињеним Америчким Државама. Лајам Јуенс (21) контактирао је интернет детективску агенцију за истраживања и пружање информација (под именом Docusearch) да ли могу да му пронађу датум рођења Еми Лин Бојер (20) којом је био опседнут још од када су пошли у средњу школу. (Наведено код Pittaro, L. Michael, op.cit., 2007, Electronic Privacy Information Center: "The Amy Boyer case", 2006, Electronic Privacy Information Center Web site http://www.epic.org/privacy/boyer/ , претражено 06.03.2015.године) Како ова потрага није уродила плодом, јер ниједна од пронађених особа са овим именом и презименом није била она коју је Јуенс тражио, он је почео да тражи број њеног социјалног осигурања и податке о месту где Бојерова ради. За ту сврху је овој агенцији платио скоро 200 долара, а једна од запослених у агенцији је звала све пронађене жене које су могле да буду „тражена" Еми Лин Бојер док коначно није пронашла адресу послодавца код кога је Бојерова радила. Октобра 1999. године Јуенс се са пиштољем упутио ка стоматолошкој ординацији у којој је Еми Лин Бојер радила, сачекао је да заврши са послом и пуцао у њу једанаест пута усмртивши је, након чега је извршио самоубиство. Тек касније, када је вођена истрага, откривено је да је Јуенс док је покушавао да пронађе Бојерову две године пре убиства направио и одржавао интернет сајт назван *Amy Boyer* (Net Crimes, http://www.netcrimes.net/Amy%20Lynn%20Boyer_files/liamsite.htm, претражено 27. 11. 2014. године), на коме је експлицитно објавио све детаље везане за његову потрагу за њом, за то како је покушавао годинама да јој уђе у траг и да је прати, за све шта је осећао према њој и како је планирао да је убије. (Spencer, 2000 наведено код Electronic Privacy Information Center: "The Amy Boyer case", 2006) На овом сајту Јуенс је објаснио како се заљубио у Бојерову док су још били у осмом разреду, како га је она одбијала када су кренули у средњу школу, а затим, као реакцију на одбијање, и његов образложени план зашто и како Бојерова мора да умре: *„Када изађе из ординације и уђе у свој ауто, ја ћу се довести до њених кола и блокирати јој пут тако што ћу да паркирам мој прозор уз њен, а затим ћу да извучем мој пиштољ и да је упуцам"*. (*Ibid.)* Управо овако се и догодило. Јуенс је планирао да убије и целу породицу Бојерове, али је очигледно променио план описан на сајту који је направио и у афекту извршио самоубиство.

Када је истрага отпочета и постојање сајта откривено, поставило се и питање како је могуће да су Јуенсове намере да почини овакав стравичан злочин могле да прођу незапажено и како нико на њих није реаговао? Како се у току поступка показало, важећи закони су заправо немоћни у виртуелном свету интернета када се интернет прогонитељи не налазе у истој држави где и жртва, а посебно када се ради о претњама а до физичког контакта није ни дошло. Поред поступка због убиства Бојерове, покренут је још један судски поступак: родитељи убијене су тужили интернет детективску агенцију којој се Јуенс обратио, због одавања личних података о сада покојној Еми Лин Бојер и грубог кршење приватности. (Случај Resmburg v. Docusearch, http://caselaw.findlaw.com/nh-supreme-court/1132429.html, претражено 27. 11. 2014. године)

3.1.3. Сексуално насиље – појам и појавни облици

Сексуално насиље путем интернета и друштвених мрежа представља један од облика злостављање када се интернет, друштвене мрежа или неки други електронски начин комуникације користи за испољавање насилног, малтретирајућег и нежељеног понашање било од стране једне особе или од стране групе.[386] Узнемиравање путем интернета може да има различите облике, почев од слања порука или фотографија путем интернета и/или мобилног телефона које имају за циљ да неког повреде, узнемире или на било који други начин код неке особе створе осећај нелагодности, упућивањем претећих порука, сексуалног насиља, подстицања на групну мржњу, нападе на приватност, вређање, несавестан приступ штетним садржајима, ширење насилних и увредљивих коментара и сл.

Најчешћи облик сексуалног насиља ван виртуелног света је сексуално узнемиравање, које, према класификацији коју је дао Тил (Till)[387] може да се испољи као родно засновано насиље, нежељена сексуална пажња и сексуално задовољење.

Сексуално узнемиравање представља широко распрострањени друштвени феномен који се јавља у свакодневним комуникацијама. Највећи број жртва ове врсте узнемиравања су жене,[388] затим мушкарци, хомосексуалци и деца. Најшире посматрано, сексуално узнемиравање представља насилнички чин усмерен против особе, који подразумева различита понашања од сексистичке дискриминације до сексуалне агресије.[389] *Родно засновано насиље* подразумева непожељне вербалне и визуелне коментаре и примедбе које вређају појединца на основу пола/рода или који има за циљ да изазове негативне емоције (нпр. постављање порнографских слика у јавности или на местима где се то сматра увредљивим, причање шовинистичких вицева, примедбе које су родно деградирајуће и сл.). *Нежељена сексуална пажња* односи се на

---

[386] Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking, Women's Aid Federation of England, 2014, www.womensaid.org.uk, претражено 08. 01. 2015. године
[387] Till, 1980, према Barak, Azy, *op.cit.,* 2005, стр. 78
[388] Gruber, 1997; Paludi & Paludi, 2003 према Barak, Azy: "Sexual harrasmet on Internet", Social Science Computer Review, Vol. 23 No. 1, 2005, стр. 77, http://construct.haifa.ac.il/~azy/SexualHarassmentBarak.pdf, претражено 09. 02. 2014. године
[389] Дефиниција дата у публикацији „Жене за живот без насиља: приручник за волонтерке СОС телефона", Београд: Буфала Бил, 2. издање, 1999, стр. 230

понашање које је нежељено и за које не постоји повод, а којим се експлицитно исказују сексуалне жеље или намере усмерене ка некој особи (нпр. сексуално експлицитни коментари и понашања, зурење у делове тела друге особе итд.). *Сексуално задовољење* подразумева вршење физичког и/или психичког притиска на неку особу како би се она натерала на „сексуалну сарадњу“ (нпр. нежељено физичко додиривање, нуђење новца за нежељени сексуални однос, претња у циљу остваривања сексуалног односа и сл.).

Све три врсте сексуалног узнемиравања које постоје у реалном свету постоје и у сајбер простору, али се, због виртуелне природе сајбер простора, већина узнемиравања изражава у облику родно заснованог злостављања и нежељене сексуалне пажње. Сексуално задовољење ретко постоји у сајбер простору, услед немогућности физичког контакта.

Узнемиравање и сексуално 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. Ова врста узнемиравања може да подразумева и слање претњи силовањем, фотографија жена које су задављене, објављивањем адреса кућа у којима жене живе саме. Скривена порука која се жаље милионима корисника интернета представља у ствари позив на нежељену комуникацију и на напад. Поједини аутори[390]сексуално насиље на интернету деле на следеће облике:

Родно засновано злостављање у сајбер простору представља веома честу појаву која може да се манифестује кроз различита понашања – кроз активне или пасивне вербалне облике злостављања или активне или пасивне графичке облике злостављања.

(1) *Активно вербално сексуално узнемиравање* се углавном манифестује кроз слање увредљивих порука сексуалног карактера (нпр.родно деградирајући коментари, сексуалне опаске, причање безобразних шала и сл.). Овакво понашање се сматра узнемиравањем јер је понижавајуће за жртву. Најчешће се јавља у причаоницама и форумима на друштвеним мрежама, али и кроз приватну електронску комуникацију.

[390] Adam, 2001; Deirmenjian, 1999; Griffith, Rogers, & Sparrow, 1998; Spitzberg & Hoobler, 2002 према Barak, Azy, *op.cit.,* 2005, стр. 80

(2) *Пасивно вербално сексуално узнемиравање* може да изгледа мање наметљиво, јер се особа која се сматра злостављачем не обраћа директно једној или више особа, већ својим надимком или корисничким именом може да вређа јавни ред или морал једног друштва.

(3) *Активно графичко сексуално родно засновано узнемиравање* подразумева намерно слање еротских или порнографских садржаја путем електронских комуникација (нпр. електронска пошта) или њихово објављивање на друштвеној мрежи или у виртуелном простору. Ови садржаји, у зависности од нивоа експлицитности и сензибилисаности жртве могу да се сматрају мање или више увредљиви.

(4) *Пасивно графичко сексуално родно засновано узнемиравање* углавном подразумева објављивање слика или видео снимака увредљивог садржаја на различите интернет портале, на којима жртва и не претпоставља да овакви садржаји могу да се налазе (нпр. аутоматско отварање тзв. pop-up „прозора“ са директним линковима са порнографским садржајима).

Степен јачине било ког од ова четири облика сексуалног узнемиравања је могуће одредити на основу следећа два фактора: (1) природа вербалног или графичког стимулуса посматрана кроз његову експлицитност и степен понављања и (2) лично ставови жртве, осетљивост и персонални начин комуникације. Комбинација ова два фактора одређује субјективни доживљај јачине сексуалног узнемиравања које особа трпи.

Нежељена сексуална пажња у сајбер простору обично подразумева непосредну, личну, вербалну комуникацију између злостављача и жртве, а манифестује се кроз поруке о којима се директно помиње секс или сексуалност (нпр. поруке које се односе на полне органе жртве, њен сексуални живот, њене интимне садржаје и сл.); као и на инсинуације или провокације сличне природе. За разлику од родно заснованог насиља, нежељена сексуална пажња има за циљ да доведе до извесног сексуалног контакта између злостављача и жртве, било у виртуелном или у личном контакту. Суштина је да је овакав контакт за жртву насилан, тј. да га жртва не жели. Оваква дела у сајбер простору се најчешће дешавају преко друштвених мрежа, јавних форума или у причаоницама, али и у приватним електронским комуникацијама између злостављача и жртве. Мотив злостављача јесте да са жртвом првенствено успостави неку врсту сексуалне

повезаности, али мотив такође може да буде наношење емотивне патње жртви, намерно злостављање и сл.

Сексуална принуда преко интернета подразумева употребу различитих средстава доступних на друштвеној мрежи или интернету уопште у циљу успостављања сексуалног контакта са жртвом која овај акт сматра нежељеним и насилним. Иако је коришћење физичке принуде у виртуелном простору немогуће, жртва може да претње које добија схвати као реалистичну физичку принуду. Експлицитне претње могу да буду извор велике забринутости за жртву. Многи аутори сматрају да је овај вид сексуалног узнемиравања најсличнији прогањању путем интернета и да неретко може да прерасте у овај облик злостављања.

Сексуално насиље на интернету и путем друштвених мрежа може да се јави као ***порнографија из освете,*** која представља поступак јавног објављивања сексуално експлицитних фотографија или видео снимака на Интернету, посебно на порнографским интернет страницама, без сагласности особе која се налази на њима, са циљем да се она осрамоти и понизи.[391] Сви материјали који се објављују обележавају се пуним именом и презименом жртве, а често садрже и број телефона, радно место или име под којим је жртва регистрована на некој од друштвених мрежа. Снимљени материјали се постављају на сајтове бесплатно, али је веома честа појава да њихови власници покушавају да уцене жртву тражећи јој да плати одређени новчани износ како материјале не би објавили. Статистике показују да је 90% жртава женског пола.[392] Снимци настају на различите начине: тако што жртва у току трајања љубавне везе насилнику сама пошаље неки снимак, партнер тајно прави снимке без сагласности оног другог, снимке праве непознате особе или се снимци „краду“ неовлашћеним упадом у рачунаре или мобилне телефоне.

Ризично понашање за сексуално насиље путим интернета и друштвених мрежа је секстинг (размењивање кратких порука и/или фотографија врло интимне или експлицитно сексуалне садржине путем chat сервиса, слање провокативних или сексуално обојених фотографија, порука или видео

[391] Кликни безбедно, http://kliknibezbedno.rs/sr/ pornografija-iz-osvete.1.118.html , претражено 15. 07. 2015. године
[392] *Ibid.*

материјала путем мобилног телефона или постављања на мрежу[393]) и сајберсекс (симулација сексуалних односа на даљину путем информационо-комуникационих технологија) због тога што се губи контрола над послатим материјалом и одлукама. То значи да сексуално експлицитан материјал постаје потенцијално свакоме видљив, да тај материјал може опстати вечно и да не постоји могућност да се спречи његово растурање, стављање на порнографске вебсајтове или друге врсте злоупотребе.[394]

Једна од најпознатијих жртава програма Blackshades је и америчка тинејџерска мис Кесиди Вулф, која је прошле године, захваљујући томе што је нападач Џеред Џејмс Абрахамс (20) користио овај алат, била месецима снимана, а нападач је забележио и тренутке док се пресвлачила у својој спаваћој соби. Абрахамс је марта 2014. године осуђен на казну затвора у трајању од 18 месеци, због вршења кривичних дела неовлашћеног упада у рачунарске системе и изнуда. Према наводима тужилаштва Калифорније, Абрахамс је хаковао рачунаре жена које је лично познавао али и жена које је пронашао на друштвеној мрежи Facebook; претпоставља се да је за 2 године узимао податке са око 150 корисничких налога. Када би злонамерним софтвером преузео контролу над компјутером жртве, Абрахамс је могао да даљински укључи веб камеру и слика жртву док се пресвлачи, а да то жртва ни не слути. Затим је фотографије које би на овај начин направио користио је да би уцењивао своје жртве претећи им да ће компромитујуће фотографије или видео снимке објавити на друштвеним мрежама ако му не пошаљу своје још интимније фотографије и видео снимке или ако не пристану на петоминутни разговор преко Скајпа (Skype) са њим током кога ће морати даураде све што им нареди. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Haker-koji-je-ucenjivao-americku-Miss-Teen-i-druge-zene-osudjen-na-18-meseci-zatvora.html, претражено 26. 01. 2015. године)

1998. године педесетогодишњи радник у обезбеђењу Гери Делапента из Калифорније, САД, и двадесетосмогодишња Бренди Барбер су имали кратку емотивну везу. Када је Барберова после пар месеци желела да прекине ову везу, Делапента је почео да јој прети најпре слањем претећих порука преко електронске поште, да би затим на интернету у причаоницама и форумима почео да се представља као њен бивши љубавник који свима открива да је Барберовој највећа фантазија да буде силована, остављајући написан њен број телефона, кућну адресу па чак и савет како да јој се уђе у кућу а да се аларм не активира. Делапента је због оваквог понашања ухапшен и осуђен на шест година затвора, по основу тада у Америци новоуведеног кривичног дела прогањања преко интернета. (Видети: Benschop, Albert, *op.cit.,* 2003)

[393] Приручник за заштиту деце и младих од сајбер насиља и примену у редовном наставном програму основних и средњих школа - "Tagged", Инцест траума центар Београд, стр. 12, http://kliknibezbedno.rs/files/materijali/ITC%20-%20Tagged%20Manual%202013.pdf, претражено 01. 10. 2015. године

[394] *Ibid.*

Користећи лажно име и лажну адресу електронске поште, Роберт Харви Александер, ђакон у једној од цркава на Флориди, користио је компјутерске терминале у локалној библиотеци како би претио женама да ће им уништити углед објављивањем различитих неистина на друштвеним мрежама, уколико не прихвате да са њим имају сексуалну конверзацију преко интернета и телефона. (McGrath, Michael, Casey, Eoghan, 2002.) Александер је на својој „листи жртава“ имао преко сто имена и електронских адреса људи које је малтретирао на овај начин. Користећи трагове о послатим имејловима и о телефонским позивима, Федерални истражни биро (ФБИ) је успео да лоцира где се Александер налази и да га ухапси. Александер је процесуиран и оптужен по постојећем кривичном закону за врсту кривичног дела уцене и клевете. (Cyber-extortion results in prison sentence - Net4TV Voice News Staff, http://www.reformation.com/CSA/RobertHarveyAlexander2.htm, претражено 24. 03. 2015. године)

3.1.4. Сексуална експлоатација и сексуално злостављање деце

а) Појам и распрострањеност. Сексуална експлоатација деце преко интернета је облик сексуалног насиља преко интернета о коме се у медијима најчешће прича и указује на његове страшне последице. Све чешће се слуша о сексуалном злостављању деце које се дешава уживо преко интернета коришћењем друштвених мрежа или ћаскаоница, док се истовремено у медије као опомена друштву пласира чињеница да на друштвеним мрежама и интернету уопште „библиотека” дечије порнографије броји више од 750.000 експлицитних слика.[395]

Деца у данашње време савремене технике и електронског доба велики део времена од најранијег узраста проводе испред рачунара и на интернету, који им, поред бројних забавних и едукативних садржаја, „нуди” и низ опасности које су сакривене у бројним начинима за социјализацију и дружење које у почетку не буде никакву сумњу. Неке од највећих опасности по децу које вребају на интернету су садржаји које на интернет може да постави било која особа и који је немогуће одредити као истинит или лажан; лако је лажно се представити као неко други; постоји много нежељеног садржаја попут насиља, порнографије, говора мржње и сл. и постојање мноштва злонамерних

[395] O’Leary, J.Robert, D’Ovidio, Robert: “Online sexual exploitation of children”, The International Association of Computer Investigative Specialists, 2007, http://www.nga.org/files/live/sites/NGA/files/pdf/0703ONLINECHILD.PDF, претражено 27. 03. 2015. године

компјутерских програма.[396] За децу и младе постоји посебна опасност од неконтролисаног коришћења интернета јер на овај начин деца ступају у комуникацију са одраслим особама које траже непримерене односе са сексуалним намерама.[397]

Сексуално злостављање деце преко интернета подразумева било какав сексуално оријентисани контакт преко интернета, производњу, прикупљање и дистрибуцију дечје порнографије; нежељено излагање деце порнографији; сексуални туризам који се односи циљано на децу и дечију проституцију.[398] Овај вид насиља подразумева сваку врсту интернет експлоатације деце која на директан или индиректан начин доводи до сексуалног контакта између одраслих и деце.[399] Овакав вид експлоатације се најчешће догађа од стране трећих лица, која се користе савременим рачунарским системима и сексуалну експлоатацију деце врше ширењем оваквих садржаја путем затворених форума на интернет страницама.[400]

Подаци Националног центра за несталу и злостављану децу[401] показују да је једно од седморо деце старости од 10 до 17 година било жртва нежељене сексуално експлицитне комуникације и сексуалног злостављања преко интернета.[402] Ову чињеницу потврђују и званичне светске статистике. [403]

---

[396] Протрка, Никола, Грубер, Кристијан, Салопек, Данко: „Сувремени начини пријављивања искоришћавања или злостављања дјеце путем интернета“, 4th International Scientific and Professional Conference „Police College Research Days in Zagreb“, 2015, стр 648, http://www.researchgate.net/profile/Nikola_Protrka/publication/275519088_Suvremeni_naini_prijavljivanja_iskoritavanja_ili_zlostavljanja_djece_putem_interneta__Modern_methods_of_reporting_exploitation_or_abuse_of_children_via_the_Internet/links/553e20640cf2522f1835ee79, претражено 23. 08. 2015. године

[397] Протрка, Никола, Грубер, Кристијан, Салопек, Данко, *op.cit.,* 2015, str. 651

[398] O'Leary, J.Robert, D'Ovidio, Robert, *op.cit.,* 2007.

[399] *Ibid.*

[400] Јокић, Мирела: "Дјечија порнографија као облик насиља над дјецом и високотехнолошког криминала", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., с. 297, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[401] National Center for Missing and Exploited Children, http://www.missingkids.com/home, претражено 10. 05. 2014. године

[402] Wolak, Janis, Mitchell, Kimberly, Finkelhor, David: "Online Victimization of Youth: Five Years Later", Washington, DC: National Center for Missing & Exploited Children, 2006, http://www.unh.edu/ccrc/pdf/CV138.pdf, претражено 27. 03. 2015. године

[403] D'Ovidio, Robert, Doyle, James, *op.cit.,* 2003, стр. 11; Wolak, Janis, Mitchell, Kimberly, Finkelhor, David:"Internet Crimes Against Minors: The Response of Law Enforcement", Washington, DC: National Center for Missing & Exploited Children, 2003, https://www.ncjrs.gov/App/abstractdb/AbstractDBDetails.aspx?id=202909, претражено 23. 03. 2015. године

Мамац за остваривање контаката са децом се обично налази у различитим форумима, ћаскањима, порукама, апликацијама, игрицама. Насилници често контакт почињу са пријатном причом без имало сексуалне конотације, јер је у тој почетној фази остваривања контакта најбитније да жртва стекне поверење у насилника. Најчешће теме о којима се прича преко друштвених мрежа су оне најопштије: шта ко воли, не воли, са ким се дружи, где се креће. Временом како су контакти учесталији и приче почињу да постепено добијају сексуални призвук, веома често насилник почиње жртви да шаље различите порнографске садржаје и да захтева да му жртва шаље своје фотографије.

Када осети да ужива потпуно поверење жртве, насилник ће тежити да развије и физичку везу са жртвом: слаће јој поклоне, инсистираће да се уживо сретну, зваће је телефоном. Према подацима из истраживања Националног центра за несталу и злостављану децу из 2005.године[404] 23% деце и младих су приликом физичког сусрета са насилником били жртве нежељених захтева сексуалне природе, што управо подржава чињеницу да је сваки физички сусрет жртве и насилника заправо веома опасан.

Министарство унутрашњих послова Републике Хрватске је 2012. године заједно са интернет порталом *www.net.hr* спровео „Истраживање о навикама и искуствима деце и младих приликом кориштења Интернета, мобитела и других сувремених технологија" под називом „Заштитимо дјецу на Интернету".[405] Узорак је био састављен од 2.700 ученика основних и средњих школа. Укупно 49% испитане деце користило је Интернет сваки дан без надзора одраслих. Око 800 ученика и ученица (41%) је добило неко интимно питање о себи, а од овог броја 39% је пријавило да је од њих затражено да се сликају или снимају на сексуално провокативан начин. Од наведеног броја, 6% је признало да је то и урадило и слику послало непознатој особи, а 31% је добио слику наге непознате особе коју су знали само преко Интернета. 14% испитаника је отишло на сусрет

[404] Wolak, Janis, Mitchell, Kimberly, Finkelhor, David, *op.cit.,* 2006.
[405] Министарство унутрашњих послова Републике Хрватске, http://www.mup.hr/UserDocsImages/topvijesti/2012/lipanj/Zastitimo%20djecu%20na%20internetu.pdf , претражено 28. 09. 2015. године

са особом коју су упознали преко интернета, а од њих, 37% је на састанак отишло без икога.[406]

б) Појавни облици. Сексуално злостављање деце путем интернета може да има различите облике. Најчешће се јављају: *дечија порнографија*, *сексуални туризам који се односи циљано на децу и дечија проституција*, *сексуални туризам који се односи циљано на децу и дечија проституција и груминг (engl.Grooming).*

Дечија порнографија подразумева визуелну, чак и компјутерски генерисану представу „детета у било каквим реалним или симулираним експлицитним сексуалним активностима или било какву сексуалну конотацију било ког дела тела детета за коју је јасно да је у сексуалне сврхе".[407] Људи који преко интернета дистрибуирају дечију порнографију се преко интернета и рекламирају, чиме је круг људи којима нуде своју „робу" веома широк и представља велику опасност за децу која су активно на интернету. Дечију порнографију је могуће учитати и снимити на рачунар, чиме је она учињена много доступнијом, а њено набављање много сигурније и брже него што је то било некада при чему се не открива идентитет ниједног гледаоца. Порнографски садржаји са децом се размењују преко различитих група на друштвеним мрежама, електронском поштом, у ћаскањима, али и на посебним интернет сајтовима који се баве дечијом порнографијом. Поједине друштвене мреже су дозвољавале дистрибутерима дечије порнографије да формирају различите групе како би размењивали своје садржаје, што је изазивало оштру осуду јавности.[408]

Излагање детета порнографским садржајима против његове воље често се јавља приликом коришћења интернета јер су порнографски садржаји преко интернета доступни свима, без обзира на године старости. Деца веома често не тражећи овакве садржаје наилазе на њих, јер већина безопасних претраживања интернета може путем тзв. искачућих прозора (енгл. pop-up) да преусмери на

---

[406] *Ibid.*
[407] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2002., United Nations Secretariat - Office of the United Nations High Commissioner for Human Rights, http://www.ohchr.org/english/law/crc-sale.htm, претражено 15. 11. 2014. године
[408] Brazilian Prosecutors Seek to Sue Google, MSNBC, 2006, http://msnbc.msn.com/id/14622759/, претражено 12. 09. 2014. године

порнографске сајтове, као и преко спам порука, инфицирањем рачунара злонамерним програмом као и намерним стварањем назива сајтова сличним дечијим како би деца доведена у заблуду грешком видела садржај који није прикладан за њих.[409]

Сексуални туризам који се односи циљано на децу и дечија проституција представља такав облик сексуалног злостављања када се интернет, као медиј који се одликује ниским трошковима око постављања, ажурирања и одржавања сајтова, користи за промовисање дечијих сексуалних услуга које се плаћају. Сајтови на којима се промовише дечија проституција често представљају и виртуелно место на коме се директно уговарају састанци и деле информације за лични контакт. Сајтови који промовишу дечију проституцију најчешће експлоатишу децу која су побегла од куће[410] и која су старости око 12 година.[411] Туристички агенти који се баве секс туризмом су такође у великој мери заступљени на интернету, а фокусирају се искључиво на децу у земљама где правни прописи који се односе на сексуалне односе са малолетницима нису толико строги односно где је граница пунолетства нижа него у већини правних система па се на тај начин избегава и санкционисање оваквих односа. Поред авионског превоза и хотелског смештаја, овакви агенти обећавају и улазнице за локалне борделе, секс клубове и контакт са агенцијама за пословну пратњу.[412] Организација Уједињених нација је прогласила употребу интернета ради проналажења малолетних лица за сексуалне услуге једним од фактора пораста броја земаља у којима је дечији секс туризам у развоју.[413]

---

[409] Познат је пример да је постојао сајт са адресом www.bobthebiulder.com која је наводила децу да мисле да је реч о сајту посвећеном дечијем цртаном филму Bob the Builder, чији се исправан сајт налази на адреси bobthebuilder.com. На овај начин, деца су била усмеравана на сајт са експлитним сликама сексуалних односа младих људи.

[410] Brunker, Mike: "Streetwalkers in Cyberspace", MSNBC, 1999, http://www.nbcnews.com/id/3078778/#.VRcei_nF-T8, претражено 07. 09. 2014. године и McKim, Jennifer: "Pimp Pleads Guilty to Prostituting Minor", Orange County Register, 2006, http://www.ocregister.com/ocregister/news/atoz/article_1209170.php, претражено 10. 09. 2014. године

[411] Alonzo-Dunsmoor, Monica:"Phoenix Officials to Crack Down on Child Prostitution", The Arizona Republic, 2006, http://www.azcentral.com/arizonarepublic/local/articles/0311prostitution0311.html, претражено 07. 09. 2014. године

[412] Hall, Macalister Malcolm.: "The Darker Side of Travel", The UK Telegraph, 2003, http://www.telegraph.co.uk/travel/destinations/asia/cambodia/728691/The-darker-side-of-travel.html, претражено 07. 09. 2014. године

[413] Asia's Child Sex Victims Ignored, BBC, 2000.,http://news.bbc.co.uk/1/hi/world/asia-pacific/926853.stm, претражено 07. 09. 2014. године

Груминг (engl.Grooming) представља предузимање намерних радњи како би се придобила дечија пажња са сврхом развијања емоционалне везе са дететом, а све у циљу припреме за покушај сексуалног злостављања.[414] Под грумингом се подразумева и предузимање низа предаторски мотивисаних поступака који насилнику омогућавају сексуалну злоупотребу малолетне особе.[415] Одрасла особа предузима конкретне радње (нпр. наговарање, врбовање, мамљење, слање поклона и сл.) како би у току интернет комуникације наговорила дете да дође до сусрета.Ове радње морају да трају краће или дуже време, али никада не представљају један појединачни акт јер се ради о јасном мотиву и умишљају. Дете или малолетна особа се „припрема за злочин“ кроз задобијање поверења, превазилажење инхибиција у односу на сексуалне релације и одвајање те младе особе од окружења у које има поверења, предатор се на разне начине полако укључује у дететову свакодневицу и проналази низ објашњења и изговора којима оправдава своје поступке.[416] Циљ груминга је да се са дететом успостави и развије контакт, оствари и одржи комуникација, а затим и оствари физички приступ детету.

в) Профил жртве и предатора . Коришћењем интернета круг деце чија је виктимизација могућа није остао уско одређен само на децу пријатеља или децу и младе из блиског окружења (школа, суседство и сл.), већ су сва деца широм света која време проводе на интернету постала потенцијална мета за виктимизацију од стране сексуалних предатора. Преко интернета корисници међусобно један другога не виде, па сама чињеница да се нечије лице не види утиче на начин понашања јер се насилници крију иза анонимности. Овакво стање ствари одговара свима који имају афинитете према сексуалној експлоатацији деце јер су за њих интернет и друштвене мреже право „игралиште” за ступање у контакт са децом, при чему сами насилници остају заштићени и сакривени.

Деца која су повучена, несигурна у себе и стидљива чешће постају жртве сексуалних насилника, јер она пре користе интернет како би склопила нова познанства, што их доводи у опасност од предатора који вребају. Деца и млади

[414] Протрка, Никола, Грубер, Кристијан, Салопек, Данко, *op.cit.,* 2015, str. 649
[415] Кликни безбедно, http://kliknibezbedno.rs/sr/gruming.1.137.html, претражено 15. 07. 2015. године
[416] *Ibid.*

који би у реалном свету избегавали контакт са непознатим људима пружиће шансу странцу који их контактира преко интернета. Интернет виктимизација настаје у дететовој околини коју оно сматра сигурном и заштићеном од стране одраслих који живе под истим кровом, она настаје док се дете налази на интернету код куће, у школи, код пријатеља, у библиотеци. Управо је то највећа опасност, јер је број напада преко интернета постао већи од броја сексуалних напада на децу у „реалном" свету.

Појединa истраживања која су испитивала сексуалне понуде упућиване деци преко друштвених мрежа показала су да су у највећем броју случајева жртва и предатор били потпуни странци, да се нису познавали и да никада пре нису имали лични контакт – чак 86% анкетиране деце и младих су изјавили да су предатора први пут упознали преко интернета.[417] Према статистикама, девојчице су чешће жртве нежељених сексуалних понуда и контаката преко интернета,[418] док су дечаци у већој мери од девојчица изложени порнографији на интернету.[419] Подаци Националног центра за несталу и злостављану децу показују да је, код испитаних корисника интернета који су старости од 10 до 17 година и који су били жртве сексуалних предатора, највећа стопа виктимизације међу младима старим 16 година (24%), затим петнаестогодишњацима (23%) и седамнаестогодишњацима (19%).[420]

Испитивањем материјала дечије порнографије који је заплењен приликом различитих хапшења стиче се увид у најчешће категорије деце која су жртве сексуалних предатора.[421] Реч је о деци старости од 6 до 12 година јер је 83% заплењеног материјала садржала снимке деце управо ове старосне доби, али међу пронађеним материјалом је било и снимака деце старости од 3 до 5 година (39%) па чак и деце млађе од 3 године (19%).

Нису сви сексуални предатори који вребају децу преко интернета и друштвених мрежа исти нити имају исте циљеве задовољења своје потребе. Једна од основних подела је на основу тога да ли криминална активност

---

[417] Wolak, Janis, Mitchell, Kimberly, Finkelhor, David, *op.cit.,* 2006.
[418] *Ibid.*
[419] *Ibid.*
[420] National Center for Missing and Exploited Children, http://www.missingkids.com/home, претражено 10. 05. 2014. године
[421] O'Leary, J.Robert, D'Ovidio, Robert, *op.cit.,* 2007.

предатора подразумева или не директан сексуални контакт са децом,[422] па се на основу тога разликују две врсте предатора: предатори који немају директан сексуални контакт са децом и предатори који имају директни сексуални контакт са децом.

Предатори који немају директан сексуални контакт са децом могу да буду: *трговци и прикривени колекционари*, они користе интернет како би приступили и учитавали са интернета дечију порнографију, али се не баве производњом дечије порнографије и директним злостављањем деце; *трговци***,** који траже и ступају у контакт са другим истомишљеницима на интернету и на друштвеним мрежама како би размењивали дечију порнографију (филмове и слике) како би направили своју колекцију; *прикривени колекционари* – пажљиво крију своју склоност ка дечијој порнографији, не ступају у контакт са сличнима себи већ најчешће праве колекције дечије порнографије тако што је купују преко интернет продавница.

Међу предаторима који имају директан сексуални контакт са децом разликују се: *усамљени колекционари* – злостављају децу како би за своју личну колекцију снимили различите порнографске материјале, које не деле нисаким нити их дистрибуирају било где јер се плаше да не привуку пажњу и буду ухваћени, јавно окарактерисани као предатори и педофили и због тога санкционисани; *кућни колекционари* – злостављају децу при чему то снимају како би створили филмове и слике који се подводе под категорију дечије порнографије, они нису стидљиви па тај снимљени материјал дистрибуирају даље, деле га преко интернета бесплатно или се са истомишљеницима размењују преко различитих интернет канала комуникације; *комерцијални колекционари* - дистрибуирају дечију порнографију у циљу стицања новчане добити, они су такође спремни да злостављају децу како би снимили што више дечијег порнографског материјала и како би га по високој цени продали другим предаторима који желе да дођу у посед оваквог материјала.

Поред наведене поделе, разликује се и тип предатора *ситуационог преступника*. Анонимност на интернету доводи до ослобађања скривених тајни,

---

[422] Klain, Eva, Davies, Heather, Hicks, Molly: "Child Pornography: The Criminal Justice System Response", Washington, DC: National Center for Missing and Exploited Children, 2001, https://www.ncjtc.org/NCJTC_Member_Resources/Public/Child%20Pornography%20Criminal%20Justice%20Response.pdf , претражено 15. 11. 2014. године

па тако и оних који се односе на сексуалну злоупотребу деце, па се ситуациони преступник постаје заправо из разлога испитивања сексуалне радозналости.[423] Ситуациони преступници заправо интернет доживљавају као могућност да гледају дечију порнографију која их привлачи али да истовремено остану сакривени иза свог рачунара јер их је заправо стид што су склони оваквим сексуалним експериментима.

Подаци о виктимизацији, различита истраживања, званичне статистике и извештаји по спроведеним полицијским истрагама показују да су мушкарци ти који у већој мери него жене сексуално нападају децу преко интернета: чак 92% ухапшених интернет предатора је било мушког пола. [424] Што се расне припадности тиче, 92% ухапшених због дела сексуалног интернет насиља према малолетницима били су белци.[425] Интересантно је да предатори нису у свим случајевима дечије интернет порнографије били одрасле особе: чак 43% извршилаца било је млађе од 18 година.[426]

г) Како се супротставити и одбранити – проблем непријављивања. Иако се доста пажње посвећује превенцији овог вида насиља, како путем подизања свести и деце и родитеља о опасностима које постоје на друштвеним мрежама и интернету, тако и све чешћем објављивању вести о судским поступцима у којима су насилници санкционисани, и даље заправо не постоје тачни подаци о обиму ове врсте криминалитета. Деца веома ретко пријављују сексуалне нападе које доживљавају преко друштвених мрежа јер их је срамота да родитељима причају о томе, нису сигурни да ли је то што им се дешава лопе или не, али уједно и страхују да ће им родитељи забранити да користе интернет и да ће надгледати све њихове активности на друштвени мрежама. Подаци Националног центра за несталу и злостављану децу из 2005.године[427] показали су да се пријави полицији или интернет провајдеру само 5% случајева сексуалног насиља које се према деци реализује путем интернета, а аларманти

---

[423] *Ibid.*
[424] Alexy, M. Eileen, Burgess, W. Ann, Baker, Timothy: "Internet Offenders: Traders, Travelers, and Combination Trader-Travelers", Journal of Interpersonal Violence, volume 20 number 7, 2005, стр. 804-812.
[425] Wolak, Janis, Mitchell, Kimberly, Finkelhor, David, *op.cit.,* 2006.
[426] Подаци Националног центра за несталу и злостављану децу (National Center for Missing and Exploited Children), http://www.missingkids.com/home, претражено 10. 05. 2014. године
[427] *Ibid.*

су и подаци да 56% жртава се није никоме поверило и испричало за насиље које су претрпели преко интернета.

Проблем са непријављивањем ових дела постоји и због тога што велики број како деце тако и родитеља не зна коме их треба пријавити. Према истраживању Националног центра за несталу и злостављану децу из 2005. године[428] 65% родитеља и 82% деце не знају коме би могли да се обраде у случају нежељених контаката са сексуалном конотацијом преко интернета.

Бројни су међународни правни документи који покушавају да искорене злоупотребу деце у порнографске сврхе. Конвенција о правима детета[429] обавезала је све државе потписнице да свако дете заштите од експлоатације и од обављања било ког посла који би могао да буде опасан по живот и здравље детета, односно који представља угрожавање и/или повреду његовог физичког, емотивног и сексуалног интегритета.[430] Конвенција Међународне организације рада бр. 182 о најгорим облицима дечијег рада[431] са Препоруком бр.190 о забрани и хитној акцији за укидање најгорих облика дечјег рада[432] (обе донете у Женеви 1999. године, а у Србији ратификоване 2003. године) донете су у циљу спречавања свих облика сексуалне експлоатације и сексуалног злостављања деце, а посебно спречавања међународне трговине децом, дечије проституције, дечије порнографије и сексуалног туризма који настају злоупотребом рачунарских система и друштвених мрежа преко којих се деца „регрутују" у поменуте сврхе. Поред ова два документа, Факултативни протокол уз Конвенцију о правима детета о продаји деце, дечјој проституцији и дечјој порнографији[433] (донет 2000. године, ратификован 2002. године) и Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања (донета 2007. године, а Србија је потписала и започела процес ратификације)

---

[428] *Ibid.*
[429] Конвенција о правима детета („Службени лист СФРЈ – Међународни уговори", бр. 15/90)
[430] Стевановић, Ивана: „Кривична дела везана за искоришћавање деце у порнографске сврхе злоупотребом рачунарских система и мрежа (међународни и домаћи кривичноправни оквир)", ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 27
[431] Конвенција Међународне организације рада (МОР) бр. 182 о најгорим облицима дечјег рада („Службени лист СФРЈ – Међународни уговори", бр. 8/03)
[432] Препорука Међународне организације рада (МОР) бр. 190 о забрани и хитној акцији за укидање најгорих облика дечјег рада („Службени лист СФРЈ – Међународни уговори", бр. 8/03)
[433] Факултативни протокол уз Конвенцију о правима детета о продаји деце, дечјој проституцији и дечјој порнографији („Службени лист СРЈ – Међународни уговори", бр. 22/02)

представљају покушај успостављања стандарда у циљу адекватније заштите деце од искоришћавања у порнографске сврхе злоупотребом рачунских система и мрежа, као и заштите деце од „регрутовања" преко друштвених мрежа.

Поред доношења одговарајуће законске регулативе, на државе се апелује да осмисле и уведу различите независне програме, пројекте и мере превенције којима би се деца заштитила од сексуалне експлоатације преко интернета. Неопходно је на свим нивоима и код свих релевантних актера (правосуђе, полиција, законодавство, родитељи, деца) подићи свест о томе шта све сексуално насиље преко интернета представља и који су све модели понашања и деловања сексуалних предатора. Један од императива је и стварање јаког националног плана за спречавање сексуалне експлоатације деце преко интернета. Неопходно је путем организовања различитих тренинга радити и на сензибилизацији полиције, судија и тужилаца који ће руководити хватањем и процесуирањем сексуалних предатора.

Поред едукације деце о могућим ризичним понашањима на друштвеним мрежама и опасностима повезивања са непознатим особама, неопходно је едуковати и родитеље, који појединим својим радњама могу да угрозе децу. Наиме, деца, поготово у доба раног детињства, не могу да дају пристанак на објављивање својих личних података и слика на друштвеним мрежама, а многи родитељи управо из љубави према својој деци и потребе да поделе са другима, објављују на друштвеним мрежама.[434] На овај начин и родитељи несвесно угрожавају приватност деце, јер се поставља питање како могу ови објављени подаци и слике да утичу на то дете које одраста. Ако је информација доступна на друштвеним мрежама када дете достигне зрелост и адолесценцију, постоји материјал за потенцијалне насилнике у школи, за потенцијалне послодавце, као и за медије, ако ово дете постане истакнута личност. На овај начин, родитељи су ти који су створили фајл „прљавог веша" за своје дете.[435]

Многи сајтови који су посвећени заштити деце на интернету (нпр. ISafe, NetSmartz, WiredKids, CyberAngels) нуде различите едукационе програме и

---

[434] Myra Hamilton: Objavljivanje detalja iz života deteta predstavlja pitanje privatnosti, извор: The Conversation.com - 25. 12. 2013. године, http://partners-serbia.org/privatnost/aktuelno/myra-hamilton-objavljivanje-detalja-iz-zivota-deteta-predstavlja-pitanje-privatnosti/, претражено 06. 03. 2014. године

[435] *Ibid.*

материјале који деци и младима указују на све опасности које вребају са интернета, уче их како да уоче потенцијално опасна понашања и како да остварују сигурне комуникације преко друштвених мрежа. Они нуде материјале који су прилагођени деци и који им дају информације о томе како да безбедно користе све погодности интернета и дружења преко друштвених мрежа.

3.1.5. Вршњачко насиље (енгл. cyber bullying)

а) Појам вршњачког насиља на интернету. Као последица повећања доступности дигиталних технологија међу децом и школском популацијом, појавио се нови облик насиља – вршњачко насиље на интернету, односно коришћење нових технологија за пласирање увредљивих, штетних, вербалних и видео записа.

Вршњачко насиље подразумева специфичан облик континуираног интергенерацијског насиља које проистиче из одређеног односа међу вршњацима у основној и средњој школи, са циљем да се жртви нанесе штета (најчешће психичка), али примарно да се насилник прикаже доминантним у групи.[436]

Ова врста насиља међу тинејџерима може довести и до нарушавања дигиталне репутације корисника друштвене мреже, тј. до стварања негативног мишљења или става који ће други имати о тој корисници/кориснику на основу онога што она/он каже или учини на мрежи.[437] Све објављене информације се великом брзином и моментално шире друштвеном мрежом и немогуће их је касније уклонити у потпуности.

Појавом и развојем друштвених мрежа и сталним коришћењем интернета, порасло је и „виртуелно" насиље међу вршњацима. Вршњачко насиље на интернету **(**интернет насиље, електронско насиље, дигитално насиље, cyber bullying**)** представља у најширем смислу сваки облик вршњачког насиља

[436] Миладиновић, Александар, Петричевић, Витомир:"Електронско вршњачко насиље", Зборник радова - Међународна научностручна конференција "Вршњачко насиље (етиологија, феноменологија, начини превазилажења и компаративна искуства)", Висока школа унутрашњих послова, Бања Лука, 2013, стр. 246, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Vrsnjacko-nasilje.pdf, претражено 14. 10. 2014. године

[437] Приручник за заштиту деце и младих од сајбер насиља и примену у редовном наставном програму основних и средњих школа - "Tagged", op.cit., 2013, стр. 17

које се догађа у виртуелном свету,[438] а може се дефинисати као употреба електронске комуникације (интернета или друге дигиталне технологије) како би се нека друга особа заплашила, застрашила, како би јој се претило а све у циљу да се та особа осећа несигурна и емоционално рањива.[439] Једна од кључних последица коју интернет насиље производи је управо да се жртва осећа емоционално рањива и повређена.[440]

Електронско вршњачко насиље такође може да се дефинише као агресиван, тенденциозан акт који група или појединац спроводи користећи електронска средства комуникације, у више наврата и током дужег периода против жртве која не може лако да се одбрани од оваквих напада.[441] То је савремени, модерни облик вршњачког насиља који се реализује помоћу средстава масовне комуникације коју користе ученици, у првом реду преко интернета и мобилних телефона, у циљу понижавања, дискредитације, омаловажавања и на друге начине наношења штете другима.[442] Овај вид насиља одликују све кључне карактеристике традиционалног вршњачког насиља – агресивно понашање изражено кроз негативне акције, намера да се друга особа повреди, несразмера моћи између учесника и репетитивност,[443] али и специфичности које га сврставају у посебно опасан облик насилничког понашања.

б) Појавни облици. Вршњачко насиље на интернету су најчешће се врши слањем електронских порука, СМС и ММС порука, у причаоницама, кроз блогове или комуникацијом преко друштвених мрежа.[444]

---

[438] Удружење „Стоп мобинг", http://www.mobing.rs/articles.php?article_id=17, претражено 03. 03. 2015. године

[439] Patchin, W.Justin, Hinduja, Sameer:"Bullies move beyond the schoolyard: a preliminary look at cyberbullying", Youth Violence Juvenile Justice, 2006; volume 4, number 2, стр. 148-169, https://www.ncjrs.gov/App/publications/abstract.aspx?ID=234986, претражено 13. 03. 2015. године

[440] Vandebosch, Heidi, Van Cleemput, Katrein: "Defining cyberbullying: a qualitative research into the perceptions of youngsters", CyberPsychology & Behavior, 2008, volume 11, number 4, стр. 499-503, http://thecyberbullyingproblem.wikispaces.com/file/view/33985751.pdf, претражено 13. 03. 2015. године

[441] Љепава, Николина: „Реално злостављање у виртуелном окружењу: Превенција и интервенција у случајевима злостављања дјеце на интернету", Часопис Актуелности, стр. 22–33, 2011, Бања Лука: Бања Лука колеџ, http://www.roditelj.org/wp-content/uploads/2011/12/aktuelnosti-2011-sajberzlostavljanje-nljepava-1.pdf, претражено 24. 03. 2015. године

[442] Миладиновић, Александар, Петричевић, Витомир, *op.cit.,* 2013, стр. 247

[443] Поповић-Ћирић, Бранислава: "Вршњачко насиље у сајбер простору", ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр.3, година 12, септембар 2009, стр. 44

[444] StopCyberbullying.org: "How It Works", http://www.stopcyberbullying.org/how_it_works/index.html, претражено 13. 03. 2015. године

Према схватању једног броја аутора[445] вршњачко насиље на интернету може се испољити као: прогањање и сексуално узнемиравање; слање непристојних, увредљивих и вулгарних порука о некој особи и то преко причаоница, група на друштвеним мрежама или саме друштвене мреже; објављивање поверљивих или интимних података о некој особи; оговарање и вређање; намерно или окрутно избацивање неке особе из одређене групе (искључивање); застрашивање преко интернета које се манифестује претњама и стављањем у изглед неког зла које ће се догодити (претње); слање и објављивање неистинитих и окрутних порука о некој конкретној особи, најчешће о њеним физичким особинама (изглед, висина, тежина и сл.), наводном промискуитету и/или сексуалном опредељењу (оговарање, клеветање); служење именом жртве како би се неком трећем слале увредљиве или претеће поруке, а све у циљу да жртва буде кривац (лажно представљање, обмањивање); затрпавање жртве порукама како би се жртви досађивало, онеспособило сандуче електронске поште или убацио у систем злонамерни програм.

Други аутори, поред наведених облика, још разликују и преузимање или злонамерно креирање дигиталног идентитета жртве (нпр.странице, профила и сл.) у оквиру кога се она приказује у негативном контексту, постављају одређени садржаји који деградирају жртву;[446] еротску или порнографску представу о жртви, где жртва покушава да се омаловажава, деградира или понизи постављањем фотографија или снимака у недоличном контексту или у оквиру порнографских страница;[447] снимање жртве без њеног пристанка (тзв. „весело шамарање", енгл. „Happy slapping"[448]) и приморавање да уради нешто понижавајуће или против своје воље или док је злостављана, а затим и

[445] Mishna, Faye, McLuckie, Alan, Saini, Michael:"Real-world dangers in an online reality: a qualitative study examining online relationships and cyber abuse", Social Work Research, 2009; volume 33, number 2, стр. 107-118, http://icbtt.arizona.edu/sites/default/files/Mishna,_McLuckie,_&_Saini_Social_Work_Research_KHP_Cyber_Abuse_0.pdf, претражено 13. 03. 2015. године, Cyberbullying and Harrasment, http://www.netce.com/coursecontent.php?courseid=1127, претражено 20. 09. 2013. године
[446] Миладиновић, Александар, Петричевић, Витомир, *op.cit.,* 2013, стр. 251
[447] *Ibid.*
[448] *Ibid.*

објављивање таквог снимка на друштвеној мрежи; слање сексуално експлицитних слика, порука и електронске поште (енгл. Sexting).[449]

С обзиром на наведене појавне облике вршњачког насиља можемо да закључимо да жртва вршњачког насиља на друштвеним мрежама може да постане и особа која није корисник ни друштвене мреже ни интернета.

У литератури су заступљена схватања[450] да је, независно од механизма комуникације који насилници користе у виртуелном свету, према специфичностима начина извршења могуће разликовати осам облика вршњачког сајбер насиља:

(1) вређање (тзв. флејминг, енгл. Flaming), које подразумева кратку и жустру расправу између две или више особа путем било које комуникационе технологије, која се састоји у намерном постављању или слању електронских порука са увредљивим, злобним, понижавајућим или вулгарним садржајима;

(2) узнемиравање (енгл. Harrasment), које се састоји у понављању слања увредљивих, провокативних, грубих и непријатељских порука једној особи или групи; за разлику од вређања овај облик насиља је једностран и траје дуже време;

(3) оговарање и клеветање (енгл. Denigration, Dissing) састоји се у слању или постављању увредљивих и неистинитих информација о некоме у намери угрожавања репутације или пријатељских односа коју та особа има, посебан облик могу да представљају тзв. „електронске књиге утисака“ (енгл. Slam book) које имају за циљ понижавање и исмевање других особа, најчешће школских вршњака;

(4) лажно представљање (имперсонација, енгл. Impersonation) састоји се у лажном представљању једне особе тако што користи шифру те особе да би приступила њеним налозима, а затим комуницирала на негативан или неприкладан начин са другима, стварајући утисак да изражава мишљење особе чији налог користи;

---

[449] O'Donovan, Eamonn:”Sexting and student discipline”, District Administration, 2010; volume 46, numeber 3, http://www.districtadministration.com/article/sexting-and-student-discipline, претражено 14. 03. 2015. године

[450] Willard, Nancy: “An Educator's Guide to Cyberbullying and Cyberthreats”, http://miketullylaw.com/library/cbcteducator.pdf, претражено 13. 03. 2015. године

(5) недозвољено саопштавање (тзв. аутинг, енгл. Outing) представља јавно показивање, постављање или прослеђивање туђих приватних слика, садржаја или личне комуникације оним особама којима те информације нису биле намењене; на овај начин се туђе личне информације чине јавним и доступним свима;

(6) обмањивање (енгл. Trickery) постоји када нападач преваром или лукавством открива личне, најчешће тајне и понижавајуће информације о некој особи, а затим их дели са другима; за разлику од недозвољеног саопштавања где је насилник у поседу одређених информација о некоме, код обмањивања он користи превару како би до поверљивих информација дошао;

(7) искључивање (енгл. Exclusion, Ostracism) представља индиректни метод сајбер насиља који се састоји у намерном искључивању неке особе из одређене виртуелне групе или заједнице (нпр. листа пријатеља, e-mail листа, соба за ћаскање и сл.);

(8) прогањање (енгл. Cyber stalking) представља коришћење електронских комуникација у циљу прогањања неке особе кроз репетитивну узнемиравајућу и претећу електронску комуникацију.

Вршњачко насиље на интернету може да се испољи на директан или индиректан начин.

Директно интернет насиље се испољава кроз слање СМС и ММС порука као и порука у „причаоницама" и на „ћаскањима" које су узнемирујућег, увредљивог и претећег садржаја, узнемиравање телефонским позивима, вређање и лажно представљање у електронској комуникацији, креирање интернет страница које садрже приче, слике, цртеже или шале на рачун одређене особе, снимање мобилним телефоном или камером, прослеђивање снимака на интернет или друштвене мреже, узнемиравање преко електронске поште (увредљиве шале, претње и сл.), узнемиравање на друштвеним мрежама, слање вируса или порнографских садржаја, постављање интернет анкета о некоме, објављивање лажних података о некоме или изношење нечијих личних прилика или тајни, крађа лозинке или надимка на друштвеној мрежи или у „причаоници". На друштвеним мрежама је такође могуће формирати групе против одређених особа, које најчешће имају називе типа „Ко мрзи (име и

презиме) из ...". Забележено је да је на друштвеној мрежи Фејсбук крајем 2011. године било 1.400 група које су садржале речи: „сви који мрзе…".[451]

Насиље преко посредника или индиректно интернет вршњачко насиље је најопаснија врста насиља преко интернета јер често укључује одрасле особе, а постоји када извршилац напада жртву преко треће особе, која тога најчешће није свесна. Примери овакве врсте насиља су чести на друштвеним мрежама: отварање лажног профила под туђим именом и објављивање различитих узнемирујућих или вулгарних ствари у име неког другог, писање негативних или осуђујућих текстова са профила неког другог корисника како би се њему нанела штета и сл.

Истраживање дигиталног вршњачког насиља, које је спроведено у 17 основних и 17 средњих школа током новембра 2012. године у Србији, у коме је учествовало 3784 ученика, показало је да је 9% основаца и 12% средњешколаца снимано мобилним телефоном или камером, док је СМС поруке узнемирујућег садржаја добило 5% ученика основношколског узраста и 9% средњошколаца. Узнемиравање на друштвеним мрежама искусило је 18% основаца и 17% средњошколаца.[452]

У истраживању у коме је испитано 1241 средњошколаца у САД, 10% испитаника је рекло да је било снимано против своје воље, при чему је током снимања било понижено или нападнуто.[453] Друго истраживање које је спроведено међу 365 учениика нижих разреда средње школе у Канади показало је да је једна трећина ових адолесцената изјавила да су се представљали као различите особе када су на интернету, а једна четвртина је признала да су се представљали као да су особе супротног пола.[454] Скоро 19% испитаника је

[451] *Ibid.*

[452] Маричић, Татјана, Ковачевић, Верица: "Вршњачко – дигитално насиље и начини превазилажења", Зборник радова - Међународна научностручна конференција "Вршњачко насиље (етиологија, феноменологија, начини превазилажења и компаративна искуства)", Висока школа унутрашњих послова, Бања Лука, 2013, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Vrsnjacko-nasilje.pdf, претражено 14. 10. 2014. године

[453] Calvete, Esther, Orue, Izaskun, Estévez, Ana, Villardón, Lourdes, Padilla, Patricia:"Cyberbullying in adolescents: modalities and aggressors' profile", Computers in Human Behavior, 2010; volume 26, number 5, стр. 1128 - 1135, http://database.cmch.tv/SearchDetailBrowser.aspx?rtrn=advnce&cid=5762, претражено 13. 03. 2015. године

[454] Cassidy, Wanda, Jackson, Margaret, Brown, N.Karen: "Sticks and stones can break my bones, but how can pixels hurt me? Students' experiences with cyber-bullying", School Psychology International, volume 30, number 4, стр. 383 - 402, Sage Publications, 2009,

навело да су лагали када су описивали свој физички изглед а 15% је признало да се намерно користило именом неке друге особе када је преко интернета ступало у контакт са другим особама.[455]

в) Профил жртве и насилника. За разлику од физичког вршњачког насиља које се догађа у школи или на улици, вршњачко насиље путем интернета може да траје 24 сата свих седам дана у недељи, а жртва интернет насиља може да доживи непријатности и у својој кући и на местима на којима се раније осећала сигурном. Анонимни насилник може да у насиље које се догађа укључи и трећа лица, што жртву доводи у неравноправан положај са насилницима, чији је број практично неограничен.[456]

У реалном свету насилник је обично крупна и снажна особа, док се у виртуелном свету јачина насилника мери према његовим посебним техничким вештинама и умећима руковања рачунарима и сналажењу на интернету.[457] Жртва и насилник уопште не морају да се познају, као и код било ког другог облика виртуелног насиља; насилник може да буде невидљив или анониман, што може да отежа његово проналажење а да код жртве изазове снажан осећај страха и незаштићености.

На основу спроведене анализе мотива и разлога због којих се јавља вршњачко насиље у виртуелном простору, поједини аутори[458] наводе следећу класификацију интернет насилника:

Осветољубиви анђео (анђео осветник, енгл. Vengeful angel) – особа која не доживљава себе као насилника већ као особу која тражи правду и штити себе или друге од „лоших људи“, за које верује да заслужују да буду виктимизирани. Сматра се да у ову категорију спадају најчешће жртве традиционалних облика

---

http://extension.fullerton.edu/professionaldevelopment/assets/pdf/bullying/sticks_and_stones.pdf, претражено 14. 03. 2015. године

[455] *Ibid.*

[456] Мирић,Филип: “Облици вршњачког насиља путем интернета и друштвених мрежа”, Зборник радова - Међународна научностручна конференција “Вршњачко насиље (етиологија, феноменологија, начини превазилажења и компаративна искуства)”, Висока школа унутрашњих послова, Бања Лука, 2013, стр. 401, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Vrsnjacko-nasilje.pdf, претражено 14. 10. 2014. године

[457] Hinduja, Sumeer, Patchin, W.Justin:”Cyberbullying Fact Sheet: What You Need To Know About Online Aggression”, http://www.cyberbullying.us/cyberbullying_fact_sheet.pdf, претражено 13. 03. 2015. године

[458] Aftab, Parry: “What methods work with the different kinds of cyberbullies?, 2006, www.stopcyberbullying.org/pdf/howdoyouhandleacyberbully.pdf, претражено 12. 03 .2014. године

насиља, које се на овај начин свете другима не схватајући да су и сами постали насилници.

Гладан моћи (енгл. Power hungry) – особа која највише личи на класичног школског злостављача који, користећи се тактиком застрашивања, покушава да успостави контролу над другима и силом стекне моћ и ауторитет. За разлику од насилника типа „осветољубиви анђео“ који углавном делује самостално, насилник „гладан моћи“ има потребу да стално има публику која ће посматрати или подржавати његове поступке. Веома често, ова врста насилника прибегава и традиционалним врстама насиља.

„Штребер" осветник (енгл. Revenge of the nerd) – особа коју средина у којој живи доживљава као „штребера“. Како би компензовао своје недостатке на које му околина указује, постаје жељан моћи и освете. Веома често он је и жртва традиционалног вршњачког насиља јер је и конституционално у највећем броју случајева ситне грађе и физички слабији од већине својих вршњака. Он се свети, а анонимност виртуелног простора му гарантује да никада неће морати да се у свакодневном животу сретне са својим жртвама и ризикује да буде физички угрожен. Због свих ових карактеристика и због својих техничких вештина може да буде најопаснији од свих виртуелних насилника.

Пакосне девојчице (енгл. Mean girls) – особе које чине насиље из досаде или ради забаве и за њих је понижавање и вређање других један од начина разоноде којом јачају свој его. Ова категорија насилника не прети својим жртвама, већ их искључиво само исмејава и омаловажава. Најчешће делују у групама јер желе да други знају ко су они и како имају моћ, као и да им се други диве. Овај тип насилника се углавном јавља међу девојчицама.

Непажљиви (енгл.Inadvertent) – особе које постају насилници када не размишљајући одговоре на примљену провокацију или када се својом непажњом уведу у индиректно сајбер насиље не размишљајући о последицама. О себи не мисле да су насилници.

Поједина истраживања спроведена међу децом узраста од 10 до 17 година показују да су интернет насилници међу вршњацима најчешће дечаци,[459]

[459] Ybarra, L.Michaele, Mitchell, J.Kimberly:"Prevalence and frequency of Internet harassment instigation: implications for adolescent health", Journal of Adolescent Health, 2004, volume 41 number 2, http://www.unh.edu/ccrc/pdf/CV157.pdf, претражено 14. 03. 2015. године

старости од 13 до 15 година.[460] Има случајева када су ови интернет насилници заправо некада били или су и даље жртве реалног насиља или се и у реалном животу понашају као насилници.[461] Највећи број насилника има слабе друштвене односе са својим вршњацима, нема јаку емотивну везу са родитељима, код њих не постоји адекватна родитељска контрола и надзор и крећу се у друштву делинквентних особа.[462]

Постоји и посебна категорија интернет насилника која је позната под називом „силеџије које воле да се попну на врх друштвене лествице" (енгл. Social climber bullies).[463] То су најчешће старији студенти из богатијих друштвених слојева, добри ученици са водећим позицијама у школским клубовима, друштвима или активностима, којима управо друштвени статус омогућује да нико не посумња да они заправо малтретирају некога. Њихове жртве су „непопуларни" ученици, „штребери" или ученици који очајно желе да им се приближе и буду део групе окупљене око њих јер постоји мала вероватноћа да ће ови ученици пријавити насиље.

Посматрајући према полу, најчешће жртве вршњачког интернет насиља су девојчице и девојке, при чему су оне у највећој мери жртве оговарања и

---

[460] Williams, R.Kirk, Guerra, G.Nancy:"Prevalence and predictors of internet bullying", Journal of Adolescent Health, 2007; volume 41 number 6, http://www.slideshare.net/WCT-Law/fp-58-prevalence-and-predictors-of-internet-bullying , претражено 14. 03. 2015. године

[461] Ybarra, L.Michaele, Espelage, L.Dorothy, Mitchell, J.Kimberly:"The co-occurrence of Internet harassment and unwanted sexual solicitation victimization and perpetration: associations with psychosocial indicators", Journal of Adolescent Health, 2007; volume 41, http://www.ncbi.nlm.nih.gov/pubmed/18047943, претражено 14. 03. 2015. године

[462] Ybarra, L.Michaele, Diener-West, Marie, Leaf, J.Phillip:"Examining the overlap in Internet harassment and school bullying: implications for school intervention", Journal of Adolescent Health, 2007; volume 41, http://www.wthlawfirm.com/for-parents/links/examining-overlap-internet-harassment-school-bullying/ ,претражено 14. 03. 2015. године

[463] Willard, E.Nancy:"Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress", Champaign, IL: Research Press; 2007, https://books.google.rs/books?id=VyTdG2BTnl4C&pg=PP6&lpg=PP6&dq=Cyberbullying+and+Cyberthreats:+Responding+to+the+Challenge+of+Online+Social+Cruelty,+Threats,+and+Distress&source=bl&ots=u5DlZGvo8v&sig=7dA7kdGtX-4VrWUMqychrTkYLk8&hl=sr&sa=X&ei=Fb8FVbbgJsfVavKLgYgO&ved=0CEsQ6AEwBQ#v=onepage&q=Cyberbullying%20and%20Cyberthreats%3A%20Responding%20to%20the%20Challenge%20of%20Online%20Social%20Cruelty%2C%20Threats%2C%20and%20Distress&f=false, претражено 14. 03. 2015. године

трачева који се међу њима шире чешће него међу дечацима. [464] Жртве интернет насиља су обично жртве и других врста насиља.[465]

г) Последице које указују на постојање вршњачког насиља на интернету и непријављивање насиља. Поједини аутори[466] указују да на постојање вршњачког насиља у реалном и виртуелном свету указују одређена понашања жртве: депресија или анксиозност, посебно у случајевима када не може да приступи интернету; депресија или анксиозност која се јавља када стигне смс или имејл порука; тешкоће са учењем и негативна промена понашања у свакодневном животу (нпр. бежање из школе, понављање, одбацивање досадашњег друштва); усамљивање од пријатеља и породице; гледање порнографског материјала на рачунару; одрицање од нормалних дневних активности како би се време проводило испред компјутера и на интернету; гашење рачунара када се приближава неко од старијих (родитељ, наставник...) и брисање историје посећених сајтова.

Највећи страхови које жртва има су: да буде одбачена и стигматизована од стране друштва у коме се налази, да јој се насилник не освети ако некоме каже да трпи насиље, да и пријатеље не увуче у невоље, да ће родитељи искључити интернет или одузети мобилни телефон уколико чују за проблем.[467]

Последице интернет насиља могу да буду велике и забрињавајуће. Поред осећања депресије и анксиозности која су праћена тугом и бесом, млади који су преживели овакво насиље веома често попуштају са успехом у школи јер нису фокусирани и концентрисани на учење, беже са часова, јер школу више не

---

[464] Lenhart, Amanda: "Data Memo: Cyberbullying and Online Teens", http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf, претражено 03. 10. 2014. године

[465] *Ibid.*

[466] Diamanduros, Terry, Downs, Elizabeth, Jenkins, J.Stephen:"The role of school psychologists in the assessment, prevention and intervention of cyberbullying", Psychology in the Schools, 2008; volume 45(8), http://www.researchgate.net/publication/227828178_The_role_of_school_psychologists_in_the_assessment_prevention_and_intervention_of_cyberbullying, претражено 03. 10. 2014. године, Delmonico, L.David, Griffin, J.Elizabeth:"Cybersex and the e-teen: what marriage and family therapists should know", Journal of Marital and Family Therapy, 2008; volume 34(4), http://www.researchgate.net/publication/23481408_Cybersex_and_the_E-teen_what_marriage_and_family_therapists_should_know, претражено 18. 12. 2014. године

[467] Cassidy, Wanda, Jackson, Margaret, Brown, N.Karen: "Sticks and stones can break my bones, but how can pixels hurt me? Students' experiences with cyber-bullying", School Psychology Internaional, 2009, volume 30(4), http://extension.fullerton.edu/professionaldevelopment/assets/pdf/bullying/sticks_and_stones.pdf, претражено 14. 03. 2015. године

доживљавају као место на коме су сигурни.[468] Самопоуздање постаје проблем и код насилника и код жртве:[469] У истраживању, које је обухватило 2.000 интервјуисаних средњошколаца, констовано је да је жеља за самоубиством била повећана међу онима који су били или насилници или жртве – жртве су 1.9 пута а насилници 1.5 пута склонији мислима о самоубиству у односу на средњошколце који немају везе са интернет булингом.[470]

Посебно забрињава чињеница да се вршњачко насиље на интернету не пријављује или се пријављује веома ретко. Истраживање које је спровела организација Stop cyberbullying[471] показало је да само 5% деце пријави овакав вид насиља родитељима. Већина не пријављује насиље јер се плаши да ће им бити одузет компјутер или мобилни телефон, неки се стиде да кажу шта им се дешава и не желе да се повере родитељима или неком старијем, што је и очекивано ако се узме у обзир да је реч о деци или младим људима. Дете се најчешће повлачи у себе, проводи доста времена за компјутером или одговарајући на поруке на телефону и видно је узнемирено после тога, избегава да разговара о томе шта ради на интернету и због чега доста времена проводи испред компјутера, затвара оно што ради на компјутеру чим неко прође поред екрана, нагло престаје да користи компјутер или мобилни телефон, има проблема са спавањем, има проблеме у школи, не осећа се добро (има главобоље, проблема са стомаком, нерасположено је, депресивно, тужно..), нагло престаје да се дружи са досадашњим пријатељима и сл.[472]

Истраживање које је у Србији спроведено 2012. године међу ученицима нижих разреда основне школе показало је да је 12% испитаних било жртва узнемиравања на интернету, 7% је било жртва снимања мобилним телефоном против своје воље, 7% је било узнемиравано СМС порукама, а 12%

---

[468] Beran, Tanya, Li, Qing:"The relationship between cyberbullying and school bullying", Journal of Student Wellbeing. 2007;volume 1(2), стр. 15-33, http://www.ojs.unisa.edu.au/index.php/JSW/article/viewFile/172/139, претражено 03. 10. 2014. године

[469] Patchin, W. Justin, Hinduja, Sameer:"Cyberbullying and self-esteem", http://www.cyberbullying.us/cyberbullying_and_self_esteem_research_fact_sheet.pdf, претражено 03. 10. 2014. године

[470] Hinduja, Sameer, Patchin, W.Justin:"Bullying, cyberbullying, and suicide", Archive of Suicide Research, 2010; volume 14(3), http://www.tandfonline.com/doi/full/10.1080/13811118.2010.494133#abstract, претражено 03. 10. 2014. године

[471] Stop Cyberbullying, www.stopcyberbullying.org

[472] *Ibid.*

телефонским позивима. Код ученика виших разреда и средњошколаци су сва ова дела била учесталија: 18% испитаних било жртва узнемиравања на интернету, 10% је било жртва снимања мобилним телефоном против своје воље, 19% је било узнемиравано СМС порукама, а 24% телефонским позивима. [473]

У држави Мисури (САД) 2006. године донет је Закон Меган Мајер о превенцији вршњачког насиља на интернету (Х. Р. 1966 - Megan Meier Cyberbullying Prevention Act),[474] који је обухватио вршњачко насиље коришћењем електронских комуникација или телефона. Повод за дошење овог закона је самоубиство Меган Мајер, тинејџерке из Мисурија, која је извршила самоубиство три недеље пре свог четрнаестог рођендана, због лажног представљања и вршњачког насиља на интернету. [475]

3.1.6. Мобинг, сајбер мобинг и манипулација личним подацима са друштвених мрежа који се односе на запошљавање

а) Појам злостављања на раду (мобинга) и мобинга путем интернета.

Научно истраживање злостављања на радном месту почело је крајем осамдесетих година прошлог века и везано је за рад и дело Хајнца Лајмана[476], немачког психолога који је први основао клинику за помоћ жртвама овог облика насиља. Лајман је 1984. године формулисао прву званичну дефиницију злостављања на радном месту или мобинга (енгл. Mobbing*)*. Према његовом схватању „мобинг или психолошки терор на радном месту обухвата одбојно и неетично опхођење које је, по једном утврђеном систему, усмерено од стране једне или више особа најчешће ка једној особи, подесној да буде изложена мобингу, која је стављена у позицију беспомоћности и без могућности да се одбрани и она се држи у тој позицији предузимањем поступака (активности) од стране мобера“.[477] Овај непријатељски или неетички вид комуникације потиче

---

[473] Блиц – дневна новина од 25. 12. 2012. године, www.blic.rs, дневна новина “Блиц” од 25. 12. 2012. године, претражено 25. 12. 2012. године

[474] The Library of Congress, http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1966:, претражено 16. 01. 2015. године

[475] Више о случају Меган Мајер на интернет страни Megan Meier Foundation, http://www.meganmeierfoundation.org/megans-story.html, претражено 03. 01. 2015. године, а видети и Decision of Defendant’s F.R.CRIM. 29(c) Motion, Case UNITED STATES of America, Plaintiff, v. Lori DREW, Defendant. No. CR 08–0582–GW. | Aug. 28, 2009., http://stanford.edu/~jmayer/law696/week1/United%20States%20v.%20Drew.pdf, претражено 03. 01. 2015. године

[476] Heinz Leymann, 1932.-1999.

[477] *Видети:* The Mobbing Encyclopaedia, Bullying; Whistleblowing; The Definition of Mobbing at Workplaces, http://www.leymann.se/English/12100E.HTM, претражено 07. 09. 2012. године

од једне или више особа, систематски је усмерен против појединца у беспомоћној или незаштићеној позицији и који се не може ослободити јер се поступци мобинга непрестано понављају, а која може да резултује пост-трауматским стресним поремећајима.[478]

Мобинг је специфично понашање на радном месту којим особа или група психички (морално) злоставља и понижава другу особу ради угрожавања њеног угледа, части, људског достојанства и интегритета све до елиминације са радног места.[479]

Назив „мобинг" потиче од енглеског глагола „to mob" који може да се преведе као „светина, руља, гомила, насрнути". Лајман је први употребио овај термин како би описао одређена понашања на радном месту,[480] а као његове синониме навео је појмове „bullying", „horizontal violence" или „psychosocial harrassment".[481] Данас, у научној литератури углавном се употребљава термин **„**mobbing**",** земље енглеског говорног подручија користе термин „bullying", а у САД најчешће се среће термин „work abuse".

Када се јавља на радном месту *(*workplace bullying*)* злостављачи су најчешће колеге, сарадници и пословни партнери који међусобно примењују различите методе присиле која нема основу у родној, расној или верској дискриминацији, они шире гласине, различите инсинуације, застрашивања, понижавања и дискредитовање, које за резултат има стварање изолације. Самим тим, мобинг представља емоционални терор групе над јединком, при чему је веома битан елемент мобинга припадност групи - мобинг започиње један

---

[478] Истраживања показују да је процентуално европски просек злостављања на радном месту 9% (у Финској је 15%, Великој Британији и Холандији 14%, док је у Италији и Португалији свега 4% радника изложено психолошком малтретирању на послу).[478] У Србији нема довољно систематског истраживања, али прелиминарна истраживања указују на то да је 43% запослених у Србији било изложено различитим видовима узнемиравања на радном месту у дужем временском периоду.[478] Виктимолошко друштво Србије је, у оквиру Службе ВДС инфо и подршка жртвама у току 2008. године забележило 109 позива због насиља на радном месту и то: 99 се јавило због психичког насиља, 6 због физичког насиља, 3 због сексуалног узнемиравања а 1 особа због сва три облика насиља на радном месту.[478] У току 2009. године, удружењу за заштиту од злостављања на радном месту јавила се за помоћ 1881 жртва мобинга (852 мушкарца и 1029 жена, са подручја Војводине 733 а са подручја Уже Србије 1198 жртава). Удружење "Стоп мобинг", http://mobing.rs/articles.php?article_id=6, претражено 03. 05. 2013. године.

[479] Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна, Костић, Миомира, *op.cit.,* 2009, стр.158

[480] The Mobbing Encyclopaedia, Bullying; Whistleblowing; The Definition of Mobbing at Workplaces, http://www.leymann.se/English/frame.html, претражено 03. 05. 2013. године

[481] *Ibid.*

припадник групе, по правилу онај који има највише предходно потврђеног интегритета у оквиру замишљене или потребне групе.

Злостављање на радном месту се различито дефинише и не постоји једна општеприхваћена дефиниција. Сваки аутор је у оквиру одређивања појма мобинга наводио различите карактеристике понашања мобера или последица које се јављају услед злостављања на радном месту. Поједини аутори мобинг дефинишу и као "емотивни напад који почиње када појединац постане мета неучтивих и штетних понашања кроз алузије, гласине и јавно дискредитовање, непријатељско окружење у коме један појединац окупља друге да вољно или невољно, учествују у сталним злонамерним акцијама које за циљ имају трајно напуштање радног места злостављане особе".[482] Постоје и мишљења да се мобинг обично дешава у радним окружењима која имају лоше организовану производњу и/или методе рада и неспособан или непажљиви менаџмент, и да су најчешће жртве мобинга "изузетни појединци који су показали интелигенцију, стручност, креативност, интегритет, посвећеност и достигнуће".[483]

И поред тога што не постоји универзално прихваћена дефиниција злостављања на раду, сви аутори су углавном сагласни да постоје понашања карактеристична за ову врсту злостављања, попут штетног понашања претпостављеног које је усмерено на подређеног запосленог, понижење и шиканирање, различито етикетирање. Заједнички елементи различитих дефиниција мобинга су одређивање мобинга као: комбинација тактика у којима се користе бројне врсте непријатељске комуникације и понашања,[484] више пута поновљено насилничко понашање, вербално злостављање или понашање које је претеће, понижавајуће, застрашујуће или сплеткарошко које утиче на квалитет посла који се извршава,[485] стално вербално и невербално злостављање на радном месту које се манифестује кроз личне нападе, социјалну неправду и још мноштво других порука које су за жртву болне и доживљавају се као

---

[482] Davenport N.Zanolli, Elliott G.Pursell, Schwartz R. Diestler: "Mobbing, Emotional Abuse in the American Workplace", 3rd Edition 2005, Civil Society Publishing. Ames, IA, http://www.mobbing-usa.com/, претражено 20. 04. 2013. године

[483] *Ibid.*

[484] Tracy, Lutgen-Sandvik, Alberts Nightmares: "Demons and Slaves, Exploring the Painful Metaphors of Workplace Bullying", 2006, Sage Publications - Management Communication Quarterly, 20(2), стр. 152

[485] Workplace Bullying Institute, http://www.workplacebullying.org/individuals/problem/definition/, претражено 20. 04. 2013. године

непријатељске,[486] систематско агресивна комуникација, манипулација и понашања која имају за циљ да некога у радној околини увреде или понизе, која стварају нездрав и непрофесионалан однос снага између злостављача и жртве, а који резултирају психолошким проблемима запослених а огромним новчаним штетама послодаваца.[487]

Активности мобера се одвијају учестало (статистички бар једном недељно), и током дужег периода времена (статистички бар током шест месеци). Због учесталог, дугог трајања непријатељског понашања, временом малтретирање ствара знатну менталну, психосоматску и социјалну патњу. Мобинг је специфичан систем који се састоји од пет доминантних фактора који су у међусобној интеракцији и који зависи од: психолошког профила и особина мобера; корпоративне климе и културе организације; психолошког профила и особина жртве; врсте конфликта који је окидач; и утицаја фактора изван организације попут вредности и норми ширег друштвеног окружења.[488]

У литератури се злостављање на радном месту коришћењем интернета и друштвених мрежа не дефинише посебно, тако да се може рећи да све што се односи на мобинг уопште важи и за интернет мобинг, с тим што се ова врста мобинга одвија преко интернета, односно друштвених мрежа. Друштвене мреже представљају погодно место за подстицање групне мржње у оквиру радног окружења, 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. Путем e-mailova или sms порука запосленима се упућују непристојне поруке, дискриминаторне поруке, поруке мржње, претње и сл.[489] како би се повредио њихов углед, част, достојанство и

---

[486] Lutgen-Sandvik, Pamela: "Take This Job and ... : Quitting and Other Forms of Resistance to Workplace Bullying", Routledge, Communication Monographs, Vol. 73, No. 4, December 2006, стр. 408

[487] Mattice, M.Catherine: "Proactive Solutions for Workplace Bullying: Looking at the Benefits of Positive Psychology", 2010., http://www.thefreelibrary.com/Helping+targets+%26+their+employers+effectively+resolve+workplace...-a0263658932, претражено 03. 05. 2013. године

[488] Барјактаровић, С.: „Главни актери мобинга и њихове карактеристике", према Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна, Костић, Миомира, 2012, стр. 159.

[489] Bowie, Vaughan, Fisher, S. Bonnie, Cooper, Cary: „Workplace Violence**",** Routledge, 2012, https://books.google.si/books?hl=sr&lr=&id=OmkQBAAAQBAJ&oi=fnd&pg=PA248&dq=cyber+wo

интегритет или како би били елиминисани са радног места. Такође је могућа манипулација личним подацима са интернета који се односе на запошљавање, када послодавци приликом избора лица које ће запослити проверавају кандидате претраживањем друштвених мрежа.[490]

б) Основна обележја мобера путем интернета и жртава. Мобери путем интернета имају основне карактеристике као и остали мобери ван виртуелног света. Велики број психолога тврди да су злостављачи (мобери) особе с извесним психолошким поремећајем личности. Они су мање способни, без капацитета за љубав, радост, игру, креативност, давање и дељење, најчешће не помажу никоме, особама са којима раде не приступају пријатељски, нису продуктивни и имају негативан став према животу уопште.

Ове особе мобингом прикривају немоћ у некој другој сфери свога живота, формирајући око себе групу у којој доказују своју моћ и важност на рачун жртве. Често се злостављачи осећају подређено, а злостављање других чине из страха да неће бити цењени, због болесне љубоморе, неостварених циљева или страха да ће и сами некоме постати жртва. Циљ им је да фрустрирају и застрашују сараднике око себе ароганцијом и играма моћи, делују деструктивно и непријатељски, желе да у сваком моменту контролишу ситуацију, па зато манипулишу и мудрују, никада се не извињавају за своја понашања. Код појединих мобера испољава се намера да нашкоде другоме или да га присиле да напусти радну средину. То чине кад се осећају угрожено или у ситуацијама кад постоји нпр. вишак радне снаге. У кризним временима неких

---

rkplaceviolence+&ots=0VUnUUGL2Q&sig=p4519veMQ5-z3k5gt9SpzoMqdQk&redir_esc=y#v=onepage&q=cyber%20workplaceviolence&f=false, претражено 12. 08. 2015. године

[490] С обзиром на то да мобинг путем интернета још увек нема одговарајућу законску регулативу и да је откривање овог облика злостављања веома тешко, ради провере постојања мобинга путем интернета могуће је запосленима поставити следећа питања: да ли имате профил на некој друштвеној мрежи; да ли често са радног места користите интернет и приступате разним друштвеним мрежама и форумума; да ли сте у некој групи на интернету (друштвеној мрежи) која почиње са 'Мрзим..' или слично; да ли сте некада добили неку нежељену поруку на мобилном, на е-маил или на ћаскању од особе са којом радите; да ли сте одсуствали са посла због тих нежељених порука; да ли је нека од особа са којима радите објавила неку неистину о вама на „ћаскањима", блогу или интернет страници; да ли вас неко од особа са којом радите исмејава због говора, држања, хода, одевања, пола, националности, порекла, приватног живота и слично на „ћаскањима", блогу или интернет страници; да ли због оваквог понашања других размишљате о промени радног места; да ли се о вама путем интернета – друштвене мреже или смс порука шире непроверене гласине, клевете или сексуалне интриге на радном месту; да ли је неко од особа са којима радите другим колегама и колегиницама слао поруке а потписао ваше име и сл.

фирми „жртвено јагње" се бира због унутрашњих проблема и напетости, па на њему сви сами себи доказују да су снажнији и способнији.[491]

Формирању личности мобера погодују одређени типови личности, као што су: *нарцисоидни тип личности* (независтан тип, није га лако застрашити, а карактерише га велика количина агресије, немогућност ступања у истинске и садржајне односе с другим људима, настоје да намећу своју вољу и своје проблеме, а могу бити трајно задовољне само са сарадницима који се потпуно жртвују за њих, не очекујући адекватно узвраћање; *манипулативни тип личности* (особе које желе да контролишу и усмеравају сараднике тако да служе њиховим циљевима, а не својим властитим; немају емоције за друге људе већ их посматрају искључиво као објекте са којима се може лако руковати; њихова тактика се састоји у томе да код жртве створе уверење да су јој наклоњени како би је потом искористили за своје циљеве), *деструктивни тип личности* (испољава тежњу да се други повреде или да се униште; ова тежња поприма веома разноврсне облике, од вербалне агресије до директног напада), *доминантан тип личности* (настоји да контролише понашање других и да га усмерава у складу са својим потребама и жељама; жели да наређује другима и да има власт, као и да одређује активности других људи у оквиру групе чији је он члан, веома ниско вреднује друге а себе прецењује), *антидемократски тип личности* (има највеће предиспозиције за изградњу особина које поседује личност „мобера", јер нема афинитете за прихватање демократских принципа функционисања друштва). [492]

За разлику од злостављача, жртве мобинга обично имају мањак самопоуздања и нису јаке и утицајне у средини у којој раде. Као најчешће жртве мобинга јављају се особе које су уочиле и пријавиле неправилности у раду послодавца, особе са инвалидитетом, млади тек запослени радници, старији запослени који су пред пензијом, особе које траже више самосталности у раду или боље услове за рад, радници запослени на одређено време, запослени који представљају вишак радне снаге, као и запослени који припадају различитим мањинским групама у друштву. Често болесне особе могу да буду жртве

[491] Катић, С.: „Психолошке карактеристике мобера", према Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна, Костић, Миомира, 2012. стр. 161.
[492] Удружење "Стоп мобинг" - Ко су мобери, , www.mobing.rs, претражено 07. 05. 2013. године

мобинга и незадовољства послодавца, због честих боловања услед погоршања здравственог стања.

Свака жртва злостављања реагује на различит начин, али се неке реакције ипак могу навести као типичне. Већина жртава најпре пролази кроз фазу почетног самоокривљивања када мисли да је она нешто скривила и да је одговорна за насталу ситуацију. У овој фази код жртве су доминантна осећања збуњености и страха (анксиозности). Како време пролази а злостављање не престаје, жртва почиње да се осећа усамљено, одбачено и посрамљено, претпоставља да јој колеге не верују па због тога не говори о свом проблему и повлачи се у себе. Уколико се и осмели да о свом проблему прича, жртва најчешће наилази на неодобравање и неверицу (тзв. двоструки мобинг). У овој фази, поред анксиозности код жртве се опажа и депресивно понашање. Као последица депресије жртва почиње да обезвређује саму себе, јер је оптерећена мислима попут сопствене неприлагођености, неспособности и осећаја мање вредности од других сарадника из радне околине. Жртва је у страху да уопште започне да се брани јер се плаши да не изгуби посао и не буде предмет јавне осуде колектива.

Иако су описана понашања посебно карактеристична за жртве мобинга ван виртуелног света, исто се може очекивати и код жртава интернет мобинга. Ипак, постоје и жртве које се боре против својих злостављача, у циљу блокаде и елиминације мобинга који се над њима спроводи. Овакво пружање отпора злостављању је карактеристично за јаке, интелигентне особе, које су свесне да су жртве интернет мобинга и које су спремне да користе сва расположива законска, психолошка, медијска и друга средства како би скренули пажњу јавног мњења да се ради о мобингу.

Све последице које мобинг и мобинг путем интернета могу да изазову код жртве обухватају: *промене на телесном, здравственом нивоу* (хронични умор, честе главобоље, сметње са пробавом, осећај притискања у грудима, губитак равнотеже праћен вртоглавицом, повећање или смањење телесне тежине, различити болни синдроми, срчане потешкоће, осипи по кожи, смањени имунитет); *промене на социјалном и емоционалном нивоу* (психички поремећаји попут депресивних понашања и честих промена расположења, осећање емоционалне празнине, стално размишљање о проблему, осећају губитка животног смисла и анксиозности, напади панике, социјална изолација, суицидно

понашање, губитак мотивације и ентузијазма, несаница, повећана потреба за алкохолом, седативима и цигаретама); *промене у понашању* (губитак концентрације, заборавност, грубост, стварање породичних проблема).

в) Манипулација личним подацима са друштвених мрежа који се односе на запошљавање. Један од веома честих облика испољавања интернет мобинга је манипулација личним подацима који се налазе на интернету, запослених и незапослених лица која траже посао, од стране послодаваца. Још 2008. године CareerBuilder.com је на основу истраживања у које је било укључено 31.000 послодаваца проценио да један од пет послодаваца користи друштвене мреже у намери да провери потенцијале кандидате за посао.[493] Међутим, како и запослена лица користе друштвене мреже, 2009. године је забележен случај да је Кимберли Свон отпуштена из компаније Ivell Marketing and Logistics Limited због тога што је на друштвеној мрежи окарактерисала свој посао као „досадан".[494] Послодавци користе друштвене мреже за проверавање својих запослених, па тако врше индиректни мобинг посредством компјутерских технологија и друштвених мрежа: 41% проверава да ли користе алкохол и наркотике, 40% да ли има неадекватних фотографија, 29% обраћа пажњу на вештине комуникације, 22% на корисничко име које користе на мрежи, 21% на криминално понашање, 19% на одавање професионалних тајни претходних послодаваца.[495]

Према извештају сигурносне фирме Sophos[496] један од најбитнијих разлога због кога послодавци забрањују запосленима да друштвеним мрежама приступају са радног места је тај што сматрају да овакво понашање не само да доводи до пада продуктивности, већ да се на овај начин у рачунарске системе послодаваца уносе злонамерни програми који се налазе на друштвеним мрежама помоћу којих је могуће откривати осетљиве личне податке о

---

[493] Havenstein, Heather: "One in five employers uses social networks in hiring process", 2008, http://www.computerworld.com/s/article/9114560/One_in_five_employers_uses_social_networks_in_hiring_process, претражено 29. 04. 2013. године

[494] News. 2009: "Sacked for Calling Job Boring on Facebook", http://news.sky.com/skynews/Home/UK-News/Facebook-Sacking-Kimberley-Swann-From-Clacton-Essex-Sacked-For-Calling-Job-Boring/Article/200902415230508Sky, претражено 29. 04. 2013. године

[495] *Ibid.*

[496] Facebook: A new battleground for cyber-crime, http://www.euractiv.com/infosociety/facebook-new-battleground-cyber-news-222406, претражено 29. 04. 2013. године

запосленима као и поверљиве пословне податке непознатим људима.[497] Овим истраживањем је обухваћено преко 500 послодаваца. Укупно 72% испитаних послодаваца је изјавило да је забринуто да овакво понашање запослених када су у питању друштвене мреже излаже целокупно њихово пословање ризику омогућавајући да поверљиви подаци стигну у погрешне руке.[498] Као друштвене мреже које су окарактерисане као најризичније препознате су Facebook (60% испитаних послодаваца), MySpace (18%), Twitter (17%) и LinkedIn (4%).[499]

Ипак, извесна граница још увек постоји - ако послодавац користи друштвену мрежу да провери кандидата за посао и онда одбаци ту особу на основу онога што је видео, могуће је да ће бити оптужен за дискриминацију.[500] Према вести коју је пренео интернет портал *www.workforce.com*[501] који је специјализован за помагање кадровским службама у регрутовању потенцијалних кандидата за посао, послодавци који се ослањају искључиво на податке друштвених мрежа (посебно Facebook) о друштвеним активностима кандидата како би проценили квалитете кандидата, понашају се дискриминаторски и могу да буду кажњени високим новчаним казнама. Оваква врста провере и етикетирања поистовећује се са дискриминацијом на националној, сексуалној, родној, политичкој припадности одређеним групама, па као таква не може бити релевантна за заснивање радног односа. На овом порталу постоје подаци да је у току октобра 2007. године 44% послодаваца користило друштвене мреже како би проверили кандидате који су аплицирали за посао, док је 39% послодавца на друштвеним мрежама проверавало профиле својих запослених.[502]

г) Начини за супротстављање интернет мобингу. Злостављање на радном месту коришћењем интернета и друштвених мрежа представља значајну претњу за здравље, безбедност и добробит људи на радном месту, а може да има и последице на послодавца, укључујући смањену профитабилност, низак морал

---

[497] *Ibid.*
[498] Facebook, Twitter users vulnerable to cyber crimes, http://www.thehindu.com/sci-tech/internet/article99159.ece, претражено 29. 04. 2013. године
[499] *Ibid.*
[500] Bowers, Toni: "Employers who check out job candidates on MySpace could be legally liable", 2008, http://www.techrepublic.com/blog/career/employers-who-check-out-job-candidates-on-myspace-could-be-legally-liable/338, претражено 29. 04. 2013. године
[501] Work force, www.workforce.com, претражено 29. 04. 2013. године
[502] *Ibid.*

и повећање флуктуације кадрова. Последице нехуманог мобинг понашања могу бити катастрофалне и разорне за саму особу, њено здравље и породицу, али и за друштво у целини. Указивање на механизме настанка и последице злостављања на радном месту, као и препознавање фактора и околности које могу да доведу до ове врсте насиља, поготово ако је злостављање на радном месту повезано са другим видовима насиља, веома је важно за превентивно деловање.

Превенција злостављања на раду коришћењем интернета и друштвених мрежа, као и превенција злостављања на раду уопште, може бити организована на три нивоа: примарна, секундарна и терцијална превенција. [503]

Примарна превенција је најважнија за смањење појаве злостављања на раду и мобинга коришћењем интернета и друштвених мрежа. Она се спроводи када до злостављања још увек није дошло и обухвата едукацију свих фактора у процесу рада – послодаваца, запослених, синдикалних активиста и судија. Примарна превенција се постиже такође законима које регулишу радне односе и злостављање на раду. За разлику од злостављања на раду које је забрањено посебним законима,[504] у већини земаља не постоје посебни законски прописи којима се регулише мобинг путем интернета и друштвених мрежа. Тако се може претпоставити да се за овај облик злостављања на раду примењују исти законски прописи као за мобинг уопште. Иста је ситуација у Србији[505] јер се у

---

[503] Костелић Мартић, Андреја: „Мобинг: психичко малтретирање на радном месту", Школска књига, Загреб, 2005.

[504] Посебни закони којима се регулише злостављање на радном месту постоје у Француској, Шведској, Норвешкој, Данској, Финској, Белгији и Швајцарској, а на новоу Европске уније Европски парламент 2001. године донео је Резолуцију бр. 2339 о злостављању на радном месту. European Parliament resolution on harassment at the workplace (2001/2339(INI)), A5-0283/2001, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:077E:0138:0141:EN:PDF, претражено 03. 05. 2013. године

[505] Пре доношења Закона о спречавању злостављања на раду, прва правоснажна пресуда која се односила на мобинг донета је у Србији 2008. године, Општински суд у Јагодини осудио је на 4 месеца затвора условно за 2 године в.д.главног и одговорног уредника недељника „Нови пут" због кривичног дела злостављања и мучења из чл. 137 КЗ РС. Уредник је осуђен за наведено кривично дело по кривичној пријави новинарке тог листа. *Видети:* www.nuns.rs/ info/news/9672/PRVA-PRESUDA-ZA-MOBNG html, претражено 05. 05. 2013. године.

После доношења Закона о спречавању злостављања на раду прву правоснажну пресуду за злостављање на раду на универзитетима у Србији по тужби за мобинг донео је 2012. године Основни суд у Новом Саду. Пресудом је професор етике обавезан да плати новчану казну оштећеном асистенту кога је спречавао да обавља своје радне дужности, слао му претеће и увредљиве смс поруке и на други начин вређао његову част и углед и уцењивао да гласа за избацивање других колега са факултета. *Видети:* Прва пресуда за мобинг: професор злостављао асистента,
http://www.vesti-online.com/Vesti/Hronika/279839/Prva-presuda-za-mobing-Profesor-zlostavljao-asistenta, претражено 05. 05. 2013. године.

Закону о спречавању злостављања на раду не помиње мобинг путем интернета и друштвених мрежа као облик злостављања на раду.[506] Кривично дело злостављања на раду није предвишено Кривичним закоником Републике Србије, али се може у тим случајевима применити чл. 137 КЗ, који се односи на злостављање и мучење. Овим чланом (ст. 1) предвиђено је кажњавање казном затвора онога који злоставља другог или према њему поступа на начин којим се вређа људско достојанство. Тежи облик постоји када неко применом силе, претње или на други недозвољен начин другоме нанесе велики бол или тешке патње с циљем да од њега или трећег лица добије признање, исказ или друго обавештење или да се он или неко треће лице застраши или незаконито казни или то учини из друге побуде заснованом на било каквом облику дискриминације. Извршилац оба облика овог кривичног дела може да буде службено лице у вршењу службе (ст. 3).

Према тексту Закона о спречавању злостављања на раду, злостављање представља свако активно или пасивно понашање према запосленом или групи запослених код послодавца које се понавља, а које за циљ има или представља повреду достојанства, угледа, личног и професионалног интегритета, здравља, положаја запосленог и које изазива страх или ствара непријатељско, понижавајуће или увредљиво окружење, погоршава услове рада или доводи до тога да се запослени изолује или наведе да на сопствену иницијативу раскине радни однос или откаже уговор о раду или други уговор. Законски појам злостављања обухвата и подстицање или навођење других на вршење било које описане активности. Извршилац злостављања може да буде послодавац са својством физичког лица или одговорно лице код послодавца са својством правног лица, запослени или група запослених код послодавца (чл. 6).[507]

---

[506] Закон о спречавању злостављања на раду ("Сл. гласник РС", бр. 36/2010) почео је да се примењује 04. 09. 2010. године. Доношење овог закона Србију сврстава у ред земаља које путем законског регулисања покушавају да реше проблем злостављања на раду, имајући у виду чињеницу да преко 50% пријављених случајева злостављања јесу управо злостављања на радном месту. Удружење "Стоп мобинг", http://www.mobing.rs/news.php, претражено 03. 05. 2013. године.

[507] Закон о спречавању злостављања на раду предвиђа обавезу послодавца да запосленог пре ступања на рад писменим путем обавести о забрани злостављања, о правима, обавезама и одговорностима запосленог и послодавца у вези са забраном злостављања. Постоје две врсте злостављања на раду према томе ко врши злостављање. Тако, злостављање на раду могу да врше запослени који су међу собом једнаки или га може вршити послодавац према запосленима. Уколико запослени сматра да га други запослени злоставља на радном месту подноси

Наведена одредба Закона о злостављању на раду може да се односи и на интернет мобинг, док се посебним законом и посебним одредбама у постојећем закону не предвиди овај облик злостављања на раду.

Поред Закона о злостављању на раду треба поменути и Правилник **о** правилима понашања послодаваца и запослених у вези са превенцијом и заштитом од злостављања на раду,[508] који поред злостављања дефинише сексуално узнемиравање, као свако вербално, невербално или физичко понашање које има за циљ или представља повреду достојанства запосленог у сфери полног живота, а које изазива страх или ствара непријатељско, понижавајуће или увредљиво окружење (чл. 11 ст. 3). У Правилнику су дате препоруке којих се понашања треба уздржавати у циљу коректне пословне комуникације између сарадника: понашања која се односе на немогућност одговарајућег комуницирања, која могу да доведу до нарушавања добрих међуљудских односа, нарушавања угледа и професионалног интегритета запосленог, до нарушавања здравља запосленог и понашања која се могу сматрати сексуалним злостављањем. Одредбе овог Правилника могу се у недостатку одговарајућих прописа применити приликом извршења интернет мобинга.

Секундарна превенција се спроводи кад је већ уочена појава злостављања на раду. Веома важну улогу имају саветници од поверења и посредници

послодавцу захтев за покретање поступка за заштиту, а обавеза послодавца је да у року од три дана од пријема овог захтева странама у спору предложи мирно решавање спора и избор посредника са листе Агенције за мирно решавање спорова. Ако се за злостављање терети послодавац, запослени може поднети захтев за заштиту или непосредно послодавцу или може покренути поступак пред надлежним судом до истека застарелости рока за покретање поступка за заштиту од злостављања, који износи шест месеци од дана када је злостављање учињено. У оба случаја, уколико поступак посредовања не успе и не дође до споразума, запослени који сматра да је дошло до злостављања може да покрене судски поступак заштите. Судски поступак је хитан, терет доказивања је на послодавцу, а запосленом који тражи заштиту се не може отказати уговор о раду или се ставити у неповољнији положај у погледу остваривања права и обавеза по основу рада. За запослене који врше злостављање предвиђене су следеће мере: опомена, удаљење са рада од 4 до 30 дана без накнаде зараде, мера трајног премештаја у другу радну околину или, ако се у наредних шест месеци понови злостављење, отказ уговора о раду. За послодавце су предвиђене прекршајне новчане казне: казне за послодавце у својству правног лица се крећу од 100.000 до 800.000 динара у зависности од прекршаја, за предузетнике од 10.000 до 400.000 динара, док су казне за одговорно лице у правном лицу од 5.000 до 40.000 динара.

[508] Правилник о правилима понашања послодаваца и запослених у вези са превенцијом и заштитом од злостављања на раду ("Сл. гласник РС", бр. 62/2010)

(медијатори). Суштина је да се стране које су у спору укључе у процес преговарања о начину превазилажења проблема који је настао.

Терцијарна превенција подразумева помоћ жртви мобинга да што брже поновно успостави психофизичко здравље и поврати уништено достојанство. Веома је важна рана дијагноза утицаја мобинга на здравље јер се тако може помоћи у смањивању последица на индивидуалном, породичном и социјалном нивоу.

Много је примера и корисника друштвених мрежа који су због свог виртуелног понашања или објава изгубили посао или били избачени из школе коју су похађали. Један од најочигледнијих примера кршења приватности и дискриминације учињен је према студенту Мајклу Гину (22) који је због своје слике у хаљини коју је објавио на друштвеној мрежи Facebook у уверењу да ће је видети само његови пријатељи избачен са колеџа који је похађао. Гин, који је хомосексуалац, избачен је из школе уз образложење да његов виртуелни живот у коме он поставља слике, прича о својим момцима и клубовима које посећује представљају грубо кршење правила понашања које кампус има. (Kornblum, Janet, Marklein, Mary Beth: „What you say online could haunt you“, USA Today, 2006, http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm, претражено 23. 08. 2014. године)

У аустријској покрајини Тирол, три раднице су моментално добиле отказ пошто су преко друштвене мреже Facebook изразиле своје незадовољство на послу и незадовољство својим односом са претпостављеним. Једна од њих је на свом профилу изразила своје незадовољство именујући свог претпостављеног, док су друге две колегинице ту објаву потврдиле притиском на дугме „Свиђа ми се“. Иако шеф кога су поменула није имао много пријатеља преко ове друштвене мреже, он је сазнао за ову објаву и моментално уручио отказ овим запосленим женама. (*Видети*: Дилигенски, Андреј, Прља, Драган, *op.cit.*, 2014, стр. 87)

Једна конобарица из Аустрије је добила отказ због објављивања слика из ноћног провода на друштвеној мрежи Facebook које су сликане у време када је била на боловању. Она је отворила боловање, али је непосредно пре истека боловања отишла у дискотеку, а затим на свој профил поставила слике са коментарима „како алкохол убија и како неће више никада излазити“. За Привредну комору покрајине Доња Аустрија ово је свакако био оправдан разлог за давање отказа, пошто представља злоупотребу права на боловање. (*Видети*: Дилигенски, Андреј, Прља, Драган, *op.cit.*, 2014, стр. 88)

3.1.7. Говор мржње на друштвеним мрежама

Интернет и друштвене мреже се дефинишу као медији ослобођени од било каквих утицаја државе и традиционалних норми. Једнаке могућности приступа и изражавања односе се на све кориснике интернета и друштвених мрежа, што значи да корисници сами креирају садржаје користећи се притом неограниченим бројем извора који су им доступни. На тај начин интернет постаје платформа за саопштавање и размењивање идеја, друштвених, културних и политичких вредности, изражавање мишљења и ставова, промовисање активизма.

Слобода изражавања је призната као људско право у чл. 19 Универзалне декларације о људским правима и она је постојала и пре појаве интернета. Она је пропорционална нивоу демократије друштва и уско повезана са слободним медијима, међу којима је и интернет, који су обавезни да грађанима пруже информације како би били функционални у друштву. Основни постулат у демократском друштву је успостављање баланса између права на слободу изражавања и других гарантованих права, као што су право на слободу мисли, савести и вероисповести или право на слободу од дискриминације. Због тога слобода изражавања на интернету има одређена ограничења јер подразумева да је интернет слободан од свих девијантних понашања, међу којима је говор мржње, којим се подстиче дискриминација, мржња или насиље против лица или групе лица због њихових личних својстава.

Иако је крајем 80-тих и током 90-тих година израз „говор мржње" ушао у широку примену, не постоји универзално прихваћена дефиниција самог појма „говор мржње". У литератури се као говор мржње квалификују изјаве које застрашују, вређају или узнемиравају појединце или групе и/или изјаве које позивају на насиље, мржњу или дискриминацију појединаца или група. У недостатку прецизне дефиниције говора мржње, може се користити пракса Европског суда за људска права, који термин „говор мржње" користи да опише облике изражавања *који шире, подстичу, промовишу или оправдавају мржњу засновану на нетрпељивости, укључујући и верску нетрпељивост*. Према схватању овог суда, говор мржње обухвата подстицање расне мржње и мржње на верској основи, са којом се изједначава и подстрекивање на мржњу на основу разлике између верујућих и неверујућих, као и подстицање на друге облике

мржње засноване на нетолеранцији, укључујући и агресивни национализам и етноцентризам. Поред тога, и хомофобични говор спада у категорију говора мржње. Говор мржње се недавно проширио и на родну нетолеранцију и ону засновану на сексуалној оријентацији, али и на нетолеранцију различитих политичких мишљења и националног и друштвеног статуса.

Другу дефиницију говора мржње која је у широј употреби дао је Комитет министара Већа Европе 1997. године. Према овој дефиницији „говор мржње подразумева све облике изражавања који шире, подстичу, промовишу или оправдавају међурасну мржњу, ксенофобију, антисемитизам или мржњу базирану на интолеранцији, укључујући и интолеранцију изражену кроз агресивни национализам или етноцентризам, дискриминацију или анимозитет према мањинама, мигрантима или људима имигрантског порекла.[509]

Говор мржње манифестује се јавним изражавањем дискриминаторских ставова путем графита, истицања порука или симбола дискриминаторне садржине, на јавним скуповима, спортским и другим јавним манифестацијама и догађајима и сл. Говор мржње представљају речи, изрази и реченице који су увредљивог садржаја, а упућене су појединцу или групи због припадности одређеној раси, нацији, вери, идеологији, сексуалном опредељењу или другом личном својству, које стигматизују, етикетирају, клевећу, повређују или исмевају одређену друштвену групу и понижавају особу која припада тој групи. Разликује се директан (изношење непроверених тврдњи, констатација и судова, употреба псовки и вулгарне лексике), индиректан (квазизакључивање са позивањем на ауторитет и извор, савети изречени квазипријатељским тоном, констатације које имитирају новинарски стил извештавања, жаргонском лексиком и антипословицама) и латентан говор мржње (нема експлицитних констатација, наизглед духовити коментари, игре речи).

На међународном нивоу говор треба поменути Међународну конвенцију за превенцију свих облика расне дискриминације,[510] коју је генерална скупштина УН усвојила 1965. године и која представља први међународни

[509] Слобода на интернету и говор мржње online: медијска политика и интернет у БИХ, Internews u BIH, Sarajevo, 2014, http://internews.ba/sites/default/files/resursi/Govor%20mrznje%20na%20internetu.pdf, претражено 02. 12. 2015. године

[510] Међународна конвенција за превенцију свих облика расне дискриминације („Службени лист СФРЈ“ бр. 6/1967)

споразум о говору мржње. Међународни пакт о грађанским и политичким правима (ICCPR) који је ступио на снагу 1976. године,[511] предвиђа да је законом забрањено свако заговарање националне, расне или међуверске мржње које садржи позивање на дискриминацију, непријатељство или насиље. Дефиниција говора мржње дата је и у Препоруци бр.P(97)20 Комитета министара државама чланицама (30. 09. 1997.): израз „говор мржње“ подразумева све облике изражавања који шире, распирују, подстичу или правдају расну мржњу, ксенофобију, антисемитизам или друге облике мржње засноване на нетолеранцији, укључујући и нетолернацију изражену у форми агресивног национализма и етноцентризма, дискриминације и непријатељства према мањинама, мигрантима и људима имигрантског порекла.[512] На регионалном нивоу, Европска конвенција о људским правима и Америчка конвенција о људским правима гарантују право на слободу изражавања, али не изричу посебну забрану говора мржње. Посебно је значајан Додатни протокол Конвенције о високотехнолошком криминалу, који обавезује државе чланице да у домаћем закону усвоје законодавне и друге мере који говор мржње online предвиђају као кривично дело.

У Републици Србији прописи који су релевантни за сузбијање говора мржње налазе се у Уставу Србије и у низу закона. Устав Србије гарантује слободу изражавања мишљења и прописује услове под којима се она може ограничити (чл. 46). Уставом је гарантована и слобода медија (чл. 50) и услови под којима се може спречити ширење информација и идеја путем средстава јавног обавештавања. Такође, изричито је забрањено изазивање и подстицање расне, националне, верске или друге неравноправности, мржње и нетрпељивости (чл. 49), као и свака дискриминација, непосредна или посредна, по било ком основу, а нарочито по основу расе, пола, националне припадности, друштвеног порекла, рођења, вероисповести, политичког или другог уверења, имовног стања, културе, језика, старости и психичког или физичког инвалидитета (чл. 21. ст. 3). Закон о забрани дискриминације дефинише говор

[511] Међународни пакт о грађанским и политичким правима (ICCPR) који је ступио на снагу 1976. године („Службени лист СФРЈ“ бр. 7/1971)

[512] Препорука бр. P(97)20 Комитета министара државама чланицама (30. 09. 1997.), www.coe.int/t/dghl/standardsetting/media/doc/translations/serbian/Rec(1997)o2o&ExpMem_sb.pdf , претражено 02. 12. 2012. године

мржње као *изражавање идеја, информација и мишљења којима се подстиче дискриминација, мржња или насиље против лица или групе лица због њиховог личног својства, у јавним гласилима и другим публикацијама, на скуповима и местима доступним јавности, исписивањем и приказивањем порука или симбола и на други начин* (чл. 11). Говор мржње у медијима забрањен је Законом о јавном информисању (чл. 38), тако што је изричито забрањено је *објављивање идеја, информација и мишљења којима се подстиче дискриминација, мржња или насиље против лица или групе лица због њиховог припадања или неприпадања некој раси, вери, нацији, етничкој групи, полу или због њихове сексуалне опредељености, без обзира на то да ли је објављивањем учињено кривично дело*. У чл 10 Закона о сузбијању дискриминације особа са инвалидитетом прописано је да је *забрањено* [је] *исписивање и истицање на јавним местима и ширење на други начин порука и симбола којима се позива на дискриминаторско поступање према особама са инвалидитетом.*

У Кривичном законику Републике Србије говор мржње на интернету и друштвеним мрежама није предвиђен као посебно кривично дело. У оквиру Главе XVII (Кривична дела против части и угледа) предвиђено је кривично дело повреда угледа због расне, верске, националне и друге припадности (чл. 174). Радња кривичног дела се састоји у јавном излагању порузи лица или групе због припадности одређеној раси, боји коже, вери, националности, етничког порекла или неког другог својства. Друго кривично дело је изазивање националне, расне и верске мржње и нетрпељивости (чл. 317 КЗ – Глава XXVII Кривична дела против уставног уређења и безбедности Републике Србије) којим је предвиђено кажњавање лица које изазива националну, расну или верску мржњу или нетрпељивост међу народима или етничким заједницама које живе у Србији. Квалификовани облик овог кривичног дела постоји када је дело учињено принудом, злостављањем, угрожавањем сигурности, излагањем порузи национаних, етничких или верских симбола, оштећењем туђе ствари, скрнављењем споменика, спомен обележја или гробова. Најтежи облик постоји када се кривично дело врши злоупотребом службеног положаја или овлашћења ли ако је услед тих дела дошло до нереда, насиља или других тешких последица за заједнички живот народа, националних мањина или етничких група у Србији.

Говор мржње има одређене последице које се састоје у изазивању страха, зебње, нелагоде или љутње. Конкретне последице се могу састојати у стварању

презира, негативних стереотипа према одређеном лицу или групи, стварању негативног стереотипа према одређеном лицу односно групи, подстицање дискриминације и непријатељства, осуду околине, изазивању осећања несигурности и страха код припадника одређене групе, у стварању осећаја код великог броја грађана да је такво понашање према припадницима одређене групе друштвено пожељно и оправдано, да ће бити толерисано и да неће бити предмет одговорности.

Интернет и друштвене мреже представљају веома погодно средство за изазивање националне, расне и верске мржње. Вређање, исмејавање, потцењивање националних, расних или верских осећања и други начини испољавање говора мржње на веб сајтовима или блоговима преносе се неограниченом броју људи, што доприноси изазивању или распиривању мржње. Извршилац може да буде једно лице, али најчешће су то групе и организације које управо имају за циљ стварање националне, расне и верске мржње и нетрпељивости. Један од најпознатијих интернет форума који распирује говор мржње је „Стормфронт“ интернет форум беле националистичке заједнице која заступа теорију о супериорности беле расе.[513] Виши суд у Београду је 2012. године донео пресуду којом је осудио Симу Владичића због претњи упућених припадницима ЛБГТ популације на Фејсбук групи „500.000 Срба против геј параде“ за кривично дело угрожавања сигурности на казну затвора у трајању од три месеца условно за две године. Сматра се да је ово прва пресуда у Србији којом је изречена санкција за претње мотивисане мржњом.[514]

Центар за нове медије „Либер” спровео је истраживање у циљу разумевања говора мржње и дијалога којим су се твитераши из Србије укључили у online расправу током „Афере пиштољ“ чији је главни актер и покретач био Драган Вучићевић, уредник новина Информер, а мета заштитник грађана Саша Јанковић.[515] Истраживање је показало да је, на основу начина на

---

[513] Николић Комлен, Лидија, Гвозденовић, Радоје, Радуловић, Саша, Милосављевић, Александар, Јерковић, Ранко, Живковић, Владан, Живановић, Саша, Рељановић Марио; Алексић Иван: „Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу“, *op.cit.,* 2010, стр. 127

[514] Блиц – дневна новина, www.blic.rs/vesti/hronika/presuda-zbog-govora-mrznje-na-internetu/Ig3etnz претражено 02. 12. 2015. године

[515] „Afera pištolj” i govor mržnje na internetu (“Affair gun” and hate speech on Twitter), Novi media centar „Liber“, http://www.blogopen.rs/afera-pistolj-i-govor-mrznje-na-tviteru-prema-kihot_ex_of-djvucicevic-istrazivanje/, претражено 05. 12. 2015. године

који су се твитераши обраћали Саши Јанковићу, он био жртва организованог групног сајбер злостављања. Истраживање, које је обухватило 6.034 оригиналних твитова, пружило је могућност да се боље изучи расположење јавности, активност јавности на одређену тему, важност акције и реакције на дијаог, развој јавног дигиталног дискурса и учешће говорног чина увреде и директног и индиректног говора мржње када је јавност посебно заинтересана за осетљиву тему. Твитове је написало 2.609 твитераша у периоду од 1 - 21. маја 2015. године. У говору мржње који се односи на Сашу Јанковића, директан говор мржње, који преовлађује, постигнут је изношењем непроверених судова као чињеница, изношењем квалификација као констатација, употребом псовки и вулгарне лексике, квазизакључивањима са позивањем на ауторитет.

Треба напоменути да је Министарство правде Немачке постигло договор са интернет компанијама Facebook, Google и Twitter да говор мржње убудуће буде уклоњен са сајтова у року од 24 часа. У заједничком саопштењу наведено је да ће на овај начин корисници и антирасистичке групе моћи лакше да маркирају говор мржње. Садржај портала ће испитивати тимови стручњака, који ће, после пажљивог прегледа, за један дан уклонити сајтове који садрже говор мржње.[516]

3.1.8. Преваре путем интернета – појам и појавни облици

Преваре путем интернета представљају најраширенији облик сајбер криминалитета. Треба их разликовати од *рачунарских превара* када се у рачунар уносе нетачни подаци или се пропушта уношење тачних података или се на било који други начин рачунар користи за остваривање преваре путем прикривања или лажног приказа података, а све у циљу стицања противправне материјалне користи којом се другоме проузрокује имовинска штета. Превара путем интернета није увек и обавезно рачунарска превара јер неке интернет преваре одговарају класичним преварама које за средство извршења имају интернет без неког посебног утицаја на електронску обраду података или рад рачунара. Преваром путем интернета обмањују се људи, док се рачунарском

[516] РТС, www.rts.rs./.../ci/.../Nemacka+uklanja+govor+mržwe+sa+interneta.html. Претражено 22.12.2015.

преваром „обмањује“ рачунар и електронска обрада наводи на погрешан резултат који је усмерен на стицање противправне имовинске користи.[517]

Превара путем интернета или интернет превара односи се на било коју превару при чијем извршењу лице које у намери прибављања противправне имовинске користи за себе и другога, искористи једну или више компоненти интернета, као што су собе за ћаскање, веб странице или електронска пошта, да би се створили услови за лажно приказивање или прикривање чињеница којим би се неко лице довело у заблуду или у њој одржавало, да би то лице учинило нешто на штету своје или туђе имовине (спровођење финансијске трансакције, преношење податка финансијској институцији која је мета напада и сл.).[518]

Појавни облици превара су многобројни, због различитих начина њиховог извршења немогуће их је у потпуности све сагледати јер се у пракси јављају како примитивне и грубе преваре тако и оне преваре код којих учиниоци испољавају висок степен вештине. Као чест облик интернет превара јављају се: „валентино“ преваре, „ланчана писма“, пирамидалне шеме, „лутајући“ трговци, трансфер новца у добротворне сврхе и лутријске преваре. *„Валентино“ преваре* су повезане са „услугама“ које се пружају усамљеним особама које желе да склопе брак или да ступе у контакт са неком особом ради дружења. После одређене припреме, која обухвата комуницирање мејловима, размену фотографија, преварант предлаже лични контакт са жртвом под условом да му уплати одређену суму новца како би допутовао до места сусрета. После трансфера новца, сваки контакт са жртвом престаје. *„Ланчана писма“* садрже захтев упућен мејлом да се добијени мејл проследи одређеном броју пријатеља и уколико се то не учини, особу ће задесити нека несрећа. Оваква писма садрже криптовене информације, које ће лицу које је послало ланчано писмо омогућити да сазна личне податке великог броја лица и да их злоупотреби. *Пирамидалне шеме* представљају такву врсту превара код којих се жртви обећава исплата одређене своте новца за „привлачење“ одређеног броја

[517] Бабовић, Милош.:„Хакерска субкултура и компјутерски криминал“, Правни живот – часопис за правну теорију и праксу, бр. 9/2004, година LIII, књига 485, стр. 749-750, Удружење правника Србије, Београд.
[518] Матијашевић, Јелена, Спалевић, Жаклина, Игњатијевић, Светлана: “Врсте интернет превара - појам, значај и утицај на економске и моралне аспекте друштвене заједнице”, ИНФОТЕХ-ЈАХОРИНА Вол. 11, 2012, стр. 563, http://www.academia.edu/3061962/Vrste_internet_prevara-pojam_zna%C4%8Daj_i_uticaj_na_ekonomske_i_moralne_aspekte_dru%C5%A1tvene_zajednice, претражено 01. 04. 2015. године

људи и укључивање у рад „пирамиде“. *„Лутајући трговци“* се баве продајом непостојеће робе, робе лажног квалитета, која може бити опасна по здравље, траже мејловима исплату новца, али нкад не изврше испоруку. Код *преваре трансфером новца у добротворне сврхе* од жртве се тражи да за одређену провизију прими на свој банковни рачун одређену суму новца, подигне га са рачуна и уплати на неки рачун у иностранству, са образложењем да ће новац бити искоришћен у добротворне сврхе. Провизија за овакву трансакцију се не добија, а оваквим трансфером се прикрива порекло новца („прање новца“). *Лутријске преваре* се састоје у томе што жртви стиже обавештење да је добитник неке премије и да пошаље одређену своту новца у циљу добијања те награде или се тражи да жртва наведе број свог банковног рачуна и одређене личне податке, што ће свакако бити злоупотребљено.

Према истраживању Америчког удружења за заштиту потрошача за откривање најчешћих интернет превара (National consumers league – NCL), које је спроведено 2006. године,[519] најчешће интернет преваре су наведене у следећој табели:

Место на	Назив преваре	Проценат жалби у односу на све	Просечан губитак
1.	Интернет аукције	34 %	1.331 $
2.	Продаја преко	33 %	1.197 $
3.	Плаћање лажним	11 %	4.053 $
4.	„Нигеријске преваре“	7 %	3.741 $
5.	Лажне лутрије	4 %	1.750 $
6.	Лажни зајмови	3 %	1.515 $
7.	Фишинг	2 %	/
8.	Наградне игре	1 %	2.447 $
9.	Преваре провајдера	1 %	920 $
10.	Инвестиције	1 %	4.759 $

[519] The top 10 Internet Frauds, National Fraud Information Center, http://www.nclnet.org/, претражено 14. 11. 2014. године

У најчешће вршене интернет преваре спадају и преваре путем интернет промоција, кредитних картица, пирамидалне новчане преваре путем мулти левел маркетинга, пословне понуде и поготово рад од куће, инвестиционе преварне шеме попут „како се лако обогатити", преваре са путовањима као и преваре коришћењем туђих бројева здравственог осигурања.[520] Међу често вршене преваре спадају преваре приликом интернет куповине аутомобила и аукцијске и малопродајне новчане преваре преко интернета.

Приликом *куповине аутомобила преко интернета*, преварант оглашава да се по веома приступачној или чак ниској цени продаје непостојеће возило, најчешће луксузан или скуп спортски ауто, чија регуларна цена може да буде и неколико пута већа од тражене. Детаљи о возилу су најчешће преузети са других сајтова који се баве продајом аутомобила преко интернета и делују врло примамљиво, па заинтересовани купци надајући се повољној куповини контактирају преваранта, који даје инструкције жртви преваре да пошаље депозит или целу уплату преко електронског трансфера како би покренуо процес „шпедиције", пошто се тражени аутомобил обично налази у иностранству. Преварант може такође да набави податке о возилу које наводно покушава да прода преко интернета тако што ће контактирати некога ко заиста покушава да прода возило преко интернета, питајући га за број шасије возила како би проверио записе о несрећама са тим возилом. Преварант ће заправо тај број искористити да употпуни слику о возилу које наводно он продаје.

Код *аукцијске и малопродајне новчане преваре преко интернета* преварант започиње продају по веома повољној цени преко интернета на сајтовима који су за то специјализовани. Најчешће су у питању скупље и вредније ствари или понекад и колекционарски примерци. Преварант прихвата уплату од победника виртуелне аукције или купца у интернет продавници, али му уопште не испоручује ствар за коју је добио новац или му испоручује предмет чија је реална вредност знатно мања од оне за коју је жртва дала новац (нпр.фалсификат или коришћен предмет уместо новог).

За извршење наведених дела, преваранти најчешће користе фишинг технике како би „отели" податке са налога легитимних корисника или налоге са

---

[520] Computer Crime Research Center: Fraud in the Internet, http://www.crime-research.org/articles/Internet_fraud_0405/, претражено 02. 11. 2013. године

веома позитивном репутацијум на интернету и користе их да поставили лажне виртуелне продавнице. Преварант оваквим поступком истовремено сакупља новац за себе, а док жртва преваре схвати да није добила оно за шта је дала новац, за кривично дело преваре ће бити оптужен прави носилац налога чији је идентитет преварант преузео.

Једна од најпознатијих светских тзв. инвестиционих интернет превара (енгл. Advance-fee fraud) је тзв *„Нигеријска превара" или „Превара 419"*, која подразумева улагање одређене своте новца у одређени „посао", уз обећање да ће се као бенефит остварити знатно већа сума новца од уложене.[521]

Неколико незапослених студената са нигеријског универзитета почело је раних осамдесетих година XX века да преваром узима новац од пословних људи са запада. Израз „превара 419" добила је назив по члану број 419 Нигеријског кривичног закона који дефинише и санкционише кривично дело преваре.

Криминална активност извршилаца састоји се у слању електронске поруке која је тако осмишљена да изгледа као да је намерно послата примаоцу поруке, а почиње убеђивањем потенцијалне жртве преваре да учествује у подели новчаних фондова ако унапред уплати одређени износ који је, у највећем броју случајева, неупоредиво мањи од оног износа који би требало да добије као корист од тог фонда. Електронском поруком се од потенцијалне жртве тражи помоћ за трансфер великих новчаних износа, а она ће заузврат добити одређени проценат као награду. У порукама се такође наводи да је реч о изузетно великој суми новца, да је пошиљалац поруке члан нигеријске владе или војске, да је спреман да подели новац са особом која му помогне да се трансфер изврши и неопходно да цео поступак остане у најстрожијој тајности. Уколико жртва пристане да учествује у спровођењу ове трансакције, достављају јој се фалсификовани документи, на основу којих ће жртва уплатити одређени новчани износ према инструкцијама које је добила. Након тога, почиње одлагање новчаних трансакција, повећање трошкова трансакција, врши се притисак на жртву, која после дужег времена схвата да је преварена.

[521] Матијашевић, Јелена, Спалевић, Жаклина, Игњатијевић, Светлана, *op.cit.,* 2012, стр. 563

Примери писма „Нигеријске преваре“:

ORIENT BANK NIGERIA PLC
PHASE 2 ,NEW APAPA ROAD,
LAGOS NIGERIA.
*CONFIDENTIAL EMAIL ADDRESS: **********
ATTN: SIR/MADAM*

I am Mr. Williams Okon, Bank Manager Orient Bank Nigeria plc, Lagos Branch and financial manager to Mr. Khaled Ali. I have urgent and very confidential business proposal for you in June 6, 1997, a JORDAN Oil consultant/contractor with the Nigerian National Petroleum Corporation, Mr. KHALED ALI Deposited two trunk boxes for twelve calendar months, valued at US$ 17,800,000.00 (Seventeen Million Eight hundred thousand Dollars) in a security company in LOME TOGO which was to be used for multi-purpose agriclutural project in west Africa before his death, Upon maturity, I sent a routine notification to his forwarding address but got no reply. After a month, we sent a reminder and finally we discovered from his contract employers, the Nigerian National Petroleum Corporation that Mr.KHALED ALI died from an autocrash accident. On further investigation and discovered that Mr. KHALED ALI did not declare any kind or relations in all his official documents, including his Bank Deposit paperwork in my Bank.

No one has ever come forward to claim it.Consequently, my proposal is that I will like you as a foreigner to stand in as the next of kin to Mr.KHALED ALI so that the fruits of this old man's labour will not get into the hands of some corrupt government officials.This is simple, I will like youto provide immediately your full names and address so that the Attorney will prepare the necessary documents and affidavits which will put you in place as the next of kin. We shall employ the service of two Attorneys for drafting and notarization of the WILL and to obtain the necessary documents and letter of probate/administration in your favorfor the transfer.

A bank account in any part of the world which you will provide will then facilitate the transfer of this money to you as the beneficiary/next of kin.The money will be paid into your account for us to share in the ratio of 80% for me and 20% for you. There is no risk at all as all the paperwork for this transaction will be done by the Attorney and my position as financial Manager guarantees the successful execution of this transaction. Here are what you are to do.

1) To come down to LOME TOGO to open account where the fund will be transfered into.

2) To assist in paying the dumurrage which the consignment have acquired for some time now, please send you direct phone number for easy communication

*If you are interested, please reply immediately via my CONFIDENTIAL email address: **********

Upon your response,I shall then provide you with more details regarding this transaction.Please observe utmost confidentiality, and be rest assured that this transaction would be most profitable for both of us because I shall require your assistance to invest parts my share in your country.MAY THE ALMIGHTY ALLAH BLESS YOU.Awaiting your urgent Reply.*

Regards,
MR.WILLIAMS OKON

INVESTMENT ASSISTANCE

Sir,

With due respect, trust and humility I write you this proposal which I believe would be of great interest to you. I am MRS TINA GOGO the wife of late DR. DONALD GOGO of blessed memory. Before my husband was killed by rebel forces loyal to Major JOHN PAUL KOROMAH. He was the Director General Gold and Diamond Mining Corporation (G.D.M.C.) of Sierra Leone.

Two days before his death, he managed to sneak a written message to me, explaining his condition and concerning trunk box of valuables containing money and diamonds, which he concealed under the roof. He instructed me to take our children and move out of Sierra Leone immediately to any neighbouring country. Eventually it resulted into full war, I became a widow overnight, helpless in this hopeless situation.

Daughter and I my son managed to escape to Abidjan, Ivory Coast through the help of my husband's friend. The cash inside the box was USD $ 25.5 MILLION (TWENTY FIVE MILLION FIVE HUNDRED THOUSAND US DOLLARS), and DIAMOND, due to fear and limit right as a refugee I deposited the items with private security company with my son's name MR. JOGO GOGO (JR). Be informed that the real content of the boxes were not disclosed to the security company as these were deposited as personal effects for security reasons. Meanwhile I want to travel out of Ivory Coast entirely with this money for investment in your country because of the unsuitable political situation and mostly for the future benefit of my children. I want you to assist us get the money out of the Security Company and transferred into your nominated private account in your country. You shall also source for good investment, so that we can invest the money wisely.

*Concerning the money, we are prepared to give you 20% of the total sum and 5% mapped out for expenses. For the interest of this business do not hesitate to call my son MR JOGO GOGO (JR) on telephone number ********** or email address: ********** immediately you receive this message for more information to enable us proceed in earnest towards concluding all arrangements, no other person knows about this money expect I, my son and you.*

Awaiting your most urgent response.
Thanks for your co-operation and GOD bless you.

У току 2008. и 2009. године на територији Републике Србије пријављено је девет кривичних дела преваре са елементима „нигеријских превара“ против непознатих учинилаца, при чему је укупна имовинска штета износила преко 60.000 евра.[522] Оштећена лица су новац извршиоцима кривичних дела слали преко сервиса Western Union и MoneyGram, углавном преко бесплатних налога за електронску пошту која је отварана на интернет сервисима који омогућују бесплатне налоге електронске поште. Коришћене су лажне интернет адресе, интернет портали, фалсификована документација државних органа и предузећа Нигерије, Гане и других држава са територије Западне Африке. Извршиоци су најчешће сву коресподенцију обављали са јавних места, као што су интернет кафеи, како не би могло да им се уђе у траг.

Након што се превара пријави, неопходно је прикупити све електронске доказе који указују на остварену комуникацију између извршилаца кривичног дела и оштећених, као и податке о финансијским трансакцијама које је оштећени извршио према инструкцијама које је добио од извршилаца. Покушава да се пронађе ИП адреса и лоцира сервер са кога су извршиоци кривичног дела слали електронске поруке оштећеном, прикупља се преглед целокупне електронске поште коју је оштећени примио, а затим се преко Интерпола врше провере корисника коме је ова адреса била додељена у тренутку вршења кривичног дела.[523]

„Нигеријске преваре“ достигле су свој врхунац 2009. године, када су жртве превара, према подацима холандске компаније Ultrascan,[524] изгубиле готово 50% више новца него 2008. године. Према извештају ове компаније, која је анализирала 8.503 случаја у преко 152 земље у току 2009. године, жртве су изгубиле 9,3 милијарде долара у односу на 6,3 милијарде долара 2008. године.[525] Укупно 51.761 превара је почињено из 69 светских земаља, док је осталих 250.000 превара почињено из Нигерије.[526]

---

[522] Урошевић, Владимир: “Нигеријска превара у Републици Србији”, часопис Безбедност, бр. 3, 2009.година, http://www.mup.gov.rs/cms/resursi.nsf/Nigerijska_prevara.pdf, претражено 17. 01. 2014. године
[523] *Ibid.*
[524] Ultrascan Advanced Global Investigations, http://www.ultrascan-agi.com/, претражено 12. 03. 2015. године
[525] *Ibid.*
[526] *Ibid.*

Да би се избегла оваква врста виктимизације или бар смањила могућност да до ње дође, корисницима друштвених мрежа се саветује да:[527]

- уколико учествују у интернет аукцијама, добро проуче како се аукције заиста спроводе, које су обавезе продаваца пре него што прода одређену ствар и које су обавезе купца; да се што боље распитају да сазнају све о продавцу и његовом пословању, као и о начину доставе купљене ствари;

- корисници добро провере да ли приликом интернет куповине нема још неких додатних и непредвиђених трошкова;

- нема потребе да за овакав вид трансакција нигде уписују број здравственог осигурања или возачке дозволе, јер су то подаци који се могу злоупотребити и за крађу идентитета и извршење различитих кривичних дела;

- како би се избегла злоупотреба кредитних картица, корисник не сме да укуцава њен број уколико није уверен да је сајт заштићен и под сигурном везом;

- приликом интернет куповине, неопходно је проверити да ли продавац заиста постоји (проверити позивом на телефонски број продавца, послати елетронску поруку да се види да ли је адреса активна и да ли се заиста користи и сл.);

- када је реч о тзв.“нигеријским преварама”, корисници морају да буду скептични по питању свих особа који им се обраћају као званичници из Нигерије а траже помоћ у новцу која мора да се уплати у неку страну банку, да не верују обећањима о великим сумамам новца које ће им бити исплаћене и да веома пажљиво чувају лозинку свог налога како га неко не би злоупотребио.

3.1.9. Трговина људима и трговина људским органима

У Протоколу за превенцију, сузбијање и кажњавање трговине људима посебно женама и децом уз Конвенцију против организованог међународног криминала, који су донеле Уједињене нације 2000. године а Република Србија ратификовала 2001. године,[528] трговина људима се дефинише као врбовање, превожење, пребацивање, скривање и примање лица, путем претње силом или

---

[527] The FBI – Common Fraud Schemes: Internet Fraud, http://www.fbi.gov/scams-safety/fraud/internet_fraud , претражено 03. 05. 2013. године

[528] Закон о потврђивању Конвенције Уједињених нација против транснационалног организованог криминала и допунских протокола („Сл.гласник СРЈ – Међународни уговори“, бр. 6/2001)

употребом силе или других облика присиле, отмице, преваре, обмане, злоупотребе овлашћења или тешког положаја или давања или примања новца или користи да би се добио пристанак лица које има контролу над другим лицем, у циљу експлоатације[529], док појам експлоатације обухвата „експлоатацију проституције других лица или друге облике сексуалне експлоатације, принудни рад или службу, ропство или однос сличан ропству, сервитут или уклањање органа". [530] У Кривичном законику Републике Србије радња извршења кривичног дела трговина људима (чл. 388) постављена је веома широко и обухвата низ активности: врбовање, превоз, пребацивање, предаја, продаја, куповина, посредовање у продаји, сакривање или држање другог лица. Све наведене активности се врше применом силе, претње, довођењем у заблуду или одржавањем у заблуди, злоупотребом овлашћења, поверења, односа зависности, тешких прилика другог, задржавањем личних исправа или давањем или примањем новца или друге користи, све у циљу експлоатације нечијег рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употребе у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима. На тај начин су у опису кривичног дела наведени и најчешћи облици у којима се јавља трговина људима. Поред трговине људима, инкриминисана је трговина малолетним лицима ради усвојења (чл. 389) и заснивање ропског односа и превоз лица у ропском односу (чл. 390) као кривична дела против човечности и других добара заштићеним међународним правом.

Трговина људима, као глобални феномен, погађа све земље у свету, али су посебно угрожене земље у политичкој и економској транзицији, неразвијене земље, земље у развоју, земље у рату и постконфликтне земље, које се најчешће појављују као земље порекла и транзита жртава. Економски развијене земље су земље дестинације, мада се економска развијеност и богатство земље дестинације не могу посматрати независно од ситуације у земљи порекла. У ланац трговине људима улази се на више различитих начина: прихватањем

[529] Чл. 3 ст. 1 тач. а) Протокола за превенцију, сузбијање и кажњавање трговине људима посебно женама и децом који допуњује Конвенцију против организованог међународног криминала („Сл.гласник СРЈ – Међународни уговори", бр. 6/2001)
[530] *Ibid.*

лажне пословне и друге понуде, коју даје особа позната жртви или у коју има поверења; лажим „забављањем“- када женска особа прихвати понуду младића, који се претвара да је са њом у љубавној вези, да напусти земљу или град и отпутује на другу дестинацију, где је наводно чека нови, срећнији живот; пријављивањем на лажне огласе за посао, који се објављују у различитим медијима (новине, интернет, друштвене мреже) и нуде боље услове рада и велику зараду; продајом од стране породице и отмицом. Трговци људима држе жртве у заточеништву и изолацији, под сталним надзором, често их пребацују са једног места на друго, без моућности да одлучују о свом животу.[531]

Трговина људима коришћењем интернета и друштвених мрежа веома је чест облик криминалитета и злоупотреба. На пословним сајтовима маскиран је у облику веома примамљивих понуда за добро плаћен посао у иностранству. Посетиоцима ових сајтова се нуди да добију посао на одређено време тако што ће најпре попунити пријаву са детаљним информацијама о материјалном, породичном и здравственом статусу, а затим остварили лични контакт и били регрутовани за трговину људима, уколико је процењено да су сасвим „безбедни“. Уписивањем личних података у потпуности се открива профил жртве и дају се велике могућности за злоупотребу. Жртве трговине људима завршавају у иностранству као јефтина радна снага, где су, лишени пасоша и новца, приморани да се баве проституцијом или тешким физичким радом за који нису плаћени.

Резултати статистичких и аналитичких података Министарства унутрашњих послова Републике Србије, Центра за заштиту жртава трговине људима и организације цивилног друштва за борбу против трговине људима („АСТРА“), показују да овај облик криминалитета добија све веће размере у Србији, као земље порекла и транзита жртава. У току 2013. године у Србији су идентификоване 92 жртве трговине људима, што представља повећање од 16% у односу на 2012. годину. Међу идентификованим жртвама било је чак 49% малолетника, нешто око половине су девојчице. Према званичним подацима у Србији је од 2000. до 2013. године идентификовано 739 жртава трговине људима. Свакако треба нагласити да ово није стварни број извршених

[531] Организација АСТРА, www.astra.org.rs/cinjenice-o-trgovini/sta-je-trgovina-ljudima. претражено 01. 12. 2015. године

кривичних дела трговине људима, јер је веома велика „тамна бројка“, односно број неоткривених кривичних дела и извршилаца.[532]

Међутим, иако је несумњиво да је коришћење интернета и друштвених мрежа за злоупотребу све чешће и у области иррегуларних миграција, посебно кријумчарења људи, као и трговине људима, још увек у Србији не постоје довољно добро дефинисане мере и механизмни за њихово спречавање и сузбијање. Такође, недостају релевантна истраживања у овој области, која би значајно допринела како универзалном теоријском уобличавању тако и изградњи одговарајућег система заштите.

Посебан облик трговине људима је *трговина људским органима*. Трговина људским органима одвија се углавном преко интернета, а интернет странице су пуне огласа о продаји органа, посебно рожњачом, бубрезима и јетром.[533] Питање које се намеће као интересантно је ко је заправо оштећени тј. жртва када је реч о извршењу овог дела, јер заправо постоји обострана сагласност и интерес.

До трговине људских органа на интернету заправо долази због несразмере између броја легално понуђених органа који су расположиви за трансплантацију, са једне стране, и далеко веће потражње органа, са друге стране.[534] Функција интернета је да преко посредника повезује доноре, примаоце органа и медицинско особље, јер се ова дела врше углавном у

---

[532] Како би испитали на који начин функционише врбовање преко интернета, АСТРА је креирала на друштвеној мрежи лик девојчице од 15 година. У соби за ћаскање у којој је постављем профил за неколико сати пријавило се 500 људи. Четвртина особа које су са њом ступиле у контакт узнемиравале су је сексуално, било је много експлицитних и узнемиравајућих порука. Просек година ових насилника био је око 30, мада је било особа старијих од 50 година. Ипак, већина, чак 63% саговорника на интернету неће да открије своје године, 90% не открива своје занимање и место становања. Сва деца из једног одељења београдске школе могла су да постану жртве трговине људима, јер ох је наставник пријавио за радну праксу у Италији. Када су хтели да провере институцију у којој ће радити, испоставило се да таква нституција не постоји, већ да је мамац за лаковерне девојке и младиће који поверују да се ради о „добро плаћеном послу“. Дневне новине Press Online, www.presssonline.rs/svet/balkan/156660/vrbuju-decu-preko-društvenih-mreža.html претражено 02. 12. 2015. године

[533] Вулетић, Дејан: “Трговина људским органима у сајбер простору”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 65

[534] У Препоруци Савета Европе о трговини људским органима у Европи бр.1611 из 2003. године, (Council of Europe Recommendation 1611 – Trafficking in organs in Europe, http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta03/EREC1611.htm, претражено 17. 06.2014.године) наведено је да је у том периоду само на територији Западне Европе око 40.000 људи чекало на трансплантацију бубрега и да између 15 % и 30 % пацијената умре чекајући трансплантацију. Наведено је да је просечно време чекања за трансплантацију органа 2003. године било три године, а према тадашњим њиховим предвиђањима, у 2010. години тај период ће достићи десет година.

организованим групама. Виртуелни простор због непрегледног броја доступних информација и непостојања географског ограничења слабо је могуће контролисати и надгледати.

Поред Конвенције УН против организованог међународног криминала, Србија је 2009. године ратификовала и Конвенцију Савета Европе о борби против трговине људима[535] коју је Савет Европе донео 2005.године.[536] Члан 5 Конвенције обавезује државе потписнице да су у обавези да предузму мере како би успоставили и учврстили националну координацију различитих тела надлежних за спречавање и сузбијање трговине људима, па самим тим и људским органима.

Поступајући у складу са Конвенцијом чија је у време доношења важећег Кривичног законика, Република Србија била само потписница, чланом 388. КЗ РС прописано је кривично дело трговина људима, које препознаје и санкционише свако силом или претњом, довођењем у заблуду или одржавањем у заблуди, злоупотребом овлашћења, поверења, односа зависности, тешких прилика другог, задржавањем личних исправа или давањем или примањем новца или друге користи, врбовање, превожење, пребацивање, предавање, продају, куповање, посредовање у продаји, сакривање или држање другог лица, а у циљу експлоатације његовог рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употреба у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима.[537] Прописана казна за извршење овог кривичног дела је казна затвора две до десет година.[538]

У Србији до 2009. године у судској пракси није регистрован ни један случај трговине људским органима.[539]

---

[535] Council of Europe Convention on Action against Trafficking in Human Beings – CETS No. 197., http://conventions.coe.int/Treaty/EN/Treaties/Word/197.doc, претражено 17. 06. 2014. године

[536] Закон о потврђивању Конвенције Савета Европе о борби против трговине људима („Службени гласник РС”, бр. 19/2009)

[537] Чл. 388 КЗ РС

[538] *Ibid.*

[539] Вулетић, Дејан, *op.cit.,* 2009, стр. 65

3.1.10. Интернет (сајбер) тероризам

Сајбер тероризам представља модеран облик тероризма, који повезује два велика страха модерног доба: виртуелни сајбер простор и терористичко деловање.[540] Интернет је веома погодан за различите терористичке активности и пословање, јер пружа могућност сигурне комуникације са веома ниским трошковима.[541] Сајбер тероризам се односи на смишљене, политички мотивисане нападе на компјутерске системе и програме, као и на податке којима треба да се изазову насиље и страх код цивилних мета.[542] Ново оружје у виртуелним ратовима који се воде чине логичке бомбе (енгл. Logic Bombs), „тројанци“ (енгл. Troyan horses), „црви“ (енгл. Worms) и „вируси“, чији је главни циљ да омогуће престанак рада система и губитак информација, а самим тим и да се преоптерете телефонске линије, омета авионска контрола и компјутери задужени за контролу и рад других видова саобраћаја, злоупотребе програми које користе велике институције и хитне службе и сл.

Не постоји јединствена и општеприхваћена дефиниција сајбер тероризма, већ су све постојеће дефиниције указивале на неке од елемената које ово дело обухвата: крађа података или хакинг, планирање терористичких напада, проузроковање насиља, напад на информационе системе и рачунарске мреже и сл. Ипак, интернет тероризам мора да се сагледа одвојено од компјутерског криминалитета, јер не представља сваки напад на рачунарске системе дело сајбер тероризма. Ако би се сајбер тероризам поистоветио са свакодневним нападима на рачунарске системе, још би био већи проблем са сигурношћу утврдити идентитет, намеру или политичку подкрепљеност извршиоца дела. Из тог разлога, сајбер тероризам је исправно дефинисати као употреба рачунара у функцији оружја или мете, од стране политички мотивисаних међународних или пара-националних група или појединаца који прете или спроводе насиље

---

[540] Abdul Manap Nazura, Moslemzadeh Tehrani Pardis: “Cyber Terrorism: Issues in Its Interpretation and Enforcement”, International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012, стр. 409, http://www.ijiee.org/papers/126-I149.pdf, претражено 17. 07. 2015. године

[541] Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана: “Интернет у функцији тероризма”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 318 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[542] Гаћиновић, Радослав: „Облици савременог тероризма“, НБП Журнал за криминалистику и право, Криминалистичко-полицијска академија, 2012.година, стр. 15, http://www.kpa.edu.rs/cms/data/akademija/nbp/NBP_2012_1.pdf, претражено 21. 06. 2015. године

како би утицали на јавност и на званичне владе да промене свој начин вођења политике.[543]

Поједини аутори, попут Џејмс Луиса, дефинишу интернет тероризам као коришћење рачунарских мрежа и алата ради прекида рада критичних националних инфраструктура (попут енергије, средстава јавног превоза, владиних активности и сл.) или како би се приморала или застрашила влада неке државе или њени грађани. Циљ реализације оваквих активности је да се критичне националне инфраструктуре онеспособе и постану зависне од рачунарских мрежа и самим тим рањивије, стварајући "масовну електронску Ахилову пету" сваког система коју ће насилне организоване групе покушати да злоупотребе.[544] Сајбер тероризам заправо користи модерну технологију како би стратешки створио слабе тачке неког система које ће затим искористити за постизања својих циљева.

Дебра Литлџон Шиндер (Debra Littlejohn Shinder) сматра да напади на рачунаре и рачунарске мреже могу бити дефинисани као сајбер тероризам ако су ефекти довољно деструктивни да производе страх упоредив са физичким актом тероризма. То је насилан облик компјутерског криминалитета, који је извршен, планиран или координисан у виртуелном простору и помоћу рачунарских мрежа.[545] Неки од најчешћих начина реализације су: комуникација електронским порукама ради постизања конспиративних договора како би се спровеле одређене терористичке активности или регрутовали нови чланови за терористичке организације, саботирање ваздушног саобраћаја како би се срушили ваздухоплови, загађивање воде преко електронских пречишћивача, упади у болничке системе како би се обрисале или мењале базе података и преписане методе лечења пацијената, напади на изворе снабдевања струјом који могу да доведу до смрти већег броја људи који се налазе на респираторима који у својим домовима имају медицинску негу а немају агрегате за струју и сл.

---

[543]Wilson, Clay: "Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress", CRS Report for Congress, 2005, стр. 5 и 7, http://fpc.state.gov/documents/organization/45184.pdf, претражено 17. 07. 2015. године

[544] Lewis, A., James: "Assessing the Risks of Cyber Washington DC, Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies, 2002, стр.1, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, претражено 24. 10. 2015. године

[545] Littlejohn Shinder, Debra: "Scene of the Cybercrime: Computer Forensics Handbook", *op.cit.*, 2002, стр. 19

Абрахам Вагнер (Abraham R, Wagner) сматра да су Интернет и друштвене мреже идеалне за спровођење терористичких активности и операција, јер омогућавају географски неограничену и временски брзу комуникацију која не кошта много. Употреба и злоупотреба од стране терориста може да се креће у четири главна правца: (1) коришћење интернета за међусобну комуникацију терориста; (2) приступ различитим информацијама које се налазе на интернету а могу да подразумевају и потенцијалне мете напада као и техничке појединости око нпр. склапања оружја; (3) коришћење интернета за ширење терористичких идеја и ораганизацију терористичких активности и (4) спровођење терористичких напада преко Интернета.[546]

Сајбер тероризам се дефинише и као криминални акт у виртуелоном простору који има за циљ да се заплаши влада или њени грађани у циљу остварења политичких циљева.[547] Техничке карактеристике извршења оваквог терористичког дела су ограничене могућности за непосредно надгледање, контролу и откривање ових активности; нове просторне и временске границе – непостојање границе покретљивост терориста у виртуелном простору, могућност деловања с велике дистанце, богатство избора мете напада, непостојање географских ограничења, мерење времена деловима секунде и могућност претходног тестирања планираних радњи чиме се ризик од евентуалног неуспеха смањује на минимум; анонимност извршилаца ових дела. Интернет тероризам представља намерну злоупотребу дигиталних информационих система, мрежа или компонената које га чине у сврху реализације терористичких активности. Резултати ових активности су директно насиље, изазивање страха, изазивање нестабилности стратешких и виталних функција институција једне државе, велике патње људи као и несрећа попут „колатералне штете".[548]

---

[546] Wagner, R. Abraham: "Fighting Terror in Cyberspace, Terrorism and the internet: use and abuse", стр. 7 https://books.google.rs/books?id=yf83KZZbeQIC&pg=PA1&lpg=PA1&dq=Wagner,+A.,+R.:+%22Fighting+Terror+in+Cyberspace,+Terrorism+and+the+internet:+use+and+abuse&source=bl&ots=OcEV_qWD_5&sig=o4qzKdNYafWWEKAby_yuksVhApM&hl=sr&sa=X&ved=0ahUKEwj3yIvsoOrJAhVC1RoKHSU6DMQQ6AEIITAB#v=onepage&q=Wagner%2C%20A.%2C%20R.%3A%20%22Fighting%20Terror%20in%20Cyberspace%2C%20Terrorism%20and%20the%20internet%3A%20use%20and%20abuse&f=false, претражено 17. 07. 2015. године

[547] Petrović, Slobodan: Kompjuterski kriminal, MUP Republike Srbije , 2001,str. 115, претражено 24. 10. 2015. године

[548] Димовски, Злате, Илијевски, Ице, Бебаноски, Кире: „Безбедоносно-криминалистичке димензије сајбер-терористичких напада", Зборник радова, међународна научностручна

Једна од страних државних организација која је свој раду у великој мери посветила делима сајбер криминалитета је амерички Центар за заштиту националне инфраструктуре (енгл. National Infrastructure Protection Center – NIPC).[549] У препоруци ППД-8[550] сајбер тероризам је дефинисан као криминално дело извршено употребом рачунара а које за последицу има насиље, смрт и/или уништавање, а којим се спроводи терор у циљу убеђивања владе да промени своју политику. То је унапред смишљен и политички мотивисан напад на рачунарски систем, којим се изазва насиље и колективни страх.

Према приручнику о тероризму који се користи за едукацију америчких војника „Интернет операције и интернет тероризам", интернет операције се састоје од дела интернет тероризма и дела интернет подршке, која се испољава кроз планирање, регрутовање и пропаганду.[551] Рачунарска мрежа се код оваквог вида активности може користити као оружје, посредник, циљ или као активност која претходи или прати физички напад. У Приручнику се наводи да су најважнији циљеви сајбер тероризма заправо губитак интегритета мете напада, смањење могућности деловања, одсуство поверења и сигурности и на крају физичка уништења.[552] Код овог облика тероризма, као најчешће мотивације препознаје се уцењивање, жеља за уништавањем, различите врсте експлоатације и освета, а као најчешће предузимане или запрећене акције су физичко уништавање, уништавање значајних података и информација, напад на рачунарске системе од великог значаја, илегални упади у рачунарске системе од јавног значаја и онемогућавање приступа битним системима, услугама и подацима.[553]

конференција, Сузбијање криминала и европске интеграције с осврtом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 68, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[549] National Infrastructure Protection Plan, http://www.dhs.gov/national-infrastructure-protection-plan, претражено 24. 10. 2015. године

[550] Us National Homeland Security - Presidential Policy Directive / PPD-8: National Preparedness, http://www.dhs.gov/presidential-policy-directive-8-national-preparedness, претражено 24. 10. 2015. године

[551] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, 2005, стр. I-1, http://www.globalsecurity.org/military/library/policy/army/other/tradoc-dcsint-hbk_1-02-2005.pdf, претражено 24. 10. 2015. године

[552] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, *op.cit.*, 2005, стр. II-3

[553] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, *op.cit.*, 2005, стр. II-8

ФБИ описује сајбер тероризам као криминалну радњу извршену употребом рачунара и телекомуникационе опреме, која за последицу има насиље, уништење и стварање страха, збуњености и несигурности код народа, и за циљ има утицање на владу те државе како би се спровела одговарајућа политичка, друштвена или идеолошка промена или циљ.[554]

На основу свих карактеристика интернет тероризма, могуће је реконструисати како би изгледала криминолошка димензија терористичког напада у виртуелном простору. Како ви се што боље схватио сајбер тероризам, неопходно је прво разумети сам виртуелни простор и његове могућности, па затим анализирати следећа кључна питања:

(1) ко су актери који реализују дела сајбер тероризма (да ли их подржава нека држава, да ли их држава одбацује, да ли су то парадржавне формације, хакерске групе или људи из власти који се баве шпијунажом);

(2) која се средства и технике користе приликом планирања и извођења напада;

(3) на који начин се примењују технике, тактике и процедуре извођења сајбер напада (методи друштвеног инжењеринга, прављење и уношење вируса и злонамерних програма);

(4) где се врши напад или које су категорије потенцијалних мета терористичких сајбер напада (информационе и комуникационе мреже, подаци, физички објекти, енергија, банкарство и финансије, виталне службе једне земље);

(5) зашто се врши напад или који су мотиви за извођење интернет терористичког напада, који резултати желе да се постигну, које су предности а које мане овакве акције;

(6) Када се напад врши или време спровођења интернет терористичког напада. [555]

Различитим методима напада могу да се нападају различите осетљиве државне и друштвене структуре, као и да се користе различита оружја. Код терористичких група издвојила су се три основна метода: *физички напад* који је

---

[554] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, *op.cit.*, 2005, стр. II-2

[555] Ashley, K. Bradley: "Anatomy of cyber terrorism: Is America vulnerable?", Air University, Maxwell AFB, AL, 2003, www.au.af.mil/au/awc/awcgate/awc/ashley.pdf, претражено 17. 07. 2015. године

извршен класичним оружјем и усмерен је на рачунарска постројења или линије преноса информационих података; *електронски напад* који под оружјем подразумева коришћење снаге елекромагнетне силе или електромагнетног пулса како би се блокирали рачунарски системи, као и убацивање злонамерних софтвера у рачуарске системе и канале преноса информација, као и *напад на рачунарску мрежу* који обично подразумева коришћење злонамерних програма у функцији оружја како би се у рачунарским и мрежним системима непријатеља пронашла и искористила слаба тачка и слабост у рачунарском програму који непријатељ користи, у конфигурацији система или сигурносним подешавањима рачунара, како би се одређени подаци украли или уништили.[556]

Да терористичке организације у великој мери користе предности Интернета за реализацију својих активности може да се види и из податка да је још 1998. године више од половине организација које су у САД биле означене као терористичке имало своје интернет презентације, да су 1999. године све имале бар једну ингтернет презентацију, а до 2007. године је на Интернету забележено преко 5.000 терористичких сајтова.[557]

Више је разлога због којих терористи користе интернет за пропагирање, планирање и спровођење својих активности, као и за регрутовање нових чланова: (1) интернет је јефтин јер све што је потребно је компјутер и приступ мрежи, није потребно куповати оружје већ је довољан само један злонамерни програм којим ће се реализовати одређена аквиност; (2) овакав начин спровођења напада штити анонимност нападача који се користе различитим надимцима па им је тешкоући у траг, не постоје физичке границе између различитих држава нао ни полицијске контроле које треба н адмудрити како би се пренело оружје; (3) број потенцијалних мета је немогуће одредити; (4) за

[556] Rodriguez, A., Carlos: "Cyber terrorism – A rising threath in the Western hemisphere", Fort Lesley J. McNair, Washington DC, 2006, http://www.library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf, претражено 17. 07. 2015. године

[557] Углавном сви терористичке интернет презентације садрже податке попут: основних циљева и мисија, историјата организације, аргументима којима се апелује на потенцијално ново чланство да прихвати мисију и циљеве организације, аудио и видео прилоге, препознатљиве логотипе организација, па чак и компјутерске игрице за децу са садржајем који је идеолошки у складу са циљевима терористичке организације. *Наведено код*: Кешетовић, Желимир, Благојевић, Марија: „Интернет и тероризам", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 47, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

реализацију акција је потребно мање физичког тренинга и спремности, мањи је ризик од погибије и није потребно далеко путовати и (5) сајбер тероризам може да утиче на много више људи од традиционалних терористичких напада.[558] Посебну опасност представља и могућност скривања тајних порука унутар медија безазленог карактера (стеганографија).[559]

Терористи данас могу да користе, поред класичних оружја, и модерна, јака и масовна оружја попут масовних медија и нових технологија. Рецимо, интернет могу да користе тројако: као оружје, као начин комуникације међу активистима и као медиј за обраћање јавности ради ширења своје идеологије.[560] Преко масовних и електронских медија најбрже се шире страх и паника.[561] Коришћење криптоване комуникације путем јавних интернет сервиса пружа могућност члановима разних ћелија да буду у сталном контакту чинећи њихово откривање, тумачење веома тешким.[562] Поред комуникације преко електронске поште, постоје и друге технике[563] за остваривање комуникације и пренос података преко интернета попут уграђивања података у дигиталне слике[564] и „Dead drop" техником.[565] Постоје на Интернету бројне јавне и приватне услуге

---

[558] Weimann, Gabriel: „ Cyber terrorism - How Real Is the Threat?", Special report 119, United States Institute of Peace, Washington, DC, 2004, http://www.usip.org/files/resources/sr119.pdf, претражено 17. 07. 2015. године

[559] Коришћењем стеганографских техника, могуће је да појединац угради сакривену поруку у дигитализоване визуелне или аудио податке, која се може детектовати само уколико се тражи на специфичан начин. Развијеније стеганографске технике, базиране на статистичком или ентропијски руковођеном кодирању, показале су се веома тешким за откривање. *Видети*: Спасић, Видоје, Васић, Александра: „Стеганографија у функцији заштите података на Интернету", Зборник Правне инфраструктурне основе за развој економије засноване на знању, Крагујевац: Правни факултет, 2012, стр. 258

[560] Гаћиновић, Радослав, *op.cit.,* 2012, стр. 16

[561] Бабић, Владица: „Нови облици дјеловања терориста (Cyber тероризам)", 4th International Scientific and Professional Conference 'Police College Research Days In Zagreb', стр. 12, http://www.mup.hr/UserDocsImages/PA/vps/idvps2015/Zbornik_radova_Konferencije.pdf, претражено 15. 08. 2015. године

[562] Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, op.cit., 2012, стр. 318

[563] *Видети*: Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.,* 2012, стр. 322; Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана: "Интернет у функцији тероризма", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 322, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[564] У слике које су доступне на Интернету, пошиљалац може да угради податке у дигиталну слику или да замени већ постојећу слику оном која већ садржи податке, а прималац може да преузме слике са интернета и да екстрахује податаке, без видљивог линка пошиљаоца. *Видети*: Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.,* 2012, стр. 322

[565] Као пошиљалац се користи место на серверу, а затим се уклони прималац датотека. Могуће је да се за ту сврху користити неки непознат сервер, име фајла остаје на серверу, али не и његов садржај. *Видети*: Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.,* 2012, стр. 322

које су интересантне за терористичке нападе, а које су из области информатике и комуникација, банкарства и финансија, енергије (нафта, гас, струја), доставе трговинских производа као и услуга од виталног значаја за човека.[566]

Друштвене мреже се од стране терориста могу користити и у сврху психолошког рата, како би се ширили дезинформације, изазивао страх и паника или слале застрашујуће претње и поруке јавности.[567] Терористи имају потпуну контролу над садржајем порука које се постављају у електронске медије и на друштвене мреже, а на овај начин покушавају такође да прикупљају и средства за финансирање својих активности,[568] за регрутовање и мобилизацију нових чланова,[569] у сврху изграђивања веза и размене информација,[570] планирања и координације активности.[571]

Финансирање терористичких организација такође може да се обавља преко Интернета и преко друштвених мрежа. Бројне терористичке групе траже директно финансијске прилоге од посетилаца својих сајтова и својих чланова и симпатизера: новац се уплаћује директно на одређене банковне рачуне, а поједине организације су примале донације и коришћењем PayPal сервиса или продајом у онлајн продавницама које се налазе у оквиру сајтова.[572] Донације нису обавезно у новцу, већ могу да буду и у стварима које терористичким активистима могу да буду од помоћи (оружје, планови различитих зграда, непробојни прслуци и сл.). Припадници терористичких група и циљу долажења до средстава за финансирање често изврше и друга дела попут злоупотребе

---

[566] Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана, *op.cit.,* 2012, стр. 324
[567] Бабић, Владица, *op.cit*., 2015, стр. 13
[568] Терористичке организације праћењем интернет сајтова могу да идентификују ствари за које се корисници интернета интересују и да им, у складу са тим, упућују захтеве за уплаћивање донација.
Видети: Бабић, Владица, *op.cit*., 2015, стр. 17
[569] Интернет може да буде иницијална тачка за контакте појединаца који својевољно желе да приступе терористичким покретима, јер се интернет користи ради ширења пропаганде и идеологије постављањем различите литературе у сврху придобијања потенцијалних преображеника у другу религију, идентификације потенцијалних људских интереса са интересима универзалне верске нације, представљање базирано на искривљеној интерпретацији вере и сл. *Видети:* Бабић, Владица, *op.cit*., 2015, стр. 18
[570] Бабић, Владица, *op.cit*., 2015, стр. 20
[571] Терористи користе интернет ради планирања и координације одређених напада, при чему користе криптоване поруке и „ђаскаонице", мапе, фотографије, путоказе, техничке каратеристике који су скривени у графичким датотекама и стеганографским алатима. *Видети:* Бабић, Владица, *op.cit*., 2015, стр. 22
[572] Кешетовић, Желимир, Благојевић, Марија, *op.cit.,* 2012, стр. 48

различитих алата за електронску трговину, платних и кредитних картица, крађе туђег идентитета, интернет превара.

Велики напори се улажу на међународном плану како би се државе ефикасно супротставиле интернет тероризму. Истовремено се потенцира међудржавна и међувладина сарадња на паралелна три нивоа:

(1) Кроз међународне организације: Уједињене нације од својих држава чланица захтевају да уложе посебне мере којима би се спречиле све потенцијалне опасности на пољу информационе сигурности, док је Интерпол септембра 2002. године основао посебно одељење против тероризма;[573]

(2) Кроз мултилатералне и мултинационалне платформе: кроз интересовање групе Г8 која се бави спречавањем тероризма и заштитом информационих технологија од тероризма, као и кроз деловање Организације за економску сарадњу и развој (ОЕЦД) која је 2002. године усвојила Водич за сигурност информационих система и мрежа[574] и позвала владе земаља чланица да промовишу информациону безбедност и безбедност рачунарских мрежа како би се спречио сајбер тероризам, уношење рачунарских вируса у системе и хаковање, а заштитила приватност појединаца и њихове личне слободе;

(3) Кроз регионално деловање: највише кроз активности Европске уније против тероризма уопште и Савета Европе, кроз оснивање Комитета експерата за сајбер тероризам (CODEXTER)[575] и доношење Конвенције о високотехнолошком криминалитету и Конвенције о превенцији тероризма.

---

[573] *Видети:* Интерпол, http://www.interpol.int/Crime-areas/Terrorism/Counter-Terrorism-Fusion-Centre, претражено 12. 12. 2015. године

[574] OECD Guidelines for the Security of Information Systems and Networks: towards a culture of security, http://www.oecd.org/sti/ieconomy/15582260.pdf, претражено 12. 12. 2015. године

[575] CODEXTER је на својим састанцима закључио да Интернет може да се на више начина искористи у терористичке сврхе и да произведе различите последице: 1) терористички напади преко интернета могу да доведу до штете не само на електронским комуникационим системима, већ и на „обичној" инфраструктури, системима и да доведу до великог броја људских жртава; 2) ширење и дистрибуција илегалних садржаја, претњи, реклама у којима се глорификује тероризам, финансирање терористичких аката, организовање обука за обучавање терориста као и регрутовање за терористичке организације, и 3) коришћење логистике и информационих технологија како би се испитале потенцијалне мете терористичких напада. *Видети:* Council of Europe – Action against Terrorism, http://www.coe.int/t/dlapil/codexter/default_EN.asp, претражено 12. 12. 2015. године и Council Of Europe - Opinion Of The Committee Of Experts On Terrorism (Codexter) For The Attention Of The Committee Of Ministers On Cyber terrorism And Use Of Internet For Terrorist Purposes, http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/4_theme_files/Cyberterrorism.asp#TopOfPage, претражено 07. 10. 2013. године

Један од вођа српских „Анонимуса“, најјаче и најпознатије хакерске групе на свету, обелоданио је да је ова група, непосредно после терористичког напада на Париз новембра 2015. године, објавила сајбер рат Исламској држави речима „Здраво. Ми смо Анонимуси. Као што знате, објавили смо рат Исламској држави у Француској, а сада долазимо у Босну и Херцеговину. Чули смо да се тамо десио терористички напад и сад ћемо се борити против група које подржавају Исламску државу. Анонимуси из целог света ће вас ловити.“ Овај хакер је навео да се њихове активности лов на џихадисте, њихове јатаке и финансијере и да Анонимуси јавно објављују податке о њима и хакују њихове налоге на друштвеним мрежама. Комуникација терориста се одвија на више начина: исписивањем порука мецима у акционим видео игрицама, методима дигиталне стенографије, сакривањем текстуалне поруке или мапе у фотографију. Интервјуисани је дао пример човека који је ухапшен пре неколико година у Немачкој, јер је у чарапи имао УСБ меморију на којој су се налазила два порно снимка. Али, немачка полиција је помоћу дигиталне формензике открила да унутар та два снимка постоје скривене поруке: у секунди једног филма има 24 фрејма, у неколико хиљада фрејмова филма се сакрије једна порука – немачкој полицији је било потребно око 2 недеље да открије око 20 порука. Ове поруке су представљале планове напада Ај Каиде, који су сви спречени. У интервјуу је такође наведено да и терористи кодисте тзв. „dark net” коме може да се приступи преко програма који омогућавају завидан ниво анонимности: корисников захтев за приступ одређеном сајту иде преко више чворова и на сваком добија нови ниво заштите, тако да последњи чвор нема никакву информацију ко је уопште послао захтев и ко је корисник. На једном оваквом сајту, интервјуисани је пронашао позив симпатизерима џихада да уплате донације у криптованој валути. У „dark net”-у може свашта и да се купи, било шта од наоружања или дроге, састојака за прављење хемијског и био ортужја за масовно уништење, лажни пасоши, идентитети ... нико се од купаца и продаваца не среће лично, све стиже на кућну адресу без спољних ознака и на тај начин овакав начин „набавке“ одговара и криминалним и кероористичким групама. (Недељне информативне новине НИН – „Ловци на тајне поруке терористе“, бр. 3387 од 26. 11. 2015. године, стр. 19-21, http://www.nin.co.rs)

3.1.11. Интернет (сајбер, дигитални, виртуелни) вандализам

Како вандализам обухвата веома широк спектар понашања, не постоји јединствена дефиниција овакве појаве. Ипак, већина аутора се слаже да вандализам представља једно малициозно понашање и агресију према околини.

Сајбер вандализам се разликује од осталих облика вандалског понашања јер је у питању уништавање и оштећивање интелектуалног власништва у виртуалном простору, без намере да се стекне материјална корист.[576] У складу са тим, поједини аутори дефинишу вандализам и кад злонамерно и бесправно уништавање, загађивање или оштећивање туђег материјалног или интелектуалног власништва, без намере да се тиме стекне директна материјална корист за себе или друге.[577]

[576] Петровић, М. Никола: „Ставови младих према сајбер вандализму”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр.76
[577] *Ibid.*, стр. 77

Два најчешћа и најпознатија облика вандализма на интернету су свакако надгледање и „затрпавање" (енгл. Spam) електронске поште и праћење и анализа „колачића" (енгл. Cookies) и намерно убацивање злонамерних програма.

Надгледање и „затрпавање" електронске поште ("нежељена пошта", енгл. Spam) представља злоупотребу електронских система у сврху слања нежељених масовних порука без икаквог критеријума. Безбројне поруке које неки корисници примају преко електронске поште, а које рекламирају производе за које никада нису изразили интересовање, обавештавају о темама на које се нису претплатили, лажне приватне поруке које воде на странице порнографског садржаја, представљање лажних корисничких профила на којима се налазе преусмерења за странице за оглашавање или интернет преваре, крађа лозинки и сл., само су неки од облика спама.

Најчешће технике[578] којима се служе особе које шаљу овај тип порука (тзв. спамери) су:

(1) Коришћење посебних програма за слање спам порука аутоматски свим пријатељима и контактима а имају облик различитих врста позива, позивница, текстова или коментара. Овакви програми користе могућност за претраживање података коју све друштвене мреже имају, преузимајући на тај начин идентитет конкретне особе која и не зна да је порука отишла са њеним потписом.

(2) Слање порука у које су уграђени линкови ка порнографским сајтовима или интернет порталима који се баве продајом ствари.

(3) Позиви пријатеља који садрже линкове за различите сајтове преко којих се нешто продаје а који имају за циљ крађу података (нпр.броја кредитне картице или различите лозинке).

(4) Постављање "спам" коментара на профилу неког од пријатеља. Наиме, спамери се труде да имају што више "пријатеља" на друштвеним мрежама како би се једним програмом инфилтрирали у што више рачунара и на

[578] ENISA Position Paper No.1: Security Issues and Recommendations for Online Social Networks, 2007, http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks , претражено 19. 03. 2015. године

што више налога, при чему се фокусирају на она места на профилима где има највише посетилаца.

(5) Крађа корисничких лозинки у циљу постављања различитих рекламних огласа на корисничке профиле других људи.

> Једна од типичних спам порука изгледа овако:
>
> *"Hey Everyone! I've moved my profile here because [Naziv društvene mreže] won't allow me to post some of my nude modelling pictures. If you want to see my more revealing pictures, I've uploaded my entire modelling photo album to my free profile here. Click Here For My Personal Pictures And Video [link ka sajtu na kome se nalazi zlonamerni program] which allows some of my more scandalous photos. Signing up takes 2 seconds as they just want to verify you are 18 or over. After you've signed up simply search for my handle "Sexy4U2" to get to my 'personal' page".*

Ризици пријема ове врсте порука су: преоптерећење интернет мреже и заузимање интернет простора, губитак поверења корисника у друштвену мрежу, преусмеравање на странице различитих непримерених или преварних садржаја, случајно учитавање злонамерних програма и крађа лозинки и/или података са зараженог рачунара. [579]

Праћење и анализа „колачића" (енгл. Cookies) и намерно убацивање злонамерних програма (софтвера) угрожава приватност корисника јер има за циљ прикупљање података о корисницима друштвених мрежа.

Први злонамерни програм (*„рачунарски" вирус")* под називом "Creeper" откривен је 1973. године, када је успео да зарази војну рачунарску мрежу, која је представљала вид претече данашњег интернета. У односу на некада, када су се злонамерни програми креирали ради забаве, данас се све више оваквих програма креира у криминалне сврхе како би се постигао неки противзаконит циљ, а најчешће ради добијања приступа финансијским подацима или важним личним подацима корисника. Поред вируса, најопаснији су „тројанци" и „црви" (енгл.Worm). „Тројанци" су програми који изгледају као да су корисни али заправо истовремено врше и оштећивање рачунара, док су „црви" програми који се шире преко електронске поште, имају могућност да се сами копирају и да се шире без знања корисника, што на крају може да доведе до потпуног загушења

[579] Сигурносни ризици друштвених мрежа, Хрватска академска и истраживачка мрежа, www.cert.hr, претражено 17. 03. 2015. године

меморије рачунара. Злонамерни програми могу такође да буду и „колачићи“ (енгл. Cookies), малвер (енгл. Malware), спајвер (енгл. Spyware) и сл.

„Колачићи” су подаци сачувани на рачунару корисника који помажу аутоматском приступу веб страницама или другим облицима информација које су тражене на комплексним веб страницама. Могу се користити и за праћење корисника чувањем специјалне употребе историјских података у „колачић” и на тај начин и доводе до нарушавања приватности корисника или до омогућавања недозвољеног приступа личним подацима. Профили на друштвеним мрежама могу да се повежу са „колачићима”, допуштајући профилу друштвене мреже да буде повезан са претраживачким навикама корисника.[580]

У последњих неколико година корисници су постали свесни штетних ефеката интернет колачића: скорашња студија случаја је показала да је 58% корисника обрисало „колачиће” са свог компјутера барем једном, а 38% чини то сваког месеца.[581] Употреба „колачића” доноси олакшице за које многи људи не знају: ако се неки сајт који захтева шифру често посећује, уз помоћ „колачића” шифра не мора сваки пут да се унесе; прати ваше приоритете; омогућава да се више веб страна користи бесплатно. Неке од ових бенефиција могу да имају негативан утицај на приватност корисника мреже када хакери преузму корисничко име и шифру корисника које колачић чува.

Приватност може да буде угрожена и намерним убацивањем одређених програма који имају за циљ прикупљање података о корисницима друштвених мрежа:

- *малвер (енгл. Malware)* представља софтвер који се користи да би нанео штету рачунару, серверу, или мрежи рачунара, најчешће преко вируса, тројанца, спајвера и сл.;

- *спајвер (енгл. Spyware)* је део софтвера који добија информације са корисниковог рачунара без његове сагласности;

- *веб буба - баг (енгл. Bugg)* је уграђена у веб страницу или електронску пошту и углавном је невидљива посетиоцу странице или читаоцу и-мејла; она

[580] Balachander, Krishnamurthy, Wills E.Craig: “On the Leakage of Personally Identifiable Information Via Online Social Networks”, http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf, претражено 12. 08. 2013. године

[581] Ibid.

омогућава проверавање да ли је особа посетила неку конкретну страницу или прочитала конкретну e-mail поруку.

У литератури најпознатији злонамерни програми[582] који су направили велику штету интернет корисницима и великим компанијама су:

Shamoon – један од најразорнијих вируса, кориснику стиже као приложена датотека (енгл. Attach) кроз електронску пошту, а уколико је корисник покрене вирус почиње да брише садржај са нападнутог рачунара и онемогућава његово поновно укључивање.

Storm Worm – појавио се 2006.године а спада у „црве", ширио се путем електронске поште која је била насловљена „230 мртвих у олујама широм Европе" а сумња се да је заразио више од 200 милиона рачунара и интернет корисника.

Sasser u Netsky оба вируса је направио тинејџер Свен Јашан из Немачке који је и ухапшен јер је процена била да је овим вирусима заразио чак 25% рачунара широм света.

MyDoom – овај „црв" је направљен 2004. године са циљем да омогући оном ко га је направио да приступи подацима сваког рачунара који је заражен, ширио се путем електронске поште и процена је да је свака дванаеста порука електронске поште била заражена.

Klez u Melissa – оба вируса су се базирала на програму „Microsoft Word", а направио их је Дејвид Л. Смит, који је кажњен новчаном казном од 5.000 долара и мером забране приласка рачунарима.

SQL Slammer – вирус се појавио 2003. године и масовно је уништавао рачунарске системе направивши општи хаос јер су банкомати појединих банака морали да буду затворени, а више авио компанија да отказује летове.

Nimda – представља „црв" који се појавио 2002. године и који је за само 22 минута од пуштања у мрежу успео да уништи хиљаде рачунарских система.

Code Red – представља вирус који је 2001. године урађен у две верзије и био је одличан показатељ несавршености програма „Windows 2000", чак постоји податак да је напао и сервере у Белој кући.

---

[582] Блиц – дневна новина од 13. 10. 2012. године, www.blic.rs, дневна новина „Блиц" од 13. 10. 2012. године, претражено 13. 10. 2012. године

I love you – представља вирус који је направљен на Филипинима а ширио се кроз електронску пошту под називом „Љубавно писмо за тебе", након његовог активирања рачунари су престајали да раде.

Заштита приватности података добила још више публицитета од стварања и повећавања популарности сајтова за друштвено умрежавање. Спокео (Spokeo)[583] не представља класичну друштвену мрежу, али представља претраживач за повезивање људи који користи податке скупљене агрегацијом. Наиме, сајт садржи информације као што су старост, статус везе, имућност, информације о ближим члановима породице као и адресе регистрованих корисника. Ове информације су сакупљене помоћу података који већ постоје на интернету а које су корисници друштвених мрежа наводили, али сајт не гарантује за тачност података.

Заштитне мере су доступне на неколико друштвених мрежа, па се на тај начин корисницима улива поверење да њихови подаци и личне информације без њихове воље и сагласности неће постати доступни свима. На Facebook друштвеној мрежи, нпр. подешавања приватности су доступна сваком регистрованом кориснику и омогућују да блокирате одређене особе да не могу да виде профил, да се ограничи приступ фотографијама и видео клиповима и сл. Подешавања приватности су такође доступна и на другим друштвеним мрежама, а сваки корисник има повластице да користи таква подешавања када оставља личне информације на интернету.

Кривични законик Републике Србије не предвиђа посебно кривично дело које се односи на сајбер вандализам, али се облици испољавања вандализма у сајбер простору могу подвести под кривична дела, као што су: оштећење рачунарских података и програма (чл. 298 - брисање и/или мењање података на туђем рачунару), прављење и уношење рачунарских вируса (чл. 300), спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303) тј. уништавање интернет сајтова и система.

[583] About Spokeo, http://www.spokeo.com/blog/about, претражено 12. 08. 2012. године

Полицијски злонамерни програми (малвери) представљају претњу са којом се корисници рачунара широм света релативно често сусрећу. Ова врста рачунарског злонамерног програма најпре инфицира рачунар, а затим има за циљ да убеди корисника зараженог рачунара да је починио неко кривично дело из области компјутерског криминала како би га натерао да плати „казну“ и тако избегне законске консеквенце. Заражени рачунар је неупотребљив јер корисник не може да приступи својим фајловима. Корисник добије информацију да треба да плати одређену казну полицији при чему је упозорење лажно али већина људи из страха плаћа казну без упуштања у испитивање истинитости обавештења које им је стигло. Најекстремнији случај наступања страшне последице једне овакве преварне радње догодио се марта 2014. године у Румунији, где је Марцел Датцу (36) извршио самоубиство зато што је поверовао да је упозорење које је видео на рачунару а којим му је због наводног кршења закона наложено да плати казну од 70.000 леја (15.519 евра) у замену за затворску казну у трајању од 11 година право и да заиста долази од полиције. Наиме, Датцу је пронађен у свом стану обешен, са четворогодишњим сином у наручју, око чијег врата је такође био конопац. Овај несрећни човек је оставио опроштајну поруку својој жени у коме се извињава свима које зна, како је добио упозорење да мора да плати 70.000 леја или да одслужи једанаестогодишњу затворску казну коју није у стању да поднесе, као и да не жели да његов син кога је убио пати због њега. Међутим, тек након ове трагедије, откривено је да ово упозорење није било право, већ да је Датцу заправо заразио рачунар овим тзв."полицијским" малвером. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Covek-izvrsio-samoubistvo-zbog-pretnje-policijskog-malvera.html , претражено 26. 01. 2015. године)

Међутим, забележени су и случајеви да је ова врста злонамерног програма заправо довела до привођења правих криминалаца правди. Наиме, Џеј Метју Рајли (21) из Сједињених Америчких Држава из Вирџиније видео на свом компјутеру лажно упозорење од злонамерног програма ФБИ под називом „Реветон“ у коме му се саопштава да је на његовом рачунару откривена дечија порнографија. Рајли је поверовао да је упозорење право и између две опције - да плати казну за прекршај или да буде кривично гоњен, Рајли се одлучио да свој рачунар сам добровољно однесе у локалну полицијску станицу, где су полицајци претражили његов рачунар и открили поруке и фотографије које је Рајли добијао од малолетних девојака, међу којима је и једна тринаестогодишња девојчица. Рајли је ухапшен и оптужен за поседовање дечије порнографије и недозвољену комуникацију са малолетним особама. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Poverovao-policijskom-virusu-i-sam-se-predao-policiji-zbog-decije-pornografije.html , претражено 26. 01. 2015. године)

2011. године, у Београду је ухапшен студент информатике који је осумњичен да је тзв. интернет „клик“ преваром једну страну компанију за три месеца оштетио за 70.000 долара при томе јој нарушивши углед. Осумњичени је најпре заразио компјутерским вирусом велики број рачунара широм света чиме је вештачки генерисао саобраћај са ових компјутера према сајтовима компаније са којом се претходно склопио уговор да ће рекламирати њихов софтвер и да ће га та компанија плаћати по свакој забележеној посети. У овој компанији нису ни слутили да је велики број посета њиховој интернет презентацији заправо последица ширења вируса. Извршењем ове преварне радње, компаније је оштећена јер је осумњиченом исплатила новац али јој је и нарушен углед због начина на који је њен сајт забележио велики број посета.

(Блиц – дневна новина од 04. 09. 2011. године, www.blic.rs, дневна новина „Блиц“ од 04.09.2011., http://www.blic.rs/Vesti/Hronika/275035/Trikovima-preko-interneta-opljackali-velike-kompanije, претражено 04. 09. 2011. године)

ФБИ је коришћењем ових злонамерних програма успео да лоцира и осумњиченог за претње бомбашким нападима на више универзитета и аеродрома широм Сједињених Америчких Држава који је користио надимак „Мо“. ФБИ испрва о бомбашу није знао ништа осим да је особа мушког пола, тамне косе, има страни акценат, носи иранску војну униформу а да са агентима ФБИ комуницира путем електронске поште, причаоница и видео причаоница. На основу онога што је открио о себи, фотографија које је послао и података које је унео приликом регистровања електронске поште ФБИ је веровао да је човек за којим трагају двадесетседмогодишњи Иранац Мохамед Ариан Фар из Техерана, а хакерски тим ФБИ направио је малвер који је требало убацити у рачунар осумњиченог када се пријави на свој налог електронске поште и отвори поруку са линком за аутоматско преузимање малвера који би на тај начин прикупио што више информација о осумњиченом које би омогућиле истражитељима да пронађу потенцијалног терористу и повежу га са претњама о бомбашким нападима. ФБИ је за реализацију овог плана морао да добије претходну сагласност суда. План је само делимично реализован јер малвер уопште није био преузет из електронске поште, али је агентима ФБИ успело да добију две ИП адресе које су потврдиле да се „Мо“ налази у Техерану и лоцирао га. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Kako-je-FBI-uz-pomoc-fisinga-i-malvera-identifikovao-osumnjicenog-za-pretnje-bombaskim-napadima.html, претражено 26. 01. 2015. године)

Интересантно је споменути американца Сенфорда Валаса (43), који је осумњичен да је до августа 2011. године корисницима друштвене мреже Facebook послао преко 27 милиона спамова, односно нежељених порука, након чега је познат под надимком „краљ спамова” и „Спамфорд”. (Блиц – дневна новина од 06. 08. 2012. године, http://www.blic.rs/Vesti/Svet/269975/Predao-se-kralj-spamova-na-Fejsbuku, претражено 06. 08. 2012. године) Валас се терети да је развио програм који је успео да заобиђе све филтере друштвене мреже Facebook и прикупи податке о налозима великог броја корисника ове друштвене мреже, а манифестовао се тако што је постављао поруке на „зидове” корисника са позивом посете одређени интернет портал преко кога су се прикупљали лични подаци корисника. Процена тужилаца је да је Валас у периоду од новембра 2008. до марта 2009. године компромитовао око 500.000 налога корисника ове друштвене мреже јер је коришћењем овог програма послао преко 27 милиона спамова. Компанија Facebook је фебруара 2009. године покренула тужбу против Валаса и двојице његових сарадника због тога што су помоћу сајтова за „пецање“ (фишинг) и на друге начине неовлашћено приступали Facebook налозима корисника а затим тако преотете налоге користили за дистрибуцију нежељених порука широм ове друштвене мреже. Октобра 2009.године Валасу је судским налогом забрањено да приступа Facebook друштвеној мрежи, а уједно је и пресудом обавезан да компанији Facebook исплати 711 милиона долара на основу кршења одредби америчког Закона о компјутерским преварама и других федералних и државних закона. Стенфорду Валасу ово није био првенац у злоупотреби података са неке друштвене мреже. Током деведесетих година прошлог века, Валас је био први човек компаније за рекламирање преко интернета CyberPromotion која је одговорна за слање 30 милиона спам електронских порука у само једном дану. Такође, маја 2008. године Валасу и једном од његових оптужених сарадника је наложено да плате компанији MySpace 234 милиона долара због фишинга на друштвеној мрежи ове компаније али је он у више наврата одбио да се појави пред судом. Валас се предао полицији августа 2012. године, а уколико се докаже да је крив за кривична дела која му се стављају на терет, постоји могућност изрицања казне зарвора у трајању до 10 година. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Podignuta-optuznica-protiv-kralja-spama-zbog-fisinga-i-spama-na-Facebook-u.html, претражено 06. 08. 2012. године)

Полиције различитих европских земаља предвођене Европолом спровеле су током 2014. године опсежну полицијску акцију у неколико европских држава током које је ухапшено 15 особа, углавном тинејџера и млађих људи, због сумње да су користили тројанске програме за даљински приступ и крађу личних података корисника друштвених мрежа. Ухапшени се сумњиче да су тројанце за даљински приступ користили за шпијунирање жртава - жртве обично инфицирају своје рачунаре тако што кликну на линк који је наводно слика или видео или на фајл који изгледа легитимно, али иза кога се крије тројанац који буде сачуван на компјутеру корисника и почиње да преноси поверљиве податке ономе ко га је направио. Операција коју је предводила Француска је део Европске мултидисциплинарне платформе против криминалних претњи (EMPACT), а у којој је учествовао и Европолов Европски центар за сајбер криминал (ECZ), као и полиције неколико европских држава, имала је за циљ да изврши координацију и прикупљање обавештајних података, да подржи европске државе у њиховим напорима да идентификују појединце које користе ове тројанске програме као и да информише јавност о претњи коју представља ова врста злонамерног компјутерског програма. Ова тема је веома значајна поготово ако се узме у обзир чињеница да су најчешћи извршиоци ових кривичних дела млади људи, на које је битно превентивно деловати како би их спречили у даљем вршењу кривичних дела. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Hapsenja-u-zemljama-EU-zbog-koriscenja-trojanaca-za-daljinski-pristup.html, претражено 26. 01. 2015. године)

Координисаном акцијом америчке и полиција шеснаесет европских земаља до новембра 2014. године угашено је стотине интернет презетнација које се жаргонски називају и „мрачни интернет“, јер се међу овим презентацијама између осталог налазе и портали преко којих се трговало недозвољеним стварима**.** На списку интернет портала који су „угашени“ налазе се портали Blue Sky, Hydra и Cloud Nine на којима се, према тврдњама америчког министартва правде, трговало наркотицима, фалсификованим новцем, украденим подацима кредитних картица и лажним идентификационим документима. На порталу Silk Road 2.0 трговало се наркотицима, хакерским алатима и фалсификованим личним идентификационим документима. Портал Executive Outcomes се бавио трговином оружјем које је испоручивано широм света, на порталу Fake Real Plastic продавале су се фалсификоване кредитне картице, на Fake ID украдени пасоши а на порталима Fast Cash и Super Notes Counter су се продавали фалсификовани еври и амерички долари. Међу „угашеним“ сајтовима су и Pandora, Topix, Flugsvamp, Cannabis Road, Black Market, Golden Nugget, Cash Machine, Cash Flow и други. Током ове полицијске акције ухапшено је 17 особа за које се сумња да су власници и администратори ових сајтова, а заплењено је око милион америчких долара и 180.000 евра у готовини, као и већа количина наркотика, злата и сребра. **(**Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Najveca-policijska-akcija-protiv-kriminala-na-mracnom-internetu-ugaseno-410-sajtova-17-osoba-uhapseno.html, претражено 26. 01. 2015. године)

Јуна 2014. године одржано је суђење Алексу Јаселу из Шведске који је као коаутор злонамерног компјутерског програма и хакерског алата под називом Blackshades продавао овај софтвер криминалцима по ценама које су се кретале у распону од 40 до 50 долара. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Autor-ozloglasenog-hakerskog-alata-Blackshades-izjasnio-se-nevinim-pred-sudom.html, претражено 26. 01. 2015. године) Куповином овог софтвера хакери су могли да са даљине контролишу заражене рачунаре и да прате шта корисници рачунара куцају на тастатури, што укључује и лозинке и приступ приватним фајловима жртава. Програм Blackshades је дизајниран да краде корисничка имена и лозинке а хакерима може да омогући и даљинску контролу над рачунаром и камером, па самим тим и прављење фотографија и видео снимака без знања жртве. Када се инсталира, Blackshades омогућава хакеру широк распон активности који могу озбиљно угрозити приватност корисника рачунара и бити веома штетне. Зараженим рачунарима се управља преко интерфејса за даљинско управљање. Претпоставка је да је овим програмом заражено пола милиона система у десетинама земаља широм света. Инфекције су биле резултат неопрезног отварања линкова у порукама електронске поште или на интернет порталу на коме се од корисника захтевало да инсталирају неки софтвер.Јасел на суђењу није признао кривицу ни за једно од дела за које се терети, ни за кривично дело завере ради вршење преваре са приступом уређајима као ни за кривично дело крађа идентитета. Уколико се у току суђења докаже његова кривица, Јасел би могао да буде осуђен на затворску казну у трајању до 17 година. За разлику од Јасела, његов сарадник Мајкл Хог је признао кривицу за дела за које се терети. Интересантно је да је у више од 100 земаља света спроведена координисана акција хапшења и заплене свега што је на било који начин повезано са програмом Blackshades, па је тако широм света ухапшено више од 100 људи а заплењено 1.900 интернет домена за команду и контролу дистрибуције Blackshades програма, 1100 десктоп и лаптоп рачунара, мобилних телефона, рутера, екстерних хард дискова и УСБ меморијских стикова. У координисаној акцији учествовале су полиције Холандије, Белгије, Француске, Немачке, Велике Британије, Финске, Данске, Аустрије, Естоније, САД, Канаде, Чилеа, Швајцарске, Хрватске, Молдавије и Италије. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Zbog-malvera-Blackshades-uhapseno-100-ljudi-u-16-zemalja.html , претражено 26. 01. 2015. године)

3.1.12. Злоупотреба фотографија

Злоупотреба фотографија на интернету представља такав облик повреде приватности када се неовлашћено користе и приказују фотографије са налога корисника друштвених мрежа без њихове сагласности. Већина корисника друштвених мрежа има дигиталне камере и своје фотографије поставља на сопствене корисничке налоге, ризикујући да те фотографије постану предмет злоупотребе.

Постоје организације које покушавају да скрену пажњу на проблеме везане за злоупотребу права на приватност. Харвардски правни преглед (Harvard Law Review) је објавио кратак чланак под називом „Улице опасности: Познавање закона о приватности“ у коме је појашњено како „закон о

приватности, у овом облику, није од помоћи људима који су без њихове сагласности означени на фотографијама“.[584] Било која особа може бити против своје воље означена (енгл. Tag) на фотографији и 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 и у чињеници да већина кривичних закона не штити особе означене на фотографијама које су направљене у јавности, јер се сматра да сама радња сликања не спада у угрожавање приватности.

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. На пример, Facebook задржава право да објави корисничке информације или да их подели са другим компанијама, адвокатима, судовима, државним службама итд. уколико сматра да је то неопходно. У чланку објављеном у „АБЦ вестима“ (ABC news), тврди се да су два тима научника открила да је лако открити информације о томе где поједини корисници живе путем фотографија објављених на интернету јер слике направљене путем телефона аутоматски прилажу географску ширину и дужину путем метаподатака, осим ако та функција није ручно онемогућена.[585]

Технологија препознавања лица може бити искоришћена за приступ личним подацима особе. Истраживачи Карнеги Мелон Универзитета (Carnegie Mellon University) су комбиновали скениране слике и профиле на друштвеним мрежама како би идентификовали особе које нису на мрежи. Добијени подаци су до те мере прецизни и детаљни да су чак садржали и број социјалног осигурања корисника. [586]

---

[584] 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, претражено 12. 08. 2012. године

[585] Савети за искључивање географског означавања на мобилним телефонима (“Tips to Turn Off Geo-Tagging on Your Cell Phone“), ABC news, 2010, http://abcnews.go.com/Technology/celebrity-stalking-online-photos-videos-give-location/story?id=11443038#.T603t8WkfTo , претражено 12. 08. 2012. године

[586] Online photos can reveal our private data say experts, BBC News, 2011, http://www.bbc.co.uk/news/technology-14386514, претражено 12. 08. 2012. године

Већина кривичних закона не штити особе чије су фотографије направљене у јавности јер се сматра да фотографисање не спада у угрожавање приватности. У кривичном законодавству Републике Србије такође није предвиђена као посебно кривично дело злоупотреба фотографија на интернету или путем друштвених мрежа, али се у недостатку посебне инкриминације, могу користити постојеће одредбе и то чл. 144, у коме се описује кривично дело неовлашћеног фотографисања и чл. 145 који се односи на неовлашћено објављивање и приказивање туђег списа, портрета и снимка. Кривично дело неовлашћено фотографисање постоји уколико извршилац начини фотографију, филмски, видео или други снимак неког лица и тиме осетно задире у његов лични живот или ко такав снимак преда или показује трећем лицу или му на други начин омогући да се са њим упозна. Други облик кривичног дела постоји уколико је извршилац службено лице и у вршењу службе неовлашћено фотографише. Кривично дело неовлашћено објављивање и приказивање туђег списа, портрета и снимка, такође забрањује објављивање и приказивање списа, портрета, фотографије, филм или фонограма личног карактера без пристанка лица које је спис саставило или на кога се спис односи, односно без пристранка лица које је приказано на портрету, фотографији или филму или чији је глас снимљен на фонограму уколико то осетно задире у лични живот тог лица. И поред тога што се злупотреба фотографија коришћењем интернета и друштвених мрежа може евентуално процесуирати на основу наведених одредби, неопходно је, ипак, инкриминисати и овај вид злоупотребе и тиме значајно допринети заштити приватности.

Џорџ Семјуел Бронк из Калифорније, САД, ухапшен је 2010. године под сумњом да је на друштвеној мрежи Фејсбук објављивао сексуално експлицитне фотографије украдене од више од 3000 жена чије је налоге претходно хаковао. Истрага је започела када се локалној полицији у Конектикату јавила жена која је тврдила да је неко објавио њене приватне снимке сексуално експлицитног садржаја на њеној Facebook страници, претпостављајући да су фотографије украдене приликом хаковања њеног емаил налога. Полиција је, поступајући по поднетој пријави, повезала ИП адресу која је коришћена приликом неовлашћеног приступа емаил налогу са Бронковим рачунаром, упала у дом осумњиченог и том приликом пронашла доказе да је реч о хиљадама жртава чије су фотографије украдене на овај начин. У компјутеру осумњиченог чак је пронађено и доста материјала који се односи на дечију порнографију. Према полицијским сумњама, сматра се да је Бронк проваљивао у емаил налоге жртава погађањем одговора на сигурносна питања која сервиси за електронску пошту постављају корисницима приликом ресетовања лозинке. Оптужница која је подигнута против Бронка садржала је оптужбе за кривична дела поседовање дечије порнографије, хаковање и крађу идентитета. (Блиц – дневна новина од 23. 04. 2014. године, www.blic.rs, дневна новина „Блиц" од 23. 04. 2014. године, претражено 23. 04. 2014. године)

У Србији је априла 2014. године пријављено постојање Facebook групе „Највеће дроље основних и средњих школа“, страница на коју је непозната особа стављала слике девојчица које је скупљала по Facebook мрежи, а које су саме девојчице постављале на своје профиле. Иако је по речима начелника Одељења за високотехнолошки криминал МУП-а могуће да починилац буде осуђен и на казну затвора у трајању до три године, постојање овакве групе је пробудило питање за које наш правни систем и даље нема одговор: каква би била квалификација једног оваквог дела уколико се узме у обзир да су девојчице саме постављале слике на своје профиле, а да их је неко без дозволе сакупио и постављањем на један овакав сајт изложио понижењу, увредио или чак изазвао осећај страха за личну безбедност. (Блиц – дневна новина од 23. 04. 2014. године, www.blic.rs, дневна новина „Блиц“ од 23. 04. 2014. године, претражено 23. 04. 2014. године)

Апелациони суд у Мичигену, САД, је 2011. године због случаја који је решавао покренуо једно веома интересантно питање – да ли је упад на налог електронске поште супружнику кривично дело или породична, приватна ствар супружника. Леон Вокера (34) који је оптужен да је упао у Gmail налог своје супруге како би проверио да ли га супруга вара суочио се са оптужницом по којој му прети изрицање максимална затворска казна од пет година зато што је користио заједнички компјутер како би прочитао електронску преписку своје супруге. Основ по коме је подигнута оптужница био је тај да је Вокер оптужен због заштите интелектуалне својине – електронског налога поште своје супруге, односно приступа њеној интелектуалној својини. (Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Optuznica-za-upad-u-Gmail-nalog-supruge-krivicno-delo-ili-privatna-stvar.html, претражено 26. 01. 2015. године)

4. Најзначајнији узроци компјутерског криминалитета и криминалних активности на друштвеним мрежама

Поред сагледавања феноменолошких карактеристика криминалних активности на друштвеним мрежама, веома значајно питање је сазнавање њихових узрока. Етиологија ове негативне друштвене појаве је веома сложена и комплексна, недовољно теоријски и емпиријски изучавана, али, у сваком случају треба констатовати да злоупотреба друштвених мрежа као део компјутерског криминалитета на макро и микро нивоу има исту криминогенезу као криминалитет уопште. То значи да је велики број егзогених и ендогених криминогених фактора исти код криминалитета уопште, компјутерског криминалитета и злоупотребе друштвених мрежа (економија, економски систем и развој; глобализација и транзиција; индустријализација и урбанизација; породичне прилике и односи; школа и образовање; неадекватно коришћење слободног времена, средства масовних комуникација и др).[587] Ипак, како се ради о посебном облику компјутерског криминалитета који има своје феноменолошке специфичности, треба указати на одређене криминогене факторе који делују као узроци, услови и поводи компјутерског криминалитета и злоупотребе друштвених мрежа.

Посебну теорију о сајбер криминалитету установио је Jaishankar 2008. године.[588] Теорију је назвао **теорија транзиције простора** (енгл. Space Transition Theory), објашњавајући да је потребно да постоји посебна теорија о узроцима криминалитета у сајбер простору, јер су уопштена теоријска објашњења феномена сајбер криминалитета недаекватна и недовољна. Теорија објашњава природу понашања особе која испољава прилагођено или неприлагођено понашање у стварном простору и у кибернетичком простору. **Просторна транзиција** обухвата померање особе из једног простора у други (на пример из стварног физичког простора у кибернетички простор и обрнуто). Према теорији транзиције простора, људи се различито понашају приликом

[587] Више о криминогеним факторима видети: Константиновић Вилић, Слободанка, Николић Ристановић, Весна, Костић, Миомира: Криминологија, *op.cit.,* стр. 337.
[588] Jaishankar, K.: "Editorial: Establishing a Theory of Cyber Crimes", International Journal of Cyber Criminology, Vol 1 Issue 2 July 2007, стр. 7, http://www.cybercrimejournal.com/Editoriaijccjuly.pdf, претражено 28. 08. 2015. године

преласка из стварног, реалног, физичког простора у виртуелни простор. Поступати ове теорије формулисани су у шест тачака:

1. Особе које су потиснуле криминално понашање у стварном или физичком простору због свог статуса или позиције, имају склоност да испоље криминалитет у виртуелном простору;
2. Флексибилност идентитета, дисоцијативна анонимност и недостатак страха у сајбер простору доводе до тога да преступник до изабере сајбер простор за извршење недозвољеног дела;
3. Криминално понашање преступника у виртуелном простору ће највероватније бити пренето и у физички простор, као што се и понашање из физичког простора може пренети у сајбер простор;
4. Повремени „испади“ преступника у сајбер простору, заједно са динамичном просторно временском природом сајбер простора дају, преступнику шансу „да побегне“, односно не буде ухваћен.
5. а) Људи који се међусобно не познају имају шансу да се уједине у сајбер простору како би извршили неки злочин у физичком простору; б) Људи који се међусобно познају у физичком простору могу да уједине како би извршили неки злочин у сајбер простору.
6. Особе из друштва које је затворено и репресивније имају веће шансе да изврше неко дело у сајбер простору него особе из отворених заједница.
7. Конфликт норми и вредности из физичког простора са нормама и вредностима у сајбер простору може да доведе до сајбер криминалитета.

Сајбер криминалитет, кога Wall (2001.) категоризује као четири главна типа: хакинг (илегални упад у компјутерски систем), сајбер преваре и крађе, сајбер порнографија и сајбер насиље, може се објаснити постулатима теорије транзиције простора.[589] Међутим, ова теорија је до сада остала само као теоријско објашњење узрока сајбер криминалитета и емпиријски није проверена.

[589] Danquah P., Longe, O.B.: “An Empirical Test of The Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana”, African Journal of Computing & ICT September 2011, Vol. 2. No. 2 Issue 1, str. 37-48, http://www.ajocict.net/uploads/V4N1P6-2011_AJOCICT_-_An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality_-_The_Case_of_Ghana_and_Beyond.pdf, претражено 28. 08. 2015. године

Друга криминолошка теорија узрочности која се повезује са компјутерским криминалитетом, посебно са крађом идентитета, је **теорија рационалног избора**[590] и у оквиру ове теорија рутинских активности и теорија стила живота. Код крађе идентитета на друштвеним мрежама, која се најчешће конкретизује кроз компромитовање налога или профила на друштвеним мрежама, мотив извршења је стицање имовинске користи на лак начин. Према теорији рационалног избора,[591] преступници ће увек тежити да изаберу оне мете које захтевају најмање напора, али које у исто време пружају високу награду и носе најмањи ризик у погледу откривања и последица неуспеха. Приликом коришћења интернета и укључивања на друштвене мреже управо стална доступност жртве, масовност корисника и отежана могућност откривања доприносе да се поједине особе одлуче на извршење дела. Полази се од претпоставке да се људи, када имају могућност избора, опредељују за одређен начин понашања. Управо се то дешава са корисницима друштвених мрежа, који се опредељују да друштвене мреже користе у складу са упутствима и утврђеним протоколима или се одлучују на разне облике злоупотреба. Свакако да се код крађе идентитета као један од криминогених фактора може сагледати олакшан приступ личним информацијама и подацима када корисници деле садржај са свим или већином корисника и на тај начин директно омогућавају повреду приватности и злоупотребу.

Теоријом рутинских активности (РАТ)[592] објашњавају се различите врсте виктимизације појединим кривичним делима, на пример, провалних крађа

---

[590] Милићевић, Слободанка, Вујовић, Срђан: „Проблем савремене доби: облици крађе и злоупотребе идентитета и мјере превенције“, Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал, *op.cit.,* стр. 310.

[591] Представници ове теорије Дерек Корниш (Derek Cornish) и Роналд Кларк (Ronald Clarke) су у раду „Рационални преступник“ (енгл. The reasoninig criminal, 1986.) навели да је основно полазиште ове теорије да се преступници приликом доношења одлуке да ли да изврше кривично дело налазе у ситуацији да бирају између алтенатива и притом врше процену користи и ризика којем се излажу. Управо однос између очекиваног ризика и користи утиче на то да ли је одређена мета „добра“ или „лоша“. Одлука преступника да ли ће у конкретној ситуацији извршити кривично дело резултат је когнитивне обраде расположивих информација и представља „рационалан избор“. Цит.према: Милић, Ненад: „Место извршења кривичног дела у теоријским промишљањима“, Журнал за криминалистику и право НБП, scindeks-clanci.ceon.is/data/pdf/0354-88721401141M претражено 09. 12. 2015. године

[592] Ова теорија се везује за рад Лоренс Коена (Lawrence Cohen) и Маркуса Фелсона (Marcus Felson), који полазе од тога да је за извршење кривичног дела потребно да се у исто време и на истом месту нађу мотивисани преступници, погодне мете (објекти) и одсуство оспособљених заштитика од преступа (чувара). Ова три елемента конституишу тзв. троугао анализе кривичног дела. *Видети:* Игњатовић, Ђорђе: „Теорије у криминологији“, Правни факултет Универзитета у

(Cohen&Felson, 1979, Cupe&Blake, 2006) крађа (Mustaine&Tewksbury, 1998), физичких напада (Stewart, Elifson&Sterk, 2004), вандализма (Tewksbury&Mustaine, 2000), оружаних пљачки (Spano&Nagy, 2005) и преваре (Holtfreter, Reisig&Pratt, 2008). Неколико аутора је кратко описало како РАТ може да се примени и на компјутерски криминалитет (Grabosky, 2001, Grabosky&Smith, 2001, Newman&Clarke, 2003, Taylor et.al., 2006, Yar, 2005)

Ипак, постоји ограничени број студија које су тестирале емпиријску вредност теорије рутинских активности у односу на извршење кривичних дела компјутерског криминалитета. Посебно Hinduja и Patchin (2008) су открили да су умешност у руковању компјутерима и време проведено на интернету у позитивној релацији са виктимизацијом од сајбер булинга за кориснике интернета који су у пубертету. Слично томе, Holt и Bossler (2009) су открили да провођење доста времена on line и у „причаоницама" и виртуелно девијантно понашање повећава могућност online узнемиравања. Теорија рутинских активности може да се примени и за неке форме сајбер криминалитета, као што су инфицирање злонамерним софтвером, али је ова веза прилично нејасна. Употреба „злонамерног" софтвера може да се класификује као врста „компјутерске крађе" уколико криминалац користи овакав софтвер како би украо нечије податке или информације. На овај начин употреба „злонамерног" софтвера дели одговара кривичном делу провале, у којој ови програми инфицирају и компромитују компјутерске системе као што би у реалном свету провалник обио врата. Већина „злонамерног" софтвера инфицира компјутер тако што користи њихову слабост или недостатке (Taylor, et. al, 2006). „Злонамерни" софтвери такође могу да блокирају антивирусне програме и остале сигурносне мере како би обезбедили сигурно преузимање података, на

Београду, Београд, 2009, стр. 116. Мотивисани преступници су индивидуе и групе код којих постоји склоност и мотивисаност да изврше дело из различитих разлога. Бити способан чувар значи да постоји способност за спречавање мотивисаног преступника да повреди или угрози жртву. Извршење злочина се објашњава се дневном рутином понашања као и присуством погодне жртве. На пример, појединци уобичајено напуштају своје домове свакодневно у приближно исто време јер иду на посао или у школу, чиме стварају предвидљиви модел који може да мотивише преступнике уверењем да су ове куће остале незаштићене. Због тога су рутинске активности битне за разумевање посебних кривичних дела до којих може да дође када људи напуштају своје домове и све оно што поседују, а има вредност. *Видети:* Bosler, A., Holt, Thomas: „Malware Victimisation, A Routline Activities Framework" и Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, Edited by K. Jaishankar, CRS Press, 2011, стр. 319, http://ruangbacafmipa.staff.ub.ac.id/files/2012/02/Cyber_Criminology__Exploring_Internet_Crimes_and_Criminal_Behavior.pdf, претражено 28. 08. 2015. године

исти начин како што провалник може да деактивира алармни систем (Kaspersky, 2003).[593] Одсуство способних чувара, као један од елемената у оквиру теорије рутинских активности, код компјутерског криминалитета може се тумачити недостатком адекватних метода заштите, али и чињеницом да се ускладиштене информације могу бескрајно користити и да је комуникација између учинилаца и жртава знатно олакшана коришћењем дигиталних мрежа.

Према **теорији стила живота** (енгл. Lifestyle/exposure to risk perspective)[594], on line стил живота директно утиче на виктимизацију од компјутерског криминалитета. Студија у којој је анализиран овај утицај[595] полази од чињенице да је компјутерски криминалитет велика претња интернет корисницима и да им наноси огромну штету, посебно када дође до крађе личних података из персоналних досијеа. Истраживања у оквиру студије су показала да студенти који воде начин живота оријентисан на коришћење компјутера и немају одговарајуће антивирус програме, имају далеко већу шанску да постану жртве компјутерског криминалитета. Могућност виктимизације се значајно смањује уколико се повећа интернет сигурност и већина корисника поседује адекватан компјутерски програм за заштиту од злоупотребе.

Поред наведених теорија, треба поменути **теорију диференцијалне асоцијације** и **теорију самоконтроле**, које објашњавају узроке појединих облика компјутерског криминалитета, сајбер тероризма, дечије порнографије и сајбер пиратерије. О теорији самоконтроле, која се везује за психолошке факторе криминалитета, биће више речи приликом анализе ендогених фактора. Теорија диференцијалне асоцијације полази од утицаја криминалних и некриминалних понашања унутар групе и опредељивања чланова групе за једо или друго понашање, зависно од утицаја који преовлађује. Битан аспект успеха терористичких група, које су своје чланство омасовиле користећи интернет и

---

[593] Bosler, A., Holt, Thomas: Malware Victimisation, A Routline Activities Framework, *op.cit.,* стр. 319

[594] Hinderlang, M., Gottfredson, M., и Garofalo, J., међу првима су развили идеју о утицају стила живота на кретање стопе криминалитета. Утврдили су да висока стопа виктимизације неких друштвених група (млади мушкарци) може бити објашњена њиховим стилом живота, који се састоји углавном у активностима ван куће и у току ноћи. Константиновић Вилић, Слободанка, Николић Ристановић, Весна, Костић, Миомира: Криминологија, *op.cit.,* стр. 307

[595] Kyung-Shick Choi: „Cyber-Routline Activities, Empirical Examination of Online Lifestile, Digital Guardians and computer Crime Victimisation“ наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior,*op.cit.* , стр. 243

друштвене мреже, управо су објашњења ове теорије о прихватању криминалних утицаја. Захваљујући интернету, терористичке групе су биле у могућности да успешно остваре односе са младим људима широм света, са различитих географских подручја и да тако координирају терористичке активности.[596]

4.1. Егзогени криминогени фактори

Свакодневно појављивање нових генерација различитих уређаја за пренос информација, комуникацију и забаву значајно утиче на стварање нових могућности за злоупотребу и противправне активности. Иновације су свакако веома корисне за развој друштва и напредак појединаца, али такође имају и своју лошу страну, јер услед велике брзине у трансформисању и иновацијама, просечан корисник нема довољно воље, времена и могућности да се упозна са опасностима коришћења ових уређаја и на тај начин постаје потенцијална жртва искусних и далеко боље едукованих појединаца, који злоупотребљавају интернет и друштвене мреже. Због тога се као значајни егзогени фактори компјутерског криминалитета и испољавања криминалних активности на друштвеним мрежама јављају брзина развоја информационе технологије, масовност корисника друштвених мрежа, информатичка неписменост, несналажење и неприлагођавање новонасталим технолошким променама, непостојање свести о безбедносним ризицима коришћења интернета и друштвених мрежа. Масовност корисника друштвених мрежа последица је велике популарности ових услуга на интернету. Корисници бирају одређене друштвене мреже на основу својих афинитета, популарности појединих друштвених мрежа, једноставности коришћења и сл, али не обраћају пажњу на опасности и безбедносне ризике који су повезани са нападима на њихову приватност и осталим видовима злоупотребе. Велики број потенцијалних жртава охрабрује извршиоце јер су сигурни у успешност реализације својих активности. Уколико минимални проценат корисника одређене друштвене мреже на регионалном или локалном нивоу од укупне ппулације корисника, на пример 1%, постане жртва криминалних активности, услед великог броја

[596] Freiburger, Tina, Crane Jeffrey: The Internet as a Terrorist's Tool, A Social Learninig Perspective, наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, *op.cit.,* стр. 128

корисника ових мрежа криминалцима се исплати реализовање криминалних активности коришћењем могућности друштвених мрежа.[597]

Експанзији криминалних активности на друштвеним мрежама значајно доприноси анонимности (псеудоанонимност) корисника, коју омогућава сам концепт друштвених мрежа, јер је могуће креирање лажних профила или компромитовање постојећих профила. Псеудоанонимно или лажно представљање на друштвеним мрежама најчешће је повезано са преварама путем интернета, које су најраспрострањеније, али и са вршњачким насиљем, вербовањем жртви, прогањањем и другим облицима дигиталног насиља. Ипак, доминантан узрок превара путем интернета, поред анонимности извршилаца, је знатно отежано праћење дигиталних финансијских токова и утврђивање крајње дестинације средстава. Извршиоци интернет превара се користе најразличитијим методама за прибављање података о потенцијалним жртвама, које су најбољи извор информација јер посећујући разне рекламне сајтове или одговарајући на посебну врсту рекламних e-mail порука („спам") остављају своје личне податке и на основу прикупљеног материјала се планира превара.

Један од значајних егзогених криминогених фактора свакако је несклад између нормативног (законска регулатива која се односи на компјутерски криминалитет) и реалног (примена у пракси од стране полиције, јавног тужилаштва и судова). У нашем законодавству постигнут је велики напредак предвиђањем кривичних дела, која се односе на безбедност рачунарских података и осталих кривичних дела која у складу са Конвенцијом о високотехнолошком криминалу припадају компјутерском криминалитету, али, ипак, није посебно сагледана злоупотреба друштвених мрежа као облик компјутерског криминалитета, иако поједини облици криминалних активности на друштвеним мрежама постају све развијенији. С друге стране, треба имати у виду да је због велике тамне бројке, мала вероватноћа да ће ове криминалне активности бити откривене, што знатно отежава рад специјализованих државних органа на спречавању и сузбијању компјутерског криминалитета. Извршиоци кривичних дела користе лажне идентитете у online дружењу и

[597] Миладиновић, Александар; Петричевић, Владимир: „Криминогени аспект друштвених мрежа, Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал", Међународна научностручна конференција, Зборник радова, Лакташи 28-30. март 2012, стр. 260

мреже са јавним приступом, што знатно отежава откривање тачне локације извршења дела јер се врше са многих места широм света. Тежем откривању извршилаца доприноси и слаба међународна полицијска сарадња.

На безбедност на интернету и друштвеним мрежама утичу технички ресурси и ниво техничко технолошке структуре. Због тога се као један од значајниих фактора компјутерског криминалитета јавља неадекватна техничка опрема и недовољно познавање функционисања уређаја, који раде на принципима високе технологије, компјутерских система и мрежа, као и модерних телекомуникационих технологија. У области информационе технологије неопходна су специфична знања и искуства, посебно је важно стално праћење нових технологија, како би се у условима сталног развоја и експанзије, одржао ниво знања потребан за откривање и сузбијање компјутерског криминалитета и злоупотребе друштвених мрежа.

С друге стране, такође, треба указати на утицај недовољно развијене физичке и техничке сфере заштите информационих система. Овај аспект заштите подразумева коришћење мера које имају за циљ регулисање начина и техничких поступака којима се може умањити ризик од злонамерног нарушавања функционаности информационих система. Уколико контрола приступа рачунарима, софтверу и другим ресурсима где се чувају важни подаци, рутери и друге битне мрежне компоненте, није добро регулисана, може да дође до неовлашћеног приступа серверу. Недостатак техничких уређаја и средстава којима би се спречио неовлашћени приступ штићеном систему, отвара широке могућности за разне облике криминалних активности.

Недостаци у систему бежичног умрежавања такође могу утицати на испољавање великог броја криминалних активности на интернету и друштвеним мрежама. Приликом бежичног умрежавања неопходно је пажљиво урадити тестове за утврђивање опсега уређаја и осигурати да се снага преноса свих бежичних уређаја обавља на минимуму, који дозвољава ефикасно обављање операција. Ако се приликом бежичног умрежавања непажљиво бирају и инсталирају компоненте за бежично умрежавање, потенцијалним извршиоцима је олакшано повезивање на мрежу и прислушкивање. Узрок недозвољених активности може да буде и непоштовање одређених правила приликом инсталирања оперативних система. Правила се односе на: број инсталационих програма и процеса (што је већи број програма и процеса, већа

је вероватноћа да ће се искористити слабост система); број сервиса (постоји много сервиса који се користе и који успоравају систем и представљају претњу безбедности); протоколе; безбедносне исправке које дистрибутер објави; коришћење скенера слабих тачака да би се таква места открила и заштитила; и режим мрежних адаптера. Такође треба поштовати правила о постављању сложених лозинки за све кориснике налога, њихово често мењање; блокирање налога; уклањање и онемогућавање непотребних модема; надгледање, записивање, проверавање и детекција одрживости резервних копија и дупликата диска.[598]

Кадровски и материјални проблеми надлежних полицијских и правосудних органа за ефикасно и адекватно спровођење законских овлашћења, која су им поверена у вези са превенцијом и репресијом компјутерског криминалитета, такође у великој мери утичу на стварање повољних услова за криминалне активности везане за употребу интернета и друштвених мрежа. У том смислу треба сагледати и недостатак довољно ефикасног система надгледања интернета у циљу откривања кривичних дела компјутерског криминалитета, као и ефикасне платформе за пријављивање ових кривичних дела. При томе, приликом надгледања, пресретања и анализе порука, сакупљања порука, програма и рачунара у истражном поступку треба водити рачуна о постојању равнотеже између интереса заштите приватности и друштвеног интереса за кривично гоњење.

Међу егзогеним факторима компјутерског криминалитета посебно се издваја недостатак едукације о безбедности на интернету и друштвеним мрежама, концепту приватности и законима у области заштите података о личности и приватности, недостатак тренинга и обука, који објашњавају начине коришћења података о личности на мрежи, како се они могу злоупотребити и дефинисање опасности коју носи одређена врста понашања на интернету. Наведени садржаји се углавном занемарују и више пажње се посвећује теоријском рачунарству и програмским језицима. Наставни планови и програми у школама не садрже питања везана за информациону приватност и безбедно

[598] Путник, Ненад; Гаврић, Невена: „Мере и стратегије заштите информационих система од високотехнолошког криминала, Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал“, Међународна конференција, Зборник радова, Лакташи 28-30. март 2012, стр. 220 и 221

понашање корисника интернета и друштвених мрежа. Разни видови неформалног учења у великој мери могу подићи свест корисника о безбедносним ризицима.

4.2. Ендогени криминогени фактори

У литератури с као један од значајних ендогених фактора компјутерског криминалитета помиње ефекат online дезинхибиције. Ради се о попуштању социјалних норми и правила у интернет комуникацији, која иначе поштујемо у интеракцији са људима уживо. Приликом свакодневног коришћења интернет комуникације и друштвених мрежа, значи у сајбер простору људи чине и говоре оно што обично не би када комуницирају лицем у лице. Дезинхибиција може да се манифестује као *бенигна* (неуобичајена дарежљивост, љубазност, занемаривање својих потреба, помоћ другима и сл.) и као *токсична* (непристојно изражавање, љутња, мржња, претње, сајбер насиље и сл.), али у појединим случајевима разлика између њих није сасвим јасно испољена. Ефекат online дезинхибиције манифестује се у шест тачака: дисоцијативна анонимност, невидљивост, асинхроност, дисоцијативна имагинација, солипсистичка интројекција и минимизирање ауторитета.[599]

Дисоцијативна анонимност један је од главних фактора за ефекат дезинхибиције. Када нисмо потписани својим именом и презименом, можемо да се понашамо како нам је воља. Чак и када су корисничко име и мејл адреса видљиви, то може да завара ако је корисничко име смишљено e-mail адреса добијена од великог провајдера. Уколико то жели, особа може да сакрије поједине или све аспекте свог стварног идентитета. Анонимност утиче на већу слободу особе да се понаша девијантно и не поштује online забране, да не осећа никакву одговорност, да чак сматра да је такво понашање сасвим прихватљиво.

Невидљивост охрабрује кориснике да у сајбер простору посећују места и раде ствари за које у реалном простору не би имали довољно смелости. У текстуалном online окружењу, особе у контакту не морају да виде једна другу и то појачава ефекат дезинхибиције. У непосредном контакту обраћа се пажња на

[599] Сулер, Џон: „Ефекат онлајн дезинхибиције“, Е-волуција, бр. 11, 2005, http://www.bos.rs/cepit/evolucija/html/11/e-dezinhibicija.htm, претражено 28. 10. 2015. године

реаговање саговорника и прате се његови покрети и изрази лица. Све се то не види приликом комуникације у сајбер простору где особа не брине о томе како изгледа и звучи, што олакшава упуштање у делинквентно понашање.

Асинхроност значи да e-mail комуникација корисника и коуникација путем огласни табли није у интеракцији у реалном времену. Од слања поруке до одговора на њу може проћи дужи или краћи временски период, што такође има дезинхибиторни ефекат. Када информација стиже одложено, веће су могућности за непоштовање социјалних норми.

Дисоцијативна имагинација постоји када свесно или несвесно поједини корисници осећају да имагинарни каректери које су створили постоје у другачијем простору, у измишљеној димензији, одвојеној од реалног света. На тај начин раздвајају online фикцију и ofline чињенице и воде online живот као врсту игре у којој важе правила и норме које не важе у свакодневном животу. При томе, ове особе верују да када искључе рачунар нестаје и њихов имагинарни идентитет и све што су урадиле са тим идентитетом, што свакако није тачно.

Солипсистичка интројекција се јавља као последица одсуства комуникационих знакова приликом онлајн контакта. Особа може да има утисак да је online познаник део његовог интрапсихичког света и писана комуникација се доживљава као део сопствене имагинације. Свесно или несвесно појединац може другој особи да додели и одређену визуелну представу која одражава његово мишљење о изгледу и понашању те особе. У својој машти где се осећају сасвим безбедно, људи у online контакту се осећају слободним даураде ствари које никако не би урадили у реалном животу. Тако се текстуална комуникација путем интернета може да развије у убачену психолошку таписерију у којој „појединац сам тка ове измишљене улоге и то најчешће несвесно, манифестујући притом изражену дезинхибицију“.[600]

Мимизирање статуса и ауторитета показује да су у online комуникацији корисници интернета потпуно изједначени у могућностима да изразе себе. У реалном свету особе од ауторитета изражавају свој статус начином одевања, говора и другим статусним показатељима, што спречава

[600] *Ibid.*

многе људе нижег друштвеног статуса да изнесу своје мишљење. У online комуникацији је сасвим другачије: статус који особа има у реалном свету нема исти ефекат и утицај, а када су снаге изједначене и минимизиран утицај ауторитета, појединци су много чешће спремни да се понашају неприхватљиво

Спремност појединца да преко интернета или друштвених мрежа изрази сопствене ставове или изнесе интимне податке и емоције, зависи од индивидуалних разлика. Интензитет осећања, потреба и нагона утичу на подложност дезинхибицији. Стилови посебности се веома разликују с обзиром на снагу одбрамбених механизама и тенденцију ка суздржаности или изражајности. Још увек нема довољно истраживања о овој појави, али је извесно да су особе које карактерише хистрионски[601] стил реаговања чешће јако отворене и емотивне, док су компулсивне особе много суздржаније.[602]

У радовима појединих аутора наведени су узроци психолошког злостављања у сајбер простору, односно разлози за предузимање овог облика злостављања.[603] То су пре свега жеља за осветом, потреба за успостављањем моћи над другима у циљу контроле и ауторитета над њима, жеља за успостављањем моћи над другима због комнезације опажених сопствених мана, злостављање других из досаде или ради забаве, жеља за играњем улога. Жеља за осветом се јавља код оних сајбер злостављача који су жртве у реалном животу и мисле да на тај начин исправљају неправду, штите себе и друге од људи који због својих поступака „заслужују“ да буду виктимизирани. На тај начин и сами постају злостављачи а да тога нису свесни. Како би успоставили моћ и контролу над другима сајбер злостављачи користе електронску технологију за слање претећих и понижавајућих порука. Како би компензирали своје слабости у реалном свету, где су често жртве традиционалног злостављања, сајбер злостављачи застрашују и понижавају друге и виртуелном свету. Код појединих

---

[601] Код хистрионског поремећаја личности, особе имају сталну потребу за театралним понашањем (драматизацијом) и скретањем пажње на себе. О су шармантне, енергичне, духовите, друштвене особе али и импулсивне, склоне претераном флерту, манипулацији, несталне и захтевне према другима, *Видети*: Интернет магазин „Ваш психолог“, www.vaspsiholog. com/tag/histionski - poremećaj licnosti/, претражено 19. 12. 2015. године

[602] Приручник за родитеље – Глухи телефон, www.petzanet.hr/.../MODUL_4_roditelji-2_4.pdf, претражено 19. 12. 2015. године

[603] Спалевић, Жаклина: Карактеризација психолошког злостављања у cyber простору, INFOTEH-JAHORINA Vol. 12, March 2013, infoteh.elf.unssa.rs.ba/zbornik/2013/radovi/RSS-3/RSS-3-9.pdf, приступљено 14. 12. 2015. године

сајбер злостављача узрок њиховог недозвољеног понашања је жеља за забавом и разонодом. То су незреле и лабилне личности, које на овај начин јачају свој его; они ретко прете својим жртвама, чешће их исмевају и омаловажавају. Могуће је да се сајбер злостављање јави и услед потребе за давањем одговора на негативну комуникацију. Када особа прими поруку са негативним садржајем, има потребу да на њу одговори исто тако увредљиво и омаловажавајући не увиђајући да на тај начин и сама врши психолошко злостављање.

Међу ендогеним факторима компјутерског криминалитета и злоупотребе друштвених мрежа треба поменути и синдром интернет зависности и то специфичан вид интернет зависности, који се односи на компулсивну употребу веб сајтова за сајбер дечију порнографију.[604] Када се ради о ендогеним узроцима везаним за дечију порнографију, анализе показују да не постоји значајна узрочна повезаност између појединих психолошких црта личности (морални избор хедонистичке вредности, морални избор социјалних вредности, екстраверзија, неуротицизам, отвореност према искуству, разумност и савесност) и злоупотребе дечије порнографије. Остале психичке црте нису битно везане за интернет дечију порнографију. Експлоататорско манипулативне црте и ниске вредности моралног избора могу да се очекују због тога што особа која је укључена у дечију интернет порнографију извршава илегалне активности, па самим тим њен успех зависи од способности да манипулише и експлоатише различите људе и ствари преко интернета како би дошли до девијантних порнографских материјала. Ниске вредности моралног избора указују на то да они који конзумирају интернет дечију порнографију немају исте личне и моралне компасе попут осталих корисника интернета који знају да одреде шта је исправно а шта погрешно. Унутрашње вредности неке особе нису прописане друштвеним законима и правним одредбама, већ су заправо приватни морални избор. Корисници интернет дечије порнографије схватају можда да је њихово понашање друштвено забрањено, али не верују да је оно „погрешно“ за њих лично, за разлику од корисника порнографије која није дечија, који верују да је понашање везано за дечију порнографију морално погрешно и на друштвеном и на индивидуалном нивоу.[605]

---

[604] Ковачевић-Лепојевић, Марина: „Појам и карактеристике интернет зависности“, Специјална едукација и рехабилитација, Vol. 10, br. 4, Београд, стр. 621, http://www.casopis.fasper.bg.ac.rs/izdanja/SEIR2011/vol10br4/1Spec_Edu_i_Reh_ISTRAZIVANJA/4-Marina_Kovacevic_Lepojevic.pdf, претражено 09. 12. 2015. године

[605] Siegfrid Spellar Kathrin, Lovely Richard, Rogers Marcus: Self-Reported Internet Child Pornography Consumers. A Personality Assessment Using Bandura's Theory of Reciprocal

Узрочност дигиталне пиратерије поједини аутори повезују са теоријом самоконтроле.[606] Приликом понашања које се квалификује као дигитална пиратерија, особе са ниском самоконтролом, не поштују поверење исказано у уговору о лиценцирању између онога ко је створио дигитални медиј и онога који има ауторска права. За већину људи дигитална пиратерија је узбуђење, а интеренет једноставан уређај за манипулацију и спровођење дигиталне пиратерије. На тај начин ниска самоконтрола има директан утицај на вршење дигиталне пиратерије (Higgins, 2005, Higgins&Makin, 2004, Higgins et.al., 2005)[607]

Низак ниво самоконтроле доводи се у везу са прекомерним разоткривањем личних информација, чиме се стварају веће могућности за ризично понашање на интернету и друштвеним мрежама. Самопоштовање и друге црте личности (на пример, нарцизам) такође се могу довести у везу са понашањем људи на друштвеним мрежама, јер поједини људи користе ове друштвене мреже као један нови вид самопредстављања и самопромовисања којом потврђују личну вредност (Gonzalez i Hancock, 2011; Mehdizadeh, 2010; Stefanone et al., 2011; Wilson et.al, 2010). Друга теорија заговара да су људи под претпоставком анонимности, коју имају на интернету, подложнији мањој индивидуалности и инхибицији у сајбер окружењу, што може довести до одступања у њиховом понашању (Joinson, 1999; Kabay, 1998; Suler i Phillips, 1998).[608]

Determinism, наведено у Cyber Criminology,Exploring Internet Crimes and Criminal Behavior, *op.cit.,* стр. 72

[606] Gottfredson и Hirschi су 1990. формулисали теорију самоконтроле према којој је низак ниво самоконтроле на индивидуалном нивоу узрок криминалитета и девијантности. Ниска самоконтрола представља индивидуалну склоност ка криминалитету и девијантности, а може да буде резултат слабог или неефективног родитељства које дете искуси пре осме године живота. Како би се развио одређени ниво самоконтроле родитељи морају да развију емоционалну везу са својим дететом. Једном када се ова веза развије родитељи имају могућност да сакупе бихевијоралне информације о свом детету. Онда родитељи могу да анализирају ове информације како би одредили да ли је понашање девијантно или може да прерасте у девијантно. Када родитељи слабо или уопште не обављају ову улогу, дете има веће шансе да развије ниски степен самоконтроле. Особе са ниском самоконтролом склоније су извршавању једноставнијих и лакших задатака, чешће бирају физичке а не менталне активности, ангажоване су у ризичним понашањима, фокусиране на себе и не могу да контролишу свој темперамент. *Видети:* Gottfredson, M.and Hirschi, T.: A general theory of crime, Stanford, CA: Stanford University Press, *цит. према* Higgins, George: Value and Choice, Examining Their Roles in Digital Piracy, наведено у Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, *op.cit.*, стр. 141

[607] *op.cit.* , стр. 141

[608] Szde,Yu: „Анализа узрока понашања на facebooku, тест сајбер профилисања“, www.defendologija-banjaluka.com/defendologija33/2srp.pdf, претражено 09. 12. 2015. године

ГЛАВА III

ПРАВНА РЕГУЛАТИВА ЗА БОРБУ ПРОТИВ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА И КРИМИНАЛНИХ АКТИВНОСТИ НА ДРУШТВЕНИМ МРЕЖАМА

1. Међународноправни инструменти супротстављања компјутерском криминалитету

Компјутерски или високотехнолошки криминалитет све је заступљенији у свету и непрекидно прати развој информационих и комуникационих технологија. Експанзија кривичних дела из области високотехнолошког криминалитета нужно је наметнула потребу његовог регулисања на међународном плану. Нови облици овог криминалитета свакодневно се развијају у свим земљама света, због чега компјутерски криминалитет представља велику опасност, нарочито кроз транснационално криминално деловање. Као транснационални друштвени феномен компјутерски криминалитет погађа основне вредности сваког друштва. Он се врло тешко открива и још теже доказује и процесуира. Због тога постоји интерсе свих држава у свету да се на међународном плану донесу правни документи који би обавезивале државе потписнице да у своја кривично правна и кривичнопроцесна законодавства инкриминишу понашања која припадају компјутерском криминалитету и обезбеде доказе за његово откривање.

Интернационални карактер компјутерског криминалитета захтева координирану међународну акцију у борби против њега и то како са нормативног тако и са практичног и едукативног аспекта. Посебно треба нагласити да је компјутерски криминалитет повезан са најтежим облицима криминалитета, као што су организовани криминалитет и тероризам јер компјутер и информациона технологија представљају моћна средства извршења криивчних дела ових облика криминалитета. Борба против компјутерског криминалитета не може се ни замислити без укључивања целе међународне заједнице и ангажовања међународних институција. Напори да се на међународном плану успостави ефикаснија сарадња између држава у борби против компјутерског криминалитета дали су резултате у виду писаних

докумената: конвенција, препорука, резолуција и директива. Прихватањем правних стандарда донетих на међународном плану ствара се одговарајући амбијент и правни оквир за сузбијање компјутерског криминалитета у националним оквирима.

Најзначајнији правни инструменти у борби против компјутерског криминалитета настали су под окриљем ОУН, Савета Европе и Европске Уније и они ће, због свог значаја, у раду бити детаљније објашњени. Ипак, треба поменути и друге организације и регионалне иницијативе за креирање стратешких опредељења у супротстављању компјутерском криминалитету, које се на међународном плану преко својих радних тела залажу за борбу против компјутерског криминалитета (Интерпол, Канцеларија Уједињених нација за борбу против дроге и криминала - UNODC - United Nations Office on Drugs and Crime; група држава званих Г-8: Организација америчких држава - OAS - Organization of American States; Организација за економску сарадњу Азије и Пацифика APEC - Asia Pacific Economic Cooperation, Организација за економску сарадњу и развој - OECD - The Organization for Economic Cooperation and Development), Организација за европску безбедност и сарадњу OEBS[609] – Organizacion for Security and Co-operation in Europe OSCE)[610] и др.

Интерпол представља прву међународну организацију, која се после конференције у Паризу 1979. године,[611] посветила проналажењу механизама за кривичноправно регулисање и спречавање компјутерског криминалита. Важно је да ова организација указује на огроман потенцијал компјутерског криминалитета и да поседује оперативне приручнике са најновијим подацима и упутствима за истражитеље. У оквиру међународног пројекта реализованог 1980. и 1981. године, вршена су различита анкетирања у земљама које су чланице Интерпола. После завршеног истраживања у Паризу је 1981. године

[609] Још 1982. године основана је експертска група у циљу сагледавања стања легислативе у области високотехнолошког криминалитета са задатком да сачини одговарајуће препоруке за измену законских прописа у циљу усклађивања правних норми са реалним потребама. Као резултат ове активности ОЕБС је 1986. године усвојио Препоруку за усклађивање кривичних законика. Осим тога, ОЕБС сачињава листу недозвољених понашања у сајбер простору, која обухвата рачунарске преваре и фалсификате, оштећење рачунарских података и програма и неовлашћени продор у заштићени рачунарски програм или заштићени рачунарски систем.

[610] Misija OEBS-a u Srbiji, www.osce.org/sr/serbia, претражено 15. 08. 2015. године

[611] The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979, видети http://cybercrimelaw.net/documents/Strasbourg.pdf, претражено 01. 11. 2014. године

одржан први Интерпол тренинг семинар[612] на коме је учествовало 66 делегата из 26 земаља. На овом семинару је наведено неколико области везаних за употребу компјутера које нису адекватно кривичноправно нормиране.[613] Заједнички закључак учесника био је да је неопходно да се ради на развоју и хармонизацији кривичног законодавства које би спречио пораст компјутерског криминалитета у целом свету.

Допринос правној регулативи у области компјутерског криминалитета дала је и група Г-8, коју чине представници Канаде, Француске, Италије, Јапана, Русије, Уједињеног краљевства, Немачке и Сједињених америчких држава.[614]

Експертска група виших стручњака Г-8 за информатичке технологије у области транснационалног организованог криминалитета (The High Tech Subgroup of the G-8's Senior Experts on Transnational Organized Crime) 1998. године основала је и развила службу стручне подршке – Подгрупу за високотехнолошки криминал да би се бавила успостављањем непрестаних комуникација између центара за сајбер безбедност држава чланица, али и обуком особља и побољшањем државних правних система за борбу против компјутерског криминалитета. Подгрупа је била активна седам дана у недељи и двадесетчетири часа дневно, пружала је информације и помагала при вођењу истрага за кривична дела из домена високотехнолошког криминалитета.[615] Циљ оснивања овакве службе био је да органи овлашћени за процесуирање извршилаца кривичних дела компјутерског криминалитета што пре пронађу извршиоце ових дела и да их приведу правди. Група Г-8 је на Министарској

---

[612] The First Interpol Training Seminar for Investigators of Computer Crime, Paris, December 7-11, 1981, видети http://cybercrimelaw.net/documents/Strasbourg.pdf, претражено 08. 11. 2014. године Наведене су следеће области: модификација и брисање података, као и било какво другачије мењање података са намером да се они униште; присвајање или добијање података који припадају другом; неовлашћено коришћење туђег рачунара; измена рачунарских података или релевантних података који су предмет правног промета у намери да се изврши превара; неовлашћено и неауторизовано објављивање личних и других података.

[613] Schjolberg, Stein, *op.cit.,* , 2008.

[614] University of Toronto - G8 Information Centre, http://www.g8.utoronto.ca/, претражено 07. 11. 2014. године.

[615] Schjolberg, Stein: „The history of cybercrime 1979-2014“, Cybercrime research Institute vol. 9, 2014, стр. 44, https://books.google.rs/books?id=hmiWBQAAQBAJ&pg=PA44&lpg=PA44&dq=The+High+Tech+Subgroup+of+the+G8%27s+Senior+Experts+on+Transnational+Organized+Crime&source=bl&ots=K0vra34c11&sig=EvmCdwBvxHd5x9jDv0Ct86_qE&hl=sr&sa=X&ved=0CCYQ6AEwAWoVChMIgKzOprm6xwIVRT0aCh2yxAOC#v=onepage&q=The%20High%20Tech%20Subgroup%20of%20the%20G-8's%20Senior%20Experts%20on%20Transnational%20Organized%20Crime&f=false, претражено 20. 08. 2015. године.

конференцији земаља чланица Г-8 (која је одржана 1999. године у Москви) утврдила сет од три начела која би требало да се поштују приликом вођења кривичне истраге за дела из области високотехнолошког криминалитета и које свака држава чланица и друга заинтересована држава треба да имплементира у национално законодавство.[616]

Организација америчких држава (OAS) [617] донела је 2002. године Препоруку којом је формирана експертска група за проучавање кривичних дела компјутерског криминалитета. Задатак експертске групе био је да припреми за доношење правне иструменте и предлоге закона који би омогућили јачање сарадње целог америчког континента у борби против компјутерског криминалитета, са посебним освртом на заштиту права на приватност, заштиту података и информација, унификацији поступака кривичног гоњења и превенције ове врсте криминалитета. OAS и Латиноамеричка сарадња развијених мрежа (Latin American Cooperation of Advanced Networks - CLARA) донеле су бројне програме и иницијативе за сузбијање компјутерског криминалитета.

---

[616] Начела Г-8 поводом заједничке борбе против међународног организованог криминала која се односе на међународни приступ сачуваним компјутерским подацима, су: 1.чување постојећих података у компјутерском систему - једна држава може од друге да захтева да друга држава обезбеди брзо чување и обезбеђење рачунарских електронских података који постоје у компјутерских системима или код интернет провајдера, а који се налазе на њеној територији, а који су посебно осетљиви и подложни губитку или измени, а другој држави су неопходни ради претрага, копирања, одузимања или објављивања; 2. Пружање правне помоћи у поступку хитности – по пријему формалног захтева једне државе за омогућавање приступа, претраживања, копирања, одузимања или откривања података, или давања сачуваних података, замољена држава ће, у складу са својим националним законодавством, захтев испунити што хитније поштујући традиционалне принципе међународне правне помоћи, одређене ратификоване процедуре између тих држава или коришћењем других метода правне помоћи које су дозвољене законодавством замољене државе; 3. - Међудржавна сарадња ради омогућавања приступа сачуваним компјутерским подацима не захтева процедуру као код пружања међународне правне помоћи – једна држава не сме да одбије захтев друге државе докле год је то у складу са њеним националним законодавством, а тиче се приступа јавно доступним подацима, без обзира где се они географски налазе, као и приступању, претрази, копирању или потраживању података који се налазе у компјутерским системима замољене државе уколико та држава поступа по законима или добровољном пристанку особе која је овлашћена да такве податке даје, а откривање података је у најбољем интересу државе која је податке тражила.
Видети: Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow October 19-20, 1999, Annex 1, http://www.g8.utoronto.ca/adhoc/crime99.htm, претражено 07. 11. 2014. године.

[617] Препорука Организације држава Америке (Organization of American States (OAS)), 2002, http://www.oas.org/juridico/english/cyber.htm, претражено 12. 11. 2014. године.

Удружење за економску сарадњу Азије и Пацифика[618] састоји се из 21 државе чланице[619] које су у потпуности посвећене доношењу свеобухватне законодавне регулативе из области компјутерског криминалитета и информатичке сигурности, а у великој мери се ослањају на Резолуцију бр. 55/63 УН из 2000. године и Конвенцију Савета Европе о високотехнолошком криминалу бр.185 из 2001. године.

Удружење југоисточних азијских народа[620] чини десет држава[621] које су на састанку одржаном у Банкоку јануара 2004. године[622] препознале потребу да се ефикасном међународном правном сарадњом победи у борби против високотехнолошког криминалитета. На састанку одржаном на Брунејима 2008.године иницирано је усвајање резолуције о компјутерском криминалитету[623].

Рад и ангажовање међународних организација на сузбијању компјутерског криминалитета значајно су утицали на правну регулативу овог облика криминалитета у многим државама у свету. Правна регулатива компјутерског криминалитета почиње да се развија и усавршава почев од друге половине осамдесетих година, када су 1986. године у Сједињеним Америчким Државама донети Закон о интернет компјутерској превари[624] и Закон о приватности електронских комуникација.[625] Закон о заштити интернет

---

[618] Asian Pacific Economic Cooperation (APEC), www.apecsec.org, претражено 12. 11. 2014. године

[619] Аустралија; Брунеји; Канада; Кина; Хонг Конг; Индонезија; Јапан; Република Кореја; Малезија; Мексико; Нови Зеланд; Папуа Нова Гвинеја; Перу; Филипини; Русија; Сингапур; Таипеј; Тајланд; Сједињене Америчке Државе и Вијетнам.

[620] Association of Southeast Asian Nations (ASEAN), www.aseansec.org, претражено 12. 11. 2014. године

[621] Брунеји; Камбоџа; Индонезија; Лаос; Малезија; Мајнамар; Филипини; Сингапур; Тајланд и Вијетнам.

[622] First ASEAN Plus Three Ministerial Meeting on Transnational Crime (AMMTS+3), http://www.asean.org/communities/asean-political-security-community/item/joint-communique-of-the-first-asean-plus-three-ministerial-meeting-on-transnational-crime-ammtc3-bangkok-10-january-2004, претражено 12. 11. 2014. године.

[623] The Association of Southeast Asian Nations, http://www.asean.org/communities/asean-political-security-community/item/joint-communique-of-the-28th-asean-chiefs-of-police-conference-brunei-darussalam-25-29-may-2008, претражено 12. 11. 2014. године.

[624] Закон о интернет компјутерској превари Сједињених Америчких Држава - 18 U.S. Code § 1030 Computer Fraud and Abuse Act (CFAA), http://www.law.cornell.edu/uscode/text/18/1030, претражено 02. 11. 2014. године.

[625] Закон о приватности електронских комуникација Сједињених Америчких Држава - 18 U.S. Code § 2510-22 - Electronic Communications Privacy Act of 1986 (ECPA), http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119, претражено 02. 11. 2014. године.

приватности деце,[626] који је донет 1998. године, предвиђена да интернет базе не смеју да сакупљају податке о деци млађој од 13 година, па је због тога на бројним друштвеним мрежама установљено је старосно ограничење на минимум 13 година старости.

Реформа законодавства у области компјутерског криминалитета је затим настављена у Аустралији[627] и Великој Британији, где је 1988. године донет Закон о компјутерском криминалу.[628]

Борба против компјутерског криминалитета почела је у Европи пар година касније и утемељена је, пре свега, на значајним међународним документима. Многе земље су од тада измениле и ускладиле своја национална кривична законодавства са документима који су донети на међународном нивоу. Међу првима је то, поред Велике Британије учинила и Холандија, где је 1993. године донет Закон о компјутерском криминалу.[629] У Немачкој је 1970. године у покрајини Есен донет Закон о заштити података, али су тек 1977. године у савезном Закону о заштити података биле предвиђене кривичноправне санкције за заштиту аутоматске обраде података. Посебним Кривичним законом за сузбијање привредног криминалитета 1988. године предвиђен је низ кривичних дела компјутерског криминалитета, као што су: крађа података, компјутерска шпијунажа, компјутерска превара, фалсификовање података, обмана у правном промету при обради података, промена података и компјутерска саботажа. Низ кривичних дела компјутерског криминалитета регулисана су француском кривичним законом, али посебним Законом о заштити података из 1978. године уређена је обавеза свих корисника банака да се за свако отварање нове базе података морају обратити писаним захтевом Комисији за информатику и слободу грађана за одобрење.[630]

---

[626] Закон о заштити интернет приватности деце Сједињених Америчких Држава - The Children's Online Privacy Protection Act (COPPA), http://www.coppa.org/coppa.htm, претражено 12. 08. 2013. године.

[627] Закон о компјутерском криминалу Аустралије - Malicious Communications Act 1988, http://www.neiladdison.pwp.blueyonder.co.uk/law/matcomm.htm, претражено 02. 11. 2014. године

[628] Закон о злонамерним комуникацијама Велике Британије - Malicious Communications Act 1988, http://www.legislation.gov.uk/ukpga/1988/27/contents/enacted, претражено 02. 11. 2014. године

[629] Закон о компјутерском криминалу Холандије - Computer Crime Act (Wet computercriminaliteit), http://www.ejcl.org/143/art143-10.pdf, претражено 02. 11. 2014. године.

[630] Цит. према Шетка, Гојко; Ратковић, Жељко: Високотехнолошки криминал у Републици Српској, Зборник радова, међународна научностручна конференција, Сузбијање криминала и

Неке од држава чланица Уније Афричких земаља[631] попут Маурицијуса, Јужноафричке републике и Замбије су у своја национална законодавства већ имплементирале правне одредбе о кривичним делима високотехнолошког криминалитета. Боцвана је донела Закон о компјутерском криминалитету 2007. године,[632] Уганда 2008. године (ревидиран 2011. године),[633] Алжир 2009. године,[634] док су Замбија, Зимбабве, Јужна Африка, Малави и Мозамбик хармонизацију закона о високотехнолошком криминалу отпочеле 2005. године.[635]

Државе организоване кроз Лигу арапских држава[636] и Уједињени Арапски Емирати (2006)[637] такође су правно регулисале област компјутерског криминалитета.

Народна Република Кина, Русија, Казахстан, Киргистан, Таџикистан и Узбекистан су 2001. године основали Шангајску организацију за сарадњу[638] чији је циљ борба против тероризма, сепаратизма и екстремизма, при чему се под тероризмом подразумева и напад на информатичку сигурност. [639]

европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28 - 30. 03. 2012. године, стр. 210 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

631 *Видети* Africa Union www.africa-union.org, претражено 12. 11. 2014. године I http://www.au.int/, претражено 23. 07. 2015. године

632 Закон о компјутерском криминалитету Боцване (Cybercrime Bill for Botswana), видети Molokomme, L. Athaliah: „The Botswana Experience with cybercrime legislation and other measures", Speaking notes at the opening session of the Octopus Conference on Cooperation Against Cybercrime - Strasbourg, France, 6th June, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus2012/presentations/Octopus_2012_Botswana.pdf, претражено 20. 11. 2014. године.

633 Закон о компјутерском криминалитету Уганде (The Computer Misuse Bill), http://www.hingx.org/Share/Details/774, претражено 20. 11. 2014. године

634 Закон о компјутерском криминалитету Алжира (Cybercrime Bill for Algeria), https://algerianreview.wordpress.com/2010/01/09/algeria-cybercrime-law/, претражено 20. 11. 2014. године.

635 *видети* Cyber Crime Law, http://www.cybercrimelaw.net/AU.html, претражено 20. 11. 2014. године

636 *видети* Arab League Online, www.arableagueonline.org, претражено 20. 11. 2014. године

637 Закон о компјутерском криминалитету Уједињених Арапских Емирата (United Arabic Emirates federal cyber crimes law (Law No. 2 of 2006 Concerning Combating Information Technology Crimes)), 2006., http://www.lexology.com/library/detail.aspx?g=1d072cdf-3cd5-4ad9-8c54-28c045057d02, претражено 20. 11. 2014. године.

638 Shanghai Cooperation Organisation (SCO), www.sectsco.org, претражено 20. 11. 2014. године

639 Шангајска Конвенција о борби против тероризма, сепаратизма и екстремизма (The Shanghai Convention on combating terrorism, separatism and extremism), 2001, http://eurasiangroup.org/files/documents/conventions_eng/The_20Shanghai_20Convention.pdf, претражено 20. 11. 2014. године.

Може се констатовати да је на међународном плану у погледу нормативног регулисања компјутерског криминалитета постигнут значајан напредак, али да и даље постоје значајни проблеми који се односе на међународну сарадњу и глобалне напоре за сузбијање компјутерског криминалитета.[640]

1.1. Активност Организација Уједињених Нација на сузбијању компјутерског криминалитета

Уједињене нације су у оквиру рада Генералне скупштине усвојиле неколико резлуција које се баве високотехнолошким криминалитетом. Ове резолуције немају обавезујућу снагу за државе чланице и углавном су декларативног карактера, али их треба поменути јер садрже позив свим државама да што пре усагласе законодавстве у овој области како би се елиминисале тзв. „сигурне државе“ за компјутерски криминалитет у којима штетна понашања везана за злоупотребу компјутера, информационих и комуникационих технологија нису инкриминисана и санкционисана. Рад на пољу правног регулисања компјутерског криминалитета ОУН су започеле 1990. године, када је усвојена Резолуција о законодавству у области компјутерског криминалитета[641] на VII Конгресу УН о спречавању криминала и поступању са преступницима (8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders) одржаном у Хавани. После усвајања ове Резолуције, 1994. године

[640] Као најважнији проблеми наводе се: различито правно дефинисање радњи извршења кривичних дела компјутерског криминалитета; недовољна обученост полицајаца, тужилаца и судија који поступају у предметима компјутерског кримиалитета; неусклађеност процесних правила у кривичним законима када се ради о истрази и процесуирању кривичних дела компјутерског криминалитета; нефункционисање или непостојање међународне правне помоћи. Видети опширније: Бејатовић, Станко: Високотехнолошки криминал и кривичноправни инструменти супротстављања, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28 - 30. 03. 2012. године, стр. 22, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[641] Резолуција Уједињених Нација о законодавству у области компјутерског криминалитета (UN resolution on computer crime legislation), http://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf, претражено дана 11. 11. 2014. године

донет је Приручник ОУН о спречавању и контроли компјутерског криминала,[642] а затим маја 1998. године Женевска резолуција о злоупотреби интернета у сврху сексуалне експлоатације[643]. Женевска резолуција је констатовала да је Интернет у том моменту најнерегулисанија комуникациона мрежа у свету са новим технологијама које представљају велики изазов за национално и међународно регулисање и примену и алармирала да се у циљу сексуалне забаве на Интернету промовишу различити видови сексуалне експлоатације. У циљу смањења ових појава, Резолуција садржи препоруке како би утицала на смањење трговине људима, проституције и сексуалне експлоатације на Интернету.[644]

Генерална скупштина ОУН је 2000. године усвојила Резолуцију о борби против злоупотребе информационих технологија.[645] У овој Резолуцији истакнут је значај појединих мера у борби против против злоупотребе информационих технологија.[646]

---

[642] Приручник УН о спречавању и контроли компјутерског криминала (United Nations Manual on the Prevention and Control of Computer-related Crime), 1994, http://www.uncjin.org/Documents/EighthCongress.html, претражено 11. 11. 2014. године

[643] Резолуција Уједињених Нација (тзв.Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације (UN Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation), http://www.uri.edu/artsci/wms/hughes/ppr.htm, претражено 05. 03. 2015. године

[644] У препорукама је сугерисано владама држава потписница и невладиним организацијама да, као приоритет размотре, допуне и примене постојеће законе или донесу нове законе како би се спречила злоупотреба интернета за трговину, проституцију и сексуалну експлоатацију жене и деце; наставе истрагу у вези са злоупотребом интернета за сврхе промовисања и/или спровођења трговине, проституције и сексуалне експлоатације жена и деце; предузму енергичније мере у циљу елиминације трговине људима, експлоатације проституције и сексуалне експлоатације на интернету; развију образовне програме, политику и законе који се тичу коришћења интернета од стране корисника проституције; спроведу истрагу и користе као евиденцију кривичних дела и аката дискриминације рекламирање, коресподенцију и друге видове комуникације преко интернета који се користе у циљу промовисања сексуалне трговине, проституције, сексуалног туризма, трговине невестама и силовања; развију добру сарадњу на нивоу националних и регионалних органа криминалистичких служби у борби против ескалирања трговине и проституције жена и деце, глобализације ове индустрије и злоупотребе интернета за промовисање и спровођење аката сексуалне трговине, сексуалног туризма, сексуалног насиља и сексуалне експлоатације.

[645] Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија (UN resolution A/res/55/63 on combating the criminal misuse of information technologies), 2000, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, претражено 11. 11. 2014. године

[646] Као најзначајније мере наведене су две мере: прва да државе морају да обезбеде такве законе и праксу које ће елиминисати свако могуће „уточиште“ за оне који у кривичноправном смислу злоупотребљавају информационе технологије; и друга да правни систем мора да штити и поштује поверљивост, интегритет и доступност електронских података и рачунарских система, како не би дошло до њихове злоупотребе и неовлашћеног коришћења и како би сваки учинилац оваквог кривичног дела био санкционисан.

Резолуција је ревидирана 2001. године (*Резолуција бр. 55/63* од 22.1.2001)[647] када су се државе чланице ОУН усагласиле око десет мера у борби против компјутерског криминалитета. Као најважније предложене мере могу се издвојити: координација свих заинтересованих држава у вези са сарадњом у истрази и гоњењу међународних случајева злоупотребе информационих технологија; размењивање информација између држава и сарадња приликом решавања проблема везаних за компјутерски криминалитет; едукација и савремени методи обуке лица ангажованих на откривању и кривичном гоњењу извршилаца компјутерског криминалитета; упознавање јавности са опасностима које прете из сајбер простора и указивање на мере превенције; коришћење информационих технологија за откривање криминалних понашања и др. Резолуција садржи и упозорење државама да у борби против компјутерског криминалитета мора да се очува баланс између индивидуалних права и слобода гарантованих сваком појединцу, са једне стране, и права држава да кривично гони извршиоце кривичних дела, са друге стране.[648]

Резолуција Генералне скупштина ОУН[649] усвојена 23. 01. 2002. године указује на потребу да се приликом усвајања закона, као и приликом утврђивања политика кривичног гоњења, узму у обзир резултати рада Комисије за превенцију криминала и кривично правосуђе, као и других релевантних међународних организација.

Економско социјални савет ОУН донео је 26. 07. 2007. године Резолуцију 2007/20[650] и позвао државе чланице да модернизују национално законодавство новим инкриминацијама с обзиром на драматичан пораст транснационалног привредног криминалитета и у вези са тим употребу модерних рачунарских

[647] Ревидирана Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија (UN resolution A/res/55/63 on combating the criminal misuse of information technologies), 2001, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, претражено 11. 11. 2014. године

[648] Ромић, Миодраг; Грбић-Павловић Николина: Међународноправни документи којима се уређује област високотехнолошког криминала, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28 - 30. 03. 2012. године, стр. 196, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

[649] Резолуција Уједињених Нација A/res/56/121 о борби против злоупотребе информационих технологија (UN resolution A/res/56/121 on combating the criminal misuse of information technologies), 2002, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, претражено 20. 08. 2015. године

[650] Резолуција 2007/20 од 26. 07. 2007. године, www.un.org/.../ecosoc/.../2007 /Resolution%2020, претражено 25. 04. 2015. године

технологија као средства за извршење ових кривичних дела. Националним законодавствима је предложено да предвиде као кривична дела неовлашћену употребу или израду идентификационих докумената, као и података о идентитету. Такође је постигнута сагласност да се питања привредног криминалитета и злоупотребе идентитета размотре у оквиру рада Комисије за превенцију криминалитета и кривично правосуђе ОУН.

На глобалном плану ОУН се кроз рад својих специјализованих тела и радних група активно укључила у сектор безбедности информатичког друштва. Једно од најзначајнијих специјализованих тела ОУН и једна од најактивнијих институција ОУН домену борбе против високотехнолошког криминалитета, којој је поверена водећа улога у поступку хармонизације националних законодавстава и безбедности у сајбер простору, је Међународна телекомуникациона унија (International Telekommunication - ITU), чије је седиште у Женеви у Швајцарској. Ова институција је свој активни рад започела маја 2007. године, када је донет Меморандум о глобалној сајбер безбедности (*A Global Cybersecurity Agenda - GCA of the International Telecommunication Union*),[651] у циљу стварања глобалног оквира за дијалог и међународну сарадњу приликом предлагања стратегије за повећање безбедности у сајбер простору. Платформа садржи седам главних стратешких циљева, од којих је најбитнији доношење одговарајуће правне регулативе и њена инкорпорација у национална законодавства.

Борбу против високотехнолошког криминалитета ОУН спроводе у још неколико својих организација, међу којима је најзначајнија *Канцеларија УН за контролу наркотика и превенцију криминала (United Nations Office on Drugs and Crime – UNDOC)*[652] и *Канцеларија УН за послове разоружања (United Nations Office for Disarmament Affairs UNODA)*. UNDOC се посебно бави криминалном злоупотребом идентитета, промовисањем легислативе о високотехнолошком криминалитетом и обуком припадника полиције и других органа гоњења, док

[651] Глобална платформа о сајбер сигурности Међународне телекомуникационе уније (Global Cybersecurity Agenda (GCA) of the International Telecommunication Union), www.itu.int/osg/csd/cybersecurity/gca, претражено 11. 11. 2014. године

[652] Организација је основана 1997. године у циљу решавања међународних проблема и питања забрањене трговине наркотицима, превенцији криминалитета и међународног тероризма. Видети у: United Nations Office of Drugs and Crime, 2008, www.undoc.org/en/about-undoc/index, претражено 15. 08. 2015. године

UNODA, поред осталих активности укључује у своју делатност питања везана за информациони рат и сајбер тероризам.

Новембра 2005. године донета је Туниска агенда[653] на Светском самиту УН о информатичком друштву (World summit on the information society - WSIS). Посебно треба поменути као веома значајне параграфе 40 и 42 Туниске агенде, којима се гарантује стабилност и сигурност интернета, промовише борба против компјутерског криминалитета, обавеза заштите и поштовања права на приватност и слободе изражавања (пар. 42) и којима се све земље позивају да сарађују у стварању неопходног правног оквира у оквиру кога би се водила истрага и кривично гоњење починилаца дела компјутерског криминалитета (пар. 40).

Октобра 2007. године формирана је експертска група са више од сто чланова, која је јуна 2008. године допунила и разрадила платформу супротстављања компјутерском криминалитету кроз пет области: законодавне мере, техничке и процедуралне мере, организациона структура, стварање предуслова и међународна сарадња. Главни задатак који је ова експертска група имала био је да се постигне консензус на међународном плану по питању рачунарске безбедности и безбедности електронских података и како би се ефикасно решавао проблем компјутерског криминалитета.

Рад на легислативи из области компјутерског криминалитета наставила је 2010. године Генерална скупштина Уједињених Нација усвајањем Резолуције 65/230,[654] у којој је предложено да се формира међувладина експертска група која би спровела свеобухватну студију о компјутерском криминалитету и о томе како државе реагују на поједине случајеве ове врсте криминалитета.[655] Студија је имала за циљ да сагледа и ојача постојеће механизме реаговања на компјутерски криминалитет, да предложи начине за побољшање постојећих

---

[653] Туниска агенда бр.WSIS-05/TUNIS/DOC/6 (Rev. 1) за информатичко друштво (Tunis agenda no. WSIS-05/TUNIS/DOC/6 (Rev. 1) for the information society), 2005, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, претражено 12. 11. 2014. године

[654] Резолуција Уједињених Нација 65/230 (UN General Assembly resolution 65/230), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement, 2010, претражено 12. 11. 2014. године

[655] Comprehensive Study on Cybercrime – Draft, United Nations office on drugs and crime, Vienna, February 2013, United Nations, New York 2013, стр. Ix, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, претражено 12. 10. 2014. године

механизама као и да укаже на начине на који је могуће остварити превенцију компјутерског криминалитета.[656] Свеобухватност студије се огледа у томе што је проблем компјутерског криминалитета сагледан из перспективе влада, приватног сектора, научне елите и међународних организација. Резултати су груписани у осам поглавља која се односе на повезаност између приступа интернету и компјутерског криминалитета, компјутерски криминалитет у најширем смислу, правну регулативу компјутерског криминалитета, санкционисаност компјутерског криминалитета, улогу полиције у вођењу истраге за дела компјутерског криминалитета, електронске доказе у кривичним поступцима, међународни правну помоћ у области решавања случајева компјутерског криминалитета и превенцију компјутерског криминалитета.

1.2. Допринос Савета Европе у регулисању компјутерског криминалитета

Хронолошки посматрано, прва иницијатива да се на међународном нивоу регулише и санкционише компјутерски криминалитет настала је 1976. године од стране Савета Европе, када је одржана Европска конференција о криминолошким аспектима привредног криминалитета у Стразбуру,[657] када је први пут превара препозната и као облик компјутерског криминалитета.

Савет Европе је био једна од првих међународних организација које су покренуле иницијативу за стварање правних претпоставки за сузбијање компјутерског криминалитета удруженим напорима више земаља: у области кривичног права, одржано је преко двадесет конвенција и усвојено је више од осамдесет препорука. Савет министара (Committee of Ministers), састављен од министара иностраних послова држава чланица Савета Европе, 1989. године је усвојио Препоруку о криминалним активностима везаним за употребу рачунара

---

[656] Основни закључци наведени у студији били су: да се изврши утицај на национална законодавства да доведу до хармонизације са међународним прописима из ове области; да се све земље придржавају прописа и допуштених средстава међународне правне помоћи у кривичним стварима са иностраним и међународним елементом, а посебно када је реч о компјутерском криминалитету и обезбеђивању електронских доказа; регулисати какву улогу треба да има место/локација на којој се доказ налази; да се унапреде и усаврше мере спречавања настанка дела компјутерског криминалитета.

[657] A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, стр. 225 - 229, https://openlibrary.org/works/OL11001385W/Criminological_aspects_of_economic_crime, претражено 08. 11. 2014. године

89(9),[658] којом су државе чланице позване да размотре увођење нових прописа који се односе на сузбијање и санкционисање компјутерског криминала. Препорука је садржала „листу минимума“ дела која морају у националним законодавствима бити препозната и инкриминисана као кривична дела: рачунарска злоупотреба, рачунарски фалсификат, оштећење рачунарских података или рачунарских програма, рачунарска саботажа, неовлашћени приступ, неовлашћено ометање, неовлашћено копирање заштићеног рачунарског програма и неовлашћено копирање топографије.[659] Конвенција о заштити права појединаца у вези са аутоматском обрадом личних података, која је ступила на снагу 1. октобра 1985. године, имала је за циљ јачање правне регулативе због пораста употребе рачунарске технологије у административне сврхе.

Препоруку за кривичнопроцесно право у вези са информационим технологијама R(95)13 бр. 95,[660] усвојио је Савет Европе 11. септембра 1995. године. У Препоруци се користи термин „злочини повезани са информационом

---

[658] Препорука Савета Европе о криминалитету везаном за рачунаре бр. 89 (9), (Council of Europe Computer-related crime Recommendation No. R (89) 9, 1989) http://www.oas.org/juridico/english/89-9&final%20Report.pdf, претражено 07. 11. 2014. године и 29. 11. 2014. године

[659] *Рачунарска злоупотреба* (унос, измена, брисање или потискивање рачунарских података или програма, као и остале врсте мешања у обраду података које утичу на њен резултат, чиме се изазива економски или имовински губитак другог лица са намером да се стекне незаконита економска добит за себе или треће лице - алтернатива - са намером да се то лице лиши имовине на незаконит начин);
Рачунарски фалсификат (унос, измена, брисање или потискивање рачунарских података или програма, као и остале врсте мешања у обраду података на рачунару или под условима, предвиђеним домаћим законом, који би представљао дело фалсификата да је почињен у односу на класичан предмет таквог кривичног дела);
Оштећење рачунарских података или рачунарских програма (бесправно брисање, оштећивање, кварење или потискивање рачунарских података или рачунарских програма);
Рачунарска саботажа (унос, измена, брисање или потискивање рачунарских података или рачунарских програма или мешање у рачунарски систем са намером да се онемогући функционисање рачунара или телекомуникационог система);
Неовлашћени приступ (бесправан приступ рачунарском систему или мрежи кршењем мера безбедности);
Неовлашћено ометање (бесправно ометање техничким средствима улазне, излазне или комуникације унутар рачунарског система или мреже);
Неовлашћено копирање заштићеног рачунарског програма (бесправно копирање, дистрибуција или јавно објављивање рачунарских програма заштићених законом);
Неовлашћено копирање топографије (бесправно копирање законом заштићене топографије, полупроводничког производа или бесправно комерцијално коришћење или увоз у те сврхе топографије или полупроводничког производа направљеног коришћењем топографије).

[660] Recommendation No. R (95) 13 of the Committee of Ministers to Member States concering problems of Criminal Procedural Law connected with Information Technology, www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp, претражено 07. 11. 2014. године

технологијом“ *(Offences connected with Information Tehnology – IT offences IT crimes)* и наводи се да, у фази истраге за било које кривично дело повезано са информационом технологијом, овлашћени органи морају добити приступ свим информацијама које се обрађују или преносе комјутерским системима. Препорука садржи осамнаест основних принципа борбе против компјутерског криминалитета и представља први покушај међународног дефинисања процедура проналажења и заплене, надгледања, прикупљања и оцене електронских доказа, шифровање података и установљавања принципа међународне правне помоћи у области кривичних дела компјутерског криминалитета путем сарадње држава на међународном плану.

У оквиру Савета Европе настала је за сада једина међународна конвенција која уређује питања везана за високотехнолошки криминалитет на наднационалном нивоу – Конвенција о високотехнолошком криминалу бр. 185 (Будимпешта, 2001) Заједно са Додатним протоколом који се односи на инкримисање дела расистичке и ксенофобичне природе извршених путем компјутера (Страсбур, 2005), Конвенција представља основни правни извор о високотехнолошком криминалу на европском нивоу.

Поред Конвенције значајни међународни документи које је усвојио Савет Европе су: Конвенција о заштити права појединаца у вези са аутоматском обрадом личних података,[661] Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања,[662] Конвенција о спречавању тероризма[663] и Препорука Савета министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама.[664]

---

[661] Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података („Сл.лист СФРЈ – Међународни уговори“ бр. 1/92, „Сл.лист СЦГ-Међународни уговори, бр.11/2005-др.закон и „Сл. галсник РС – Међународни уговори“ бр. 98/2008-др. Закон и 12/2010).

[662] Закон о потврђивању Конвенције о заштити деце од сексуалне експоатације и сексуалног злостављања („Службени гласник РС – Међународни уговори“ бр. 1/10).

[663] Закон о потврђивању Конвенције Савета Европе о спречавању тероризма („Службени гласник Републике Србије – Међународни уговори бр. 19/2009).

[664] Препорука Савета Министара Савета Европе CM/Rec(2012)4 државама чланицама која се односи на заштиту људских права на друштвеним мрежама (Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services), 2012, https://wcd.coe.int/ViewDoc.jsp?id=1929453, претражено 09. 07. 2014. године

1.2.1. Конвенција Савета Европе о високотехнолошком криминалу 185 из 2001. године са Додатним протоколом

а) Значај Конвенције Савета Европе о високотехнолошком криминалу 185 и Додатног протокола. Конвенција Савета Европе о високотехнолошком криминалу 185 из 2001. године (CETS 185 у даљем тексту Конвенција) и Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система (Стразбур, 28.01.2005),[665] представљају прве међународне документе којима се регулише материјалноправни, процесноправни, организациони и међународни оквир кривичних дела извршених путем интернета и других рачунарских мрежа. Усвајање ових докумената резултат је иницијативе Савета Европе формално покренуте 1996. године оснивањем Комитета стручњака за криминал у сајбер простору. Задатак Комитета била је анализа кривичних дела која се могу извршити путем телекомуникационих мрежа, првенствено Интернета, да би се на основу анализе сачинио Нацрт међународне Конвенције. Фебруара 1997. године формиран је Комитет експерата о криминалу у сајбер простору (Committee of experts on crime in cyber-space PC-CY), чији је основни задатак био да се испита распрострањеност и појавни облици компјутерског криминалитета, дефинишу уочени преступи, утврде надлежности, предложе механизми заштите рачунарских података и дефинишу обавезе и одговорности интернет провајдера за податке који се шаљу преко њихових мрежа.

Разлози за доношење Конвенције су многобројни: постојање ризика да се због дигитализације, конвергенције и сталне глобализације рачунарске мреже и електронске информације могу користити и за извршење кривичних дела и да докази који се односе на таква дела могу бити сачувани и пренесени преко тих мрежа; потреба међународне сарадње између држава због транснационалног карактера високотехнолошког криминалитета; потреба заштите легитимних

---

[665] Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система („Службени гласник РС”, бр. 19/2009) и Додатни протокол уз Конвенцију Савета Европе о високотехнолошком криминалитету бр.185 који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених путем компјутерских система (Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems), 2005, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, претражено 09. 07. 2014. године

интереса у коришћењу и развоју информационе технологије; олакшавање откривања, истраге и гоњења кривичних дела компјутерског криминалитета на националном и међународном нивоу јер је тамна бројка веома велика; као и потреба поштовања и заштите права на приватност, личних података, сопственог мишљења и слободе изражавања.

Значај Конвенције је пре свега у томе што је њено доношење омогућило националним законодавствима да на темељу одредби Конвенције развију сопствену мрежу борбе против компјутерског криминалитета. Конвенцију је до 16.08.2015.године потписало 47 држава чланица Савета Европе, а затим су је ратификовале све државе потписнице осим Андоре, Грчке, Ирске, Лихтенштајна, Монака и Шведске. [666]

Државе из окружења које су потписале и ратификовале Конвенцију су:

- Албанија - потписала 2001. и ратификовала 2002. године;
- Аустрија - потписала 2001. и ратификовала 2012. године;
- Босна и Херцеговина - потписала 2005. и ратификовала 2006. године;
- Бугарска - потписала 2001. и ратификовала 2005. године;
- Грчка - потписала 2001. године и још увек је није ратификовала;
- Мађарска - потписала 2001. и ратификовала 2003. године;
- Македонија- потписала 2001. и ратификовала 2004. године;
- Румунија - потписала 2001. и ратификовала 2004. године;
- Словенија - потписала 2002. и ратификовала 2004. године;
- Хрватска - потписала 2001. и ратификовала 2002. године,
- Црна Гора - потписала 2005. у оквиру постојања Државне заједнице Србије и Црне Горе, а ратификовала 2010. године.

Чињеница да су Конвенцију потписале и поједине земље које нису чланице Савета Европе указује на то колики је значај овог међународноправног документа за ефикасно сузбијање високотехнолошког криминалитета. Укупно 21 држава која није чланица Савета Европе је потписала, а 8 држава је ратификовало Конвенцију - Сједињене Америчке Државе су потписнице од 2001. године, а ратификовале су је 2006. године; Канада је потписала 2001. а

[666] Council of Europe – Treaty Office, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, претражено 09. 11. 2014. године и 16. 08. 2015. године

ратификовала 2015. године; Јапан је потписао 2001. године а ратификовао 2012. године; Јужноафричка Република је потписала 2001. године и још увек није ратификовала, док је Аустралија 2012. године Конвенцију ратификовала без потписивања.[667]

Република Србија је 7. априла 2005. године у Хелсинкију потписала Конвенцију и Додатни протокол у време постојања Државне заједнице Србије и Црне Горе, а 2009. године Народна скупштина Републике Србије је ратификовала оба документа.[668] Обавеза примене ратификоване Конвенције почела је августа 2009. године. Ови документи су послужили као основа за доношење одговарајућих криивчноправних и кривичнопроцесних прописа, а утицали су и на формирање посебних државних органа специјализованих за борбу против компјутерског криминалитета. Међутим, и поред значајног успеха у националном правном регулисању, поједине области су и даље остале правно нерегулисане и несанкционисане.

У Додатном протоколу (Поглавље II – чл. 3 - 6) утврђена је обавеза страна уговорница да на националном нивоу у кривичним законима предвиде кривична дела која нису предвиђена Конвенцијом: ширење расистичког и ксенофобичног материјала преко рачунарских система, претња мотивисана расизмом и ксенофобијом извршена преко рачунарског система, увреда мотивисана расизмом и ксенофобијом пласирана преко рачунарског система (јавно вређање преко рачунарског система лица или групе лица који се разликују по раси, боји коже, наследном, националном или етничком пореклу или вери), порицање, значајно умањивање, одобравање или оправдавање геноцида или злочина против човечности учињено уз помоћ рачунарског система.[669] За постојање свих наведених кривичних дела потребно је да су

---

[667] Council of Europe – Treaty Office, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, претражено 09. 11. 2014.године и 31. 07. 2015. године

[668] Закон о потврђивању Конвенције о вискотехнолошком криминалу и Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система („Службени гласник РС“ 19/2009)

[669] *Ширење расистичког и ксенофобичног материјала преко рачунарских система* подразумева сваку радњу којом се овакав материјал чини доступним јавности коришћењем рачунара, односно рачунарског система (слање на већи број e-mail адреса или постављање на интернет презентацију). Државама је остављено да предвиде кривичну одговорност за овакав поступак или да ставе резерве на она понашања која су према њиховом унутрашњем праву дозвољени као

извршена са намером или противправно. Додатни протокол дефинише појам „расистичког и ксенофобичног материјала“ (чл. 2), подразумевајући под њим сваки писани материјал, сваку слику или свако друго представљање идеја или теорија које заговарају, промовишу или подстрекавају мржњу, дискриминацију или насиље против било којег појединца или групе појединаца, засновано на раси, боји коже, наследном, националном или етничком пореклу или припадности одређеној вери.

б) Садржај Конвенције и најзначајније одредбе материјалног и процесног права. Конвенција садржи, између осталог, материјалне и процесне кривичноправне одредбе, чијом би имплементацијом у национална законодавства држава потписница требало да се постигне висок степен хармонизације националних законодавстава и да се убрза и квалитативно унапреди међународна сарадња на плану борбе против компјутерског криминалитета. Одредбе Конвенције систематизоване су у четири поглавља: прво поглавље се односи на дефинисање појмова, друго, на мере које је потребно предузети на нивоу појединих држава у оквиру кривичног материјалног и процесног законодавства, треће, на међународну сарадњу у оквиру узајамне помоћи у борби против компјутерског криминалитета и четврто, на завршне одредбе потписавања и ступања на снагу (приступање, територијална примена, изјаве, резерве, решавање спорова, отказ, итд.).

Разлози за доношење Конвенције су многобројни: постојање ризика да се због дигитализације, конвергенције и сталне глобализације рачунарске мреже електронске информације могу користити и за извршење кривичних дела и да докази који се односе на таква дела могу бити сачувани и пренесени преко тих мрежа; потреба међународне сарадње између држава због транснационалног карактера високотехнолошког криминалитета; потреба заштите легитимних

вид изражавања слободе говора. *Претња мотивисана расизмом или ксенофобијом* састоји се у стављању у изглед појединцу или групи (који се издвајају према својој раси, боји коже, пореклу, националној, етничкој или верској припадности) да ће према њима бити извршено неко тешко кривично дело коришћењем рачунара или рачунарских система. *Увреда мотивисана расизмом или ксенофобијом* има исте елементе као претходно дело само није реч о претњи, већ о вређању. *Порицање, значајно умањење, одобравање или оправдање геноцида или злочина против човечности* обухвата намерно или противправно извршену дистрибуцију или на други начин чињење доступним путем рачунара и рачунарских система материјала који поричу, значајно умањују, одобравају или оправдавају дела која представљају геноцид или злочине против човечности, прописане међународним правом и признатим као таквим коначним и обавезујућим одлукама Међународног војног трибунала или другог међународног суда.

интереса у коришћењу и развоју информацине технологије; олакшавање откривања, истраге и гоњења кривичних дела компјутерског криминалитета на националном и међународном нивоу јер је тамна бројка веома велика; као и потреба поштовања и заштите права на приватност, личних података, сопственог мишљења и слободе изражавања.

У Конвенцији (чл.1) су наведене дефиниције: *рачунарског система* (сваки уређај или група међусобно повезаних или зависних уређаја, од којих један или више њих, на основу програма, врше аутоматску обраду података), *рачунарског податка* (свако представљање чињеница, информација или концепата у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију), *даваоца услуга* (сваки јавни или приватни субјект који корисницима своје услуге пружа могућност комуницирања преко рачунарског система; сваки други субјект који обрађује или чува рачунарске податке у име такве комуникационе услуге или корисника такве услуге), *податак о саобраћају* (сваки рачунарски податак који се односи на комуникацију преко рачунарског система, произведену од рачунарског система који је део ланца комуникације, а у којој су садржани подаци о пореклу, одредишту, путањи, времену, датуму, величини, трајању или врсти предметне услуге).

У даљем тексту Конвенције објашњене су мере које треба предузеети на националном нивоу у области материјалног кривичног права и процесног права. У области материјалног кривичног права наведено је низ дела које стране уговорнице треба да предвиде у кривичним законима, при чему су сва дела груписана у четири одељка, а у посебним одељцима наведени су: други облици одговорности и санкције, покушај, помагање или подстрекавање; одговорност правног лица и санкције и мере.

Према одредбама Конвенције (чл. 2 – 10) неопходно је да у националне кривичне законе буду унета дела против поверљивости, целовитости и доступности рачунарских података и система (незаконит приступ, незаконито пресретање, ометање података, ометање система, злоупотреба уређаја), дела у вези са рачунарима (фалсификовање у вези са рачунарима, превара у вези са рачунарима), дела у вези са садржајем (дела у вези са дечијом порнографијом, дела у вези са кршењем ауторких и сродних права).

Незаконит приступ, према тексту Конвенције, обухвата противправно приступање рачунарском систему ако целини или неком његовом делу са намером прибављања рачунарских података или неком другом нечасном намером или је у вези са рачунарским системом повезаним са другим рачунарским системом. *Незаконито пресретање* се односи на противправно пресретање преноса рачунарских података који нису јавне природе, ка рачунарском систему, од њега или унутар самог система, укључујући електромагнетно емитовање из рачунарског система којим се такви подаци преносе учињено са намером и уз помоћ техничких уређаја. Као *ометање података* дефинисано је противправно оштећење, брисање, погоршање, мењање или прикривање рачунарских података, учињено са намером, с тим што у национално законодавству може бити превиђено да је дело имало тешке последице. Озбиљно *ометање рада рачунарског система*, како се наводи у Конвенцији, може бити извршено уношењем, преношењем, оштећењем, брисањем, погоршавањем, мењањем или прикривањем рачунарских података и мора бити учињено са намером. Конвенција препоручује да национална кривична законодавства инкриминишу *злоупотребу уређаја* која се састоји у намерној и противправној производњи, продаји, набављању ради употребе, увозу, дистрибуцији и другим облицима стављања на располагање уређаја, укључујући и рачунарски програм, рачунарску лозинку, приступну шифру или сличног податка помоћу којег може да се приступи рачунарском систему као целини или неком његовом делу, као и поседовање неке од тих ствари ради предузимања наведених радњи извршења.

Фалсификовање у вези са рачунарима се односи на намерно и противправно уношење, мењање, брисање или прикривање рачунарских података, што за последицу има неверодостојност података, учињено са циљем да се ови подаци сматрају веродостојним и да се са њима у правном саобраћају поступа као са веродостојним подацима. У вези са употребом рачунара Конвенција предлаже да се у национална законодавства унесе кривично дело *преваре у вези са рачунарима*, које се састоји у намерном и противправном уношењу, мењању, брисању или прикривању рачунарских података са преваром или нечасном намером да се неовлашћено прибави противправна имовинска корист за себе или другог и нанесе имовинска штета другом лицу.

Код *дела у вези са дечијом порнографијом* у Конвенцији најпре се прописују радње учињене са намером и противправно (производња дечије порнографије у сврху њене дистрибуције преко рачунарског система; нуђење и чињење доступним дечије порнографије преко рачунарског система; дистрибуција или преношење дечије порнографије преко рачунарског система; набављање дечије порнографије преко рачунарског система за себе или за друго лице; поседовање дечије порнографије у рачунарском систему или на медијумима за чување рачунарских података), затим се дефинише израз „дечија порнографија“ (порнографски материјал који визуелно приказује: малолетника који учествује у експлицитно сексуалној радњи, лице које изгледа као малолетник, које учествује у експлицитно сексуалној радњи, као и реалистичне слике које представљају малолетника који учествује у експлицитно сексуалној радњи) и израз „малолетник“ (сва лица млађа од 18 година, с тим што у националном законодавству може да буде предвиђена и нижа старосна граница малолетства, али не нижа од 16 година).

У вези са кршењем ауторских и сродних права Конвенција се позива на обавезе земаља потписница које су преузеле Париским актом од 24. јула 1971. године, којим се ревидира Бернска конвенција за заштиту књижевних и уметничких дела,[670] Споразумом о комерцијалним аспектима права на интелектуалну својину (Agreement on trade-related aspects of intellectual property rights, 1995), WIPO уговором о ауторском праву, [671] Међународном конвенцијом о заштити извођача, произвођача фонограма и установа за радио-дифузију (Римска конвенција)[672] да заштите ауторска права и предвиде у кривичним законима кривична дела повреде ауторских права извршена преко рачунарског система.

Из одредби Конвенције произилази да није довољно да само материјално кривично право прати развој информационо комуникационих технологија и санкционише њихову злоупотребу приликом коришћења, већ је потребно да у оквиру процесног законодавства буду предвиђене нове мере и поступци који ће

[670] Закон о ратификацији Бернске конвенције за заштиту књижевних и уметничких дела (“Сл. лист СФРЈ”, бр. 14/75 и “Сл. лист СФРЈ – Међународни уговори”, бр. 4/86 - уредба)
[671] Закон о потврђивању WIPO уговора о ауторском праву (“Сл. лист СФРЈ – Међународни уговори”, бр. 13/2002)
[672] Закон о потврђивању међународне конвенције о заштити извођача, произвођача фонограма и установа за радио-дифузију (“Сл. лист СФРЈ – Међународни уговори”, бр. 13/2002)

омогућити, поред осталог, успешно прикупљање доказа за кривична дела у електронском облику и примену нових истражних техника за откривање и сузбијање компјутерског криминалитета. У том смислу, Конвенција предвиђа обавезу држава потписница да предузму све неопходне законодавне и друге мере за увођење процесних инструмената, као што су: *хитна заштита сачуваних рачунарских података*, поготово ако има основа да се верује да су подложни губитку или измени (чл.16) и *хитна заштита и делимично откривање података о саобраћају* без обзира да ли је у преношењу поруке учествовао један или више давалаца услуга (чл. 17), *издавање наредбе за предавање компјутерских података* (чл. 18), *претраживање и заплена сачуваних рачунарских података* (чл. 19), *прикупљање података о саобраћају у реалном времену* (чл. 20), *пресретање података о садржини комуникације* (чл. 21).

Од наведених мера посебно је интересантно *издавање наредбе за предавање компјутерских података (члан 18),* што подразумева да надлежни органи држава потписница могу да наређе сваком лицу на територији те државе да мора да преда одређене компјутерске податке које поседује или контролише, а који су сачувани у рачунарском систему или на медијуму за чување рачунарских података, као и да сваком даваоцу услуга који своје услуге врши на територији те државе нареди да преда податке о претплатнику на те услуге које тај даваоц услуга поседује или контролише. Ово је веома флексибилна мера коју би припадници органа откривања компјутерског криминалитета могли да примене када нема услова за примену других мера, као што су наредба о претресу, пресретању комуникација или заплени јер је за ове мере потребно додатно испуњење правних и техничких услова.

С обзиром на то да се рачунарски подаци могу поделити на: податке о саобраћају, податке о садржини комуникације и податке о претплатнику, Конвенција утврђује да израз *„подаци о претплатнику”* означава сваки податак садржан у облику рачунарског податка или у било ком другом облику, који поседује давалац услуга и који се односе на претплатнике тих услуга, осим података о саобраћају или података из садржаја који се преноси. Значи, појам претплатника широко је постављен јер укључује широк круг клијената. На основу ових података може се утврдити: врста коришћене комуникацијске услуге, технички детаљи и временски период коришћења услуге; идентитет

претплатника, поштанска адреса или географско одредиште, број телефона и остали бројеви приступа, подаци о рачунима и плаћањима, доступни на основу уговора или споразума о коришћењу услуге, као и свака друга информација о месту постављања комуникационе опреме доступне на основу уговора или споразума о коришћењу услуге. Све наведене информације о претплатнику могу бити веома значајне приликом вођења истраге, посебно код кривичних дела рачунарске преваре, као и кривичних дела против имовине, платног промета и привреде.

Одредбе Конвенције о *Претраживању и заплени ускладиштених компјутерских података* (члан 19), обавезују државе потписнице да усвоје законодавне и друге мере на основу којих ће се омогућити претраживање и приступ рачунарском систему или његовом делу, као и медијуму за чување рачунарских података на коме рачунарски подаци могу да се сачувају. Посебне мере предвиђене за обезбеђивање рачунарских података обухватају: заплену или други начин обезбеђења рачунарских података; прављење и задржавање копија рачунарских података; одржавање целовитости битних сачуваних рачунарских података; чињење рачунарских података недоступним или уклањање из рачунарског система коме је приступљено. Надлежни органи би, према тексту Конвенције, требало да буду овлашћеи да наређе сваком лицу које познаје начин рада рачунарског система или мере примењене за заштиту рачунарских података на том систему, да пружи податке неопходне за предузимање мера.

Прикупљање рачунарских података о саобраћају о реалном времену (члан 20) предвиђено је Конвенцијом како би надлежни органи држава потписница Конвенције могли да на својој територији примењујући техничка средства пркупљају или снимају *податке о саобраћају* одређених комуникција на њеној територији пренетих преко рачунарског система. Овлашћења надлежних органа треба да се односе и на обавезивање даваоца услуга да чувају у тајности спровођење сваке превиђене мере и информацију у вези са спровођењем мера.

Надлежност државних органа такође треба да обухвати *пресретање података из садржаја електронских комуникација* (чл. 21), што значи да могу да, примењујући техничка средства, *прикупљају или снимају податке из садржаја електронских комуникација* пренетих преко рачунарског система. Ова

област интервенције државних органа је најосетљивија јер се односи на прислушкивање електронских комуникација пре свега оних везаних за интернет, што може бити злуоупотребљено и значајно угрозити право на приватност. Осим генералног ограничења да се при извршењу ове мере морају поштовати међународни стандарди људских права и слобода наведени у међународним документима и да се мера „пресретања" може предузети за „озбиљна дела", Конвенција не садржи ограничења за њену примену и гаранције да неће бити повређено право на приватност нити одређује која су то „озбиљна дела".[673] У сваком случају, државе морају прописати услове под којима ће даваоци услуга (провајдери), који учествују у сакупљању ових информација чувати у тајности спровођење сваког овлашћења и сваку информацију.

У III поглављу Конвенције (чл. 23-35) регулисана је међународна сарадња и помоћ у кривичним стварима које се односе на рачунаре, рачунарски систем, податке који су генерисани од стране рачунара, податке који су употребљени или на други начин искоришћени у току рачунарске комуникације, као и прикупљање доказа у електронској форми у вези извршења кривичних дела компјутерског криминалитета. С обзиром на чињеницу да извршиоци кривичних дела користе најсавременије облике информационо комуникативних технологија, као и на велику осетљивост рачунарских података, могућност њиховог брисања или уништења само са неколико притисака на рачунарску тастатуру, неопходно је веома брзо и хитно пружање међународноправне помоћи како на основу одредби Конвенције тако и на основу билатералних и мултиралних споразума о кривичноправној сарадњи и осталих облика регулисања правне помоћи у овој области. У том смислу Конвенција предвиђа коришћење брзих средстава комуникације, као што су: факс, електронска пошта, коришћење шифри уз накнаду формалну потврду и сл. Из одредби Конвенције произилази да је неопходно праћење развоја информационо комуникационе технологије и њихово искоришћавање ради што брже размене података и комуникација приликом међународне сарадње.

---

[673] У пракси се сматра да је једино оправдана примена ове и сличних мера када се ради о истрагама које могу довести до једног или више извршилаца кривичних дела као што су: преваре, тероризам, злостављање деце, трговина људима и сл.

У оквиру регулисања међународне правне помоћи у кривичним стварима посебну улогу заузима постојање тзв. „24/7 мреже“ (чл. 35) која представља мрежу тачака контакта међу земљама које су ратификовале Конвенцију и које се у највећем броју случајева налазе при министарствима унутрашњих послова и јавним тужилаштвима. Свака држава треба да одреди место за контакт које ће бити доступно 24 сата дневно свих 7 дана у недељи током целе године, ради омогућавања хитног одговора и помоћи у истрагама и процедурама међународне правне помоћи. Тачке контакта морају бити оспособљене да директно и самостално уз сарадњу других надлежних органа земље чланице пруже технички савет, чување и прибављање података, прибављање доказа, давање правних информација, као и идентификацију и локацију на којој се налази осумњичено лице. Један од кључних задатака које контакт тачке ове мреже треба да испуне је могућност успостављања брзог извршења оних функција и задатака који су неопходни ради брзог поступања у кривичноправној материји.

Конвенција садржи посебне одредбе које се односе на: хитну заштиту сачуваних рачунарских података, хитно откривање заштићених података о саобраћају, узајамну помоћ у односу на приступање сачуваним рачунарским подацима, прекогранични приступ сачуваним рачунарским подацима уз сагласност или када су доступни јавности, узајамну помоћ у прикупљању података о саобраћају у реалном времену и узајамну помоћ у пресретању података из садржаја. За хитну заштиту сачуваних рачунарских података потребно је поднети захтев за заштиту података, чију садржину Конвенција предвиђа и тачно одређује разлоге за одбијање захтева.

1.2.2. Конвенција о заштити права појединаца у вези са аутоматском обрадом личних података

Конвенција о заштити права појединаца у вези са аутоматском обрадом личних података (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETC No. 108*)[674] усвојена је са циљем јачања правне регулативе на пољу заштите података о личности и поштовања

[674] Отворена је за потписивање државама чланицама 28. 01. 1981. године, а ступила на снагу 01. 10. 1985. године

приватности с обзиром на све интензивнији прекогранични промет личних података који су предмет аутоматске обраде. Уочено је да национана законодавства држава чланица не пружају потребан ниво заштите грађанима у погледу заштите приватности посебно када се прикупљају лични подаци аутоматском обрадом за потребе државних органа и других правних лица.

Централни део Конвенције садржан је у другом поглављу „Основна начела за заштиту података“ (чл. 4 - 11) који обухвата: (1) квалитет прикупљања и аутоматске обраде личних података (лојалност и законитост, уношење за тачно утврђене и легитимне сврхе, наменско коришћење, брижљивост и чување у облику који омогућава идентификацију); (2) посебне категорије података (аутоматски се могу обрађивати лични подаци у вези са расним пореклом, политичким опредељењем, верским убеђењем или неком другом врстом убеђења, здравственим стањем, сексуалним животом, само уколико закон предвиђа одговарајуће гаранције); (3) безбедност података (обавеза да се примене одговарајуће безбедносне мере које би онемогућиле случајно или неовлашћено уништење прикупљених података, као и губитак, неовлашћени приступ, измену или дистрибуцију аутоматски прикупљених података); (4) додатне мере заштите субјекта података (увид у аутоматски прикупљене податке, добијање потврде о постојању/непостојању личних података у аутоматизованој збирци, тражење исправке или брисања података када су обрађени противно одредбама закона, подношење жалбе у случају када захтевима није удовољено); (5) изузеци и ограничења (права прописана Конвенцијом могу бити ограничена само на основу закона државе, а односе се на заштиту безбедности државе, јавног поретка, монетарног система државе, сузбијање кривичних дела, заштите права и слобода лица чији се подаци прикупљају); (6) санкције и правна средства (односе са на повреду одредаба интерног права и основних начела Конвенције); (7) шира заштита (ниједна одредба Конвенције није ограничавајућа нити онемогућавајућа за страну уговорницу да субјекту података одобри ширу заштиту од оне коју предвиђа Конвенција).

Треће поглавље Конвенције посвећено је прекограничној размени информација. Пракса је показала да постоје одређени проблеми у тзв. „прекограничном протоку информација“ нарочито у појединим областима пословања, као што су пружање банкарских услуга, туризам, употреба

кредитних и платних картица, ефикасан прекогранични проток електронских података. Због тога је суштина одредби о прекограничној размени информација да између држава чланица обезбеде несметан и слободан проток информација, лишен било каквих специјалних контролних механизама или подвргнут посебном режиму дозвола или одобрења. Међутим, постоји могућност да страна уговорница одступи од ових одредби Конвенције уколико у њеном законодавству постоје посебни прописи за неке категорије личних података или аутоматизованих збирки са личнимподацима због карактера тих података или збирки или када се проток врши са њене територије на територију неке државе која није потписница Конвенције.

У четвртом и петом поглављу Конвенције предвиђена је међусобна помоћ (сарадња међу странама уговорницама, помоћ која се пружа субјекту података који живи у иностранству, гаранције у вези помоћи коју пружају одређени надлежни органи, одбијање захтева за добијање помоћи, трошкови и процедура пружања помоћи), састав, функције и процедура Саветодавног комитета за примену одредаба Конвенције.

1.2.3. Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања

Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања (*Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25. 10. 2007.),* тзв. Ланзарот конвенција представља први међународни документ који се односи на све облике сексуалног насиља према деци. Правно регулисање овог питања на међународном нивоу настало је због забрињавајуће великог пораста сексуалне експлоатације и злоупотребе деце коришћењем информационих, рачунарских технологија и друштвених мрежа. Други разлог је неједнако правно регулисање у националним законодавствима до ког узраста се нека особа сматра дететом, због чега се кривична дела извршена према деци нису могла квалификовати као дела сексуалне експлоатације и злоупотребе деце. Због тога се у Конвенцији одређује да се под дететом подразумева свака особа млађа од 18 година.

Конвенција је тематски подељена на више поглавља: превентивне мере, специјализована тела за координацију, мере заштите и подршке жртвама, материјално кривично право, истрага, кривични прогон и процесне одредбе,

обједињена евиденција о осуђеним лицима и међународна сарадња. Основне поставке Конвенције обухватају: превентивну заштиту од насиља („prevention"), заштиту детета жртве („protection"), кривично гоњење учиниоца („prosecution") и учешће деце („participation"). Према тексту Конвенције, сексуалном експлоатацијом и сексуалним искоришћавањем сматрају се следећа кривична дела: *сексуално злостављање* (ступање у сексуалне односе са дететом које није навршило правни узраст у коме су сексуалне активности допуштене, у нашем законодавству 14 година, применом силе и принуде, злоупотребом поверења или ауторитета у односу на дете, коришћењем посебне рањивости, односно физичке и психичке ометености, детета, *кривична дела у вези са дечијом проституцијом* (ангажовање или приморавање детета на проституцију или коришћење услуга дечије проституције), *кривична дела у вези са дечијом порнографијом* (производња, нуђење, дистрибуирање или пренос, као и поседовање дечије порнографије, *учешће детета у порнографским представама или присуствовање порнографским представама са децом*, *приморавање детета да учествује као сведок сексуалног злостављања и наговарање деце на неке од ових услуга применом информационих технологија* („grooming").

За извршење свих наведених кривичних дела могу се користити компјутер и друштвене мреже. Посебно када се ради о дечијој порнографији јер се нуђење и чињење доступним дечије порнографије може извршити постављањем недозвољених *online* садржаја како би се омогућио приступ другим лицима или прављење интернет сајтова са садржајем дечије порнографије. Због тога Конвенција предвиђа обавезу држава потписница да у својим националним законодавствима инкриминишу све противправне радње у вези са дечијом порнографијом јер се дистрибуција недозвољеих порнографских садржаја може најефикасније и најбрже извршити уз употребу компјутера и коришћење друштвених мрежа. Одредбе Конвенције које се односе на умишљајно остваривање приступа садржајима дечије порнографије путем рачунарских технологија има за циљ да државе потписнице инкриминишу свако понашање учесника у ланцу дистрибуције недозвољених порнографских материјала. Неопходно је да је извршилац дела имао сазнање да

се на одређеном сајту налази дечија порнографија и да је желео да приступи сајту како би видео и дистрибуирао наведене материјале.[675]

У оквиру одредби процесноправне природе Конвенција предвиђа да кривично гоњење извршиоца треба да се настави чак и ако је жртве повукла своје изјаве и да рок застарелости кривичног гоњења почне да тече од пунолетства жртве, како би се детету жртви дала могућност да када стекне зрелост и самосталност, без страха од одмазде и уцене пријави учиниоца, што је посебно важно ако је извршилац био у односу ауторитета према жртви. Конвенцијом се такође захтева од држава да у својим законима предвиде заштиту права и интереса детета жртве у свим фазама истражног и кривичног поступка: информисање о њиховим правима и службама које им стоје на располагању као саветодавни сервис и подршка приликом пријављивања кривичних дела; онемогућавање контакта жртве и учиниоца; омогућавање малолетним жртвама да уз употребу информатичких технологија (видео исказ) дају исказ без физичког присуства у судници сл.

1.2.4. Конвенција о спречавању тероризма

Савет Европе је 1977. године усвојио Конвенцију о сузбијању тероризма[676] која је 2005. године допуњена Конвенцијом о спречавању тероризма чији је циљ предузимање делотворних мера за спречавање тероризма и супротстављање јавним провокацијама да се изврше терористичка дела и да се регрутују и обучавају лица за тероризам. Могућности које пружају информационе технологије када се ради о тероризму су многобројне и неисцрпне. Деловање терориста и терористичких организација често је усмерено ка употреби компјутера и друштвених мрежа за организовање терористичких напада, због чега се може говорити о повезаности између компјутерског (високотехнолошког) криминалитета и тероризма. Осим тога, унапред смишљен, политички мотивисан напад терориста и терористичких

---

[675] Николић Комлен, Лидија, Гвозденовић, Радоје, Радуловић, Саша, Милосављевић, Александар, Јерковић, Ранко, Живковић, Владан, Живановић, Саша, Рељановић Марио; Алексић Иван: „Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу“, Сузбијање високотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010, стр. 57

[676] Закон о потврђивању Европске конвенције о сузбијању тероризма (“Службени лист СРЈ – Међународни уговори“ бр. 10/2001 од 09. 11. 2001. године)

организација може да се односи на приступ подацима и информацијама у сајбер простору, рачунарске системе и програме, тако да изазове страх код становништва (инфотероризам или информатички тероризам, cyberterrorism).[677]

Са становишта информатичких технологија посебно су значајне одредбе Конвенције које се односе на дефинисање јавне провокације, регрутовања за тероризам и обуке за тероризам (чл. 5 - 7 Конвенције). *Јавна провокација* да се чине акти тероризма односи се на намерно ширење или достављање на други начин јавности одређене поруке у циљу подстицања на вршење терористичког кривичног дела, без обзира на то да ли је кривично дело извршено (чл. 8). Иако у Конвенцији није посебно наглашен начин на који може бити извршена јавна провокација (ширење или достављање „на неки други начин"), несумњиво је да јавно позивање на вршење тероризма, ширење или достављање писаног материјала, слика, идеја или теорија које заговарају и подстичу на вршење кривичних дела тероризма, може бити извршено злоупотребом рачунарских технологија и коришћењем интернета као глобалне мреже за комуникацију и размену информација. *Регрутовање за тероризам*, према тексту Конвенције, представља подстрекавање другог лица да изврши кривично дело тероризма или да учествује у извршењу таквог дела или да ступи у удружење или групу, како би допринело да то удружење или група изврши једно или више терористичких дела. Поступак регрутације, с обзиром на дефиницију дату у Конвенцији, може се извршити уз помоћ интернета и друштвених мрежа. *Обука за тероризам* је дефинисана у Конвенцији као „давање упутстава за производњу или коришћење експлозива, ватреног оружја или другог оружја или штетних или опасних материја или за друге специфичне методе и технике у циљу извршења или доприношења извршењу кривичног дела тероризма, уз свест о томе да ће

[677] Израз *„cyber terrorism"* користи се за означавање посебне врсте терористичких напада усмерених ка рачунарским системима и мрежама у намери остваривања политичких циљева. Сајбер тероризам представља једну од главних глобалних препрека савремене безбедности. Целокупни витални инфраструктурни систем државе (снабдевање електричном енергијом, водом, телекомуникације, саобраћај, информациони системи и др.) свакодневно су под претњом сајбер тероризма. Према једној подели информатичког тероризма, тероризам у ери информатике се састоји од: конвенционалног тероризма у коме се класична оружја (експлозиви, пушке и сл.) користе за уништавање средстава и људства у физичком смислу; технотероризам, када се класична убојна средства користе за уништавање инфраструктуре и проузроковање штете у сајбер простору и сајбер тероризам где се нова оружја (злонамеран софтвер, електромагнетна и микроталасна оружја) користе за уништавање и измену података у сајбер простору. *Цит. према* Заштита информационих система, www.fms-tivat me/PREDAVANJA 3 god/ZIS8.pdf претражено 25. 08. 2015. године

вештине којима се лице подучава бити коришћене у ту сврху“. Све наведене радње извршења такође могу бити извршене уз помоћ рачунарске технологије и интернета (електронска пошта, дискусиони форуми, причаонице и сл).

1.2.5. Препорука Савета министара Савета Европе државама чланицама која се односи на заштиту људских права на друштвеним мрежама

Препорука Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама[678] усвојена 4. априла 2012. године под окриљем Савета Европе, друштвене мреже препознаје као „средство за реализацију људских права и катализатор за демократију”.[679] Како друштвене мреже представљају средство за изражавање и комуникацију између појединаца али и директну групну комуникацију милиона људи, оне су својеврстан потенцијал за унапређење и остваривање људских права и основних људских слобода, а посебно за изражавање слободе говора, размене идеја и садржаја и слободу окупљања.

Друштвене мреже су у овом документу сагледане и кроз могућност повећања учешћа појединаца у политичком, друштвеном и културном животу, али самим тим и као потенцијално место где може да дође до непоштовања и кршења људских права која се на њима остварују. Највише су угрожена права на слободно изражавање мишљења као и право на приватност и људско достојанство, због могућности испољавања различитих дискриминаторских понашања. До оваквих проблема може да дође због непостојања одговарајућих правних и процедуралних одредби којима би се овакви појединци искључили из виртуелних заједница и санкционисало криминално понашање појединаца у виртуелном простору, посебно када је реч о делима која злоупотребљавају неадекватну заштиту деце и младих од штетних садржаја, показују отворено непоштовање туђих личних права, крше право на приватност користећи

[678] Препорука Савета Министара Савета Европе CM/Rec(2012)4 државама чланицама која се односи на заштиту људских права на друштвеним мрежама (Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services), 2012, https://wcd.coe.int/ViewDoc.jsp?id=1929453, претражено 09. 07. 2014. године

[679] Тачка 1 Препоруке Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама

немогућности подешавања нивоа заштите објављених личних података на одређеној друштвеној мрежи.

Препорука је указала и на обавезу држава да свако сакупљање података о личности мора да буде транспарентно, да се тачно нагласи сврха сакупљања и складиштења података, начин и сврха обраде ових података као и крајњи корисник сакупљене збирке података.[680] Прописана је и обавеза интернет провајдера односно платформи на којима се врши друштвено умрежавање да су у обавези да поштују људска права и владавину права (тач. 5)

Савет Министара је позвао државе да своја законодавства у области злоупотреба у области виртуелног простора ускладе са чланом 8 Европске Конвенције о људским правима,[681] који се односи на поштовање права на приватност и породични живот, чл. 10 који се односи на слободу говора и чл. 11 који се односи на слободу удруживања и окупљања, као и са Конвенцијом Савета Европе о заштити појединаца од аутоматске обраде личних података CETS бр. 108[682] која упућује провајдере друштвених мрежа како да спрече злоупотребу личних података својих корисника.

Препоруком је, такође, апеловано на кориснике друштвених мрежа да обрате пажњу на почетна подешавања својих корисничких профила, на то шта објављују, да увек морају да дају сагласност када се постави питање складиштења, чувања и обраде њихових личних података, као и да имају право да своје податке трајно повуку са виртуелног простора друштвених мрежа.

Посебна пажња је посвећена заштити деце и младих људи од неприкладних садржаја на друштвеним мрежама.[683] Сама чињеница да је на друштвеним мрежама заступљена слобода говора указује на чињеницу да се ту објављују и садржаји који могу да буду непримерени, узнемирујући или увредљиви, а како друштвене мреже играју веома важну улогу у свакодневном

---

[680] Тачка 3 Препоруке Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама

[681] Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), колоквијално називана Европском конвенцијом о људским правима, European Convention on Human Rights, http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm, претражено 12. 05. 2014. године

[682] Council of Europe Convention on Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108

[683] Тачке 5 - 11 Препоруке Савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама

животу деце и младих људи данашњице јавља се потреба да се они због својих година заштите од оваквих садржаја. Препоруком се најпре апелује на родитеље и наставнике да упућују децу како да друштвене мреже користе на прави начин, да не би доживљавали различите непријатности и упадали у опасности. На појединим мрежама постоје ограничења одређених садржаја у односу на године корисника, а апелује се да се сваки неприкладан садржај означи на одређен начин (попут „само за одрасле" или „узнемирујућег садржаја"). На државе се апелује да морају да предузму одговарајуће мере како би побољшале сигурност деце и младих на друштвеним мрежама, а да уједно не прекрше право слободе изражавања, па им се саветује да: (1) пружају јасне информације о врстама садржаја које објављују и да воде рачуна о томе да ли је он законит или није; (2) развију такву уређивачку политику којим би се одређени садржаји означили као „неприкладни" и неусклађени са условима коришћења сервиса за друштвену мрежу при томе водећи рачуна да се на овај начин не ограничава право на слободу изражавања и информисања; (3) установе лако доступне и разумљиве механизме за пријављивање сваког уоченог садржаја на друштвеној мрежи који може да се окарактерише као неприкладан или наизглед противзаконит; (4) објављују и међусобно размењују примере добре праксе којима би се спречили случајеви насиља на интернету, посебно у контексту вршњачког насиља и сексуалне експлоатације деце на друштвеним мрежама.

Препорука поред свих наведених предложених мера у циљу заштите права на приватност објављених информација, у тачкама 12 - 15 посвећује додатну пажњу личним подацима који се објављују на друштвеним мрежама. Сви објављени лични подаци могу да буду доступни другим корисницима мреже, али такође и трећим лицима, попут различитих фирми, послодаваца, рекламним агенцијама, представницима власти. На друштвене мреже се апелује да се прикупљени лични подаци не прослеђују никоме без изричите сагласности власника личних података а на државе се апелује да предузму мере којима би се заштитила права корисника на приватност тако што би обавезале сервисе за друштвене мреже да: (1) корисницима обезбеде најбоље могуће начине заштите приватности (одговарајућа подешавања, сигурносне мере, добијање сагласности пре објављивања или прослеђивања личних података, услове коришћења ових података и сл.); (2) обезбеде одговарајуће техничке услове за безбедност друштвене мреже; (3) обезбеди да осетљиви подаци имају посебну заштиту; (4)

обезбеди примену најсигурнијих мера којима би се спречила могућност да трећа лица противправно дођу у посед поверљивих и личних података корисника друштвене мреже; (5) заштите права трећих лица која су повезана са корисницима друштвене мреже, јер и друштвене мреже и њихови корисници морају да буду свесни обавеза које имају према лицима који нису корисници друштвене мреже и да не треба да објављивањем личних података који се односе на друге људе наруше њихово право на приватност; (6) обезбеде да се обрада личних података корисника врши само у складу са законом и по законом прописаној процедури и (7) упознају корисници са законима који их штите и који се примењују на правила поступања на друштвеним мрежама и коме треба да се обрате уколико мисле да им је неко право повређено.

1.3. Допринос Европске уније борби против компјутерског криминалитета

Европска унија[684] је такође дала свој допринос борби против компјутерског криминалитета и на пољу заштите информационе безбедности.[685] Комисија европских заједница (Commission of the European Communities) је априла 2002. године представила Оквирну одлуку о нападима на информационе системе.[686] Савет Европске уније је усвојио предлог ове одлуке 2003. године и Одлука је ступила на снагу 2005. године. Одлука регулише илегални приступ информационим системима, илегално ометање рачунарских система као и илегално ометање преноса података, али такође прописује и санкције за извршиоце кривичних дела компјутерског криминалитета.[687]

---

[684] Званична интернет презентација Европске Уније, www.europa.eu

[685] European Commision – Digital Agenda for Europe, http://ec.europa.eu/digital-agenda/, претражено 15. 11. 2012. године

[686] Оквирна одлука о нападима на информационе системе Комисије европских заједница (Framework Decision on attacks against information systems of the Commission of the European Communities), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN, претражено 12. 11. 2014. године

[687] Чл. 6 Одлуке предвиђа да је за неовлашћен упад у компјутерски систем и неовлашћено пресретање података прописана казна затвора у трајању од једне до три године, док је чл. 7 Одлуке предвиђено да, ценећи све отежавајуће околности извршеног дела, максимална казна затвора која може да буде пресуђена износи између две и пет година.

ЕУ је 2004. године формирала Европску агенцију за безбедност мрежа и информационих система (ENISA), [688] а затим почетком 2007. усвојила Стратегију за безбедно информационо друштво у Европи,[689] чији је циљ био да се препозна дијалог, партнерски однос и оспособљавање кључних актера, побољшају безбедности мрежа и информација, ојача ENISA и подрже напори држава чланица за постизање синергије.[690]

Од правних инструмената насталих у оквирима Европске уније треба поменути три директиве: Директива о правној заштити компјутерских програма; Директива о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронекс комуникације или јавних комуникационих мрежа и Директива 2013/40/EU.

Директива о правној заштити компјутерских програма (91/250/EEZ)[691] предвиђа обавезу држава чланица ЕУ да правно санкционишу низ понашања у вези са злоупотребом компјутера и компјутерских програма: стављање у промет копије компјутерског програма, са знањем да је копија недозвољена или постоји основана сумња у њену недозвољеност; стављање у промет или држање у комерцијалне сврхе сваког средства чија је једина сврха да олакша недозвољено уклањање или неутрализацију сваког техничког механизма направљеног за заштиту компјутерског програма. Када се ради о заштити ауторских права, занимљиво је да Директива предвиђа обавезу држава чланица да својим законима предвиде заштиту компјутерских програма као књижевних дела, узимајући у обзир Бернску конвенцију за заштиту књижњвних и уметничких дела.

Директива 2006/24/ЕУ Европског парламента и савета о чувању података који су добијени или обрађени приликом пружања јавно доступних

---

[688] Видети European Union Agency for Network and Information Security, http://www.enisa.europa.eu/

[689] Стратегија за безбедно информационо друштво у Европи –Strategy for a Secure Information Society in Europe “Dialogue, partnership, and empowerment”, http://ec.europa.eu/information_society/doc/com2006251.pdf , претражено 21.11.2014.године

[690] Резолуција Европског Савета бр. 2007/C 68/ –European Council Resolution 2007/C 68/01, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007G0324(01)&from=EN, претражено 21.11.2014.године

[691] Директива Савета Европске заједнице о правној заштити компјутерских програма (Council Directive of 14.may 1991. On the legal proctection of computer Programs) са обавезном применом у државама чланицама ЕУ почев од 1.1.1993. године, објављена је у „Службеном листу Европске заједнице бр. Л 122/42“ од 17.5.1991.године.

услуга електронске комуникације или јавних комуникационих мрежа[692] донета је 15. 03. 2006. године са основним циљем да се ускладе одредбе држава чланица које се тичу обавезе даваоца јавно доступних услуга електронске комуникације и јавних комуникационих мрежа да чувају одређене податке које добијају или обрађују како би се осигурало да ти подаци буду доступни у сврху откривања, истраге и гоњења извршилаца тешких кривичних дела. У Директиви су категорисани, таксативно наведени, разврстани у категорије и подкатегорије подаци који се чувају а који су потребни за: проналажење и идентификацију извора комуникације; откривање одредишта комуникације; утврђивање датума, времена и трајања комуникације; откривање врсте комуникације; идентификацију комуникацијске опреме корисника или опреме; откривање локације опреме за мобилне комуникације. Све наведене категорије података, према одредбама Директиве, државе чланице треба да чувају у раздобљу које није краће од шест месеци ни дуже од две године од датума комуникације.

Директива 2013/40/EU, коју је донео је Европски парламент 20. августа 2013. године *(EU Directive 2013/40/EU on attacks against informations systems)*,[693] обухвата област напада на информационе системе. У циљу приближавања кривичним законодавствима земаља чланица Европске уније, у Директиви се наводе минимална правила која се односе на дефиницију кривичних дела, кривичноправне санкције, унапређење сарадње између надлежних органа, укључујући припаднике полиције и других специјализованих агенција за спровођење закона чланица ЕУ, надлежних специјализованих агенција и тела ЕУ, као што су EUROJUST, EUROPO, Европски центар за сајбер криминалитет и Европска агенција за безбедност мрежа и информационих система ENISA. Директива, између осталог, уводи кривичне санкције за кривично дело у виду прављења и коришћења тзв. „ботнетова“[694] и указује да

---

[692] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive 2002/58/EC,
http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024, претражено 17. 08. 2015. године

[693] Directive 2013/40/EU of the European Parliament and of the Council 12. 08. 2013, Offical Journal of the European Union 218/8,
http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040, претражено 19. 08. 2015. године

[694] Да би се успоставила удаљена контрола над значајним бројем рачунара они се инфицирају кроз инсталацију малициозног софтвера и прецизно усмерене сајбер нападе. Једном када се

велики напади могу изазвати значајну економску штету, која се огледа у прекидању рада информационих система и комуникација, као и губитак или измену комерцијално битних поверљивих информација и података.

Европски савет ЕУ (European Council) је 2001. године утврдио јединствену политику приступа свих држава посебним акцијама у домену мрежне и информационе безбедности [695] - политику која је као један од шест приоритета ушла и у акциони план развоја информационих технологија у Европи, да би адекватно одговорила растућим изазовима, после доношења Директиве 2002/22/ЕС о правима корисника која се односе на електронске друштвене мреже и услуге.

Европска комисија је 2009. усвојила акциони план за заштиту критичне информационе инфраструктуре - „Заштита Европе од бројних кибернетичких напада и ометања: побољшати спремност, безбедност и отпорност“,[696] постављајући безбедност и отпорност критичне информатичке инфраструктуре као дугорочни циљ у оквиру европске политике развоја безбедности мрежа и информација.

таква мрежа креира она конституише “ботнет“ који може бити активиран без знања и пристанка корисника рачунара ради отпочињања напада у широком обиму и захвату да може изазвати знатну штету. *Цит према* Група аутора: „Високотехнолошки криминал“, Практични водич кроз савремено кривично право и примери из праксе, OSCE, Подгорица, март 2014, www.osce.org/me/montenegro/117630?download=true, претражено 15. 08. 2015. године

[695] Резолуција Европског Савета бр. 2002/C43/02 о заједничком приступу и посебним акцијама у домену мрежне и информационе безбедности –European Council Resolution on a common approach and specific actions in the area of network and information security (2002/C43/02), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022&from=EN, претражено 21. 11. 2014. године

[696] Акциони план за заштиту критичне информационе инфраструктуре „Заштита Европе од бројних кибернетичких напада и ометања: побољшати спремност, безбедност и отпорност“ – Communication on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, secuirty and resilience”, 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, претражено 21. 11. 2014. године

2. Компаративни преглед правног регулисања компјутерског криминалитета у земљама бивше СФРЈ

Све земље бивше СФРЈ потписале су и ратификовале Конвенцију бр. 185 из 2001. године са додатним Протоколом. На основу ових међународних докумената донети су одговарајући национални прописи у појединим државама. Међу потписницама нема Републике Српске, Дистрикта Брчко и Косова, што је разумљиво с обзиром на њихов специфичан државно – правни статус. Ипак, компаративним прегледом ће бити обухваћени и правни прописи везани за компјутерских криминалитет који важе на наведеним територијама.

2.1. Република Словенија

Република Словенија је Конвенцију бр. 185 потписала јула 2002. године, ратификовала је септембра 2004. године, а обавеза примене је настала од јануара 2005. године.

Казненски законик Републике Словеније[697] нема посебно издвојена кривична дела компјутерског криминалитета. Ова кривична дела су садржана неколико других глава, поред осталих кривичних дела. У Глави XXIII – **Кривична дела против имовине** (сло. Kazniva dejanja zoper premožje) предвиђено је кривично дело *напад на информациони систем* (чл. 221. – сло. napad na informacijski sistem). У Глави XVI – **Кривична дела против људских права и слобода** (сло. Kazniva dejanja zoper človekove pravice in svoboščine) кривична дела која могу припадатаи компјутерском криминалитету одређена су као: *повреда тајности писама* (чл.139 – сло. Kršitev tajnosti občil) и *злоупотреба личних података* (чл.143 – сло. Zloraba osebnih podatkov). Код кривичног дела „повреда тајности писама“ предвиђено је да се кривичним делом сматра и употреба техничких и хемијских средстава како би се отворило туђе писмо или телеграф и како би се сазнала њихова садржина, односно употреба техничких средстава како би се пресрела порука која се шаље путем телефона или другим средством електронске комуникације. Из описа радње кривичног дела

[697] Казненски законик Републике Словеније („Уредни лист РС“, шт. 50/2012), доступно на http://projuris.org/Zakoni_Slovenije/Krivicni_zakonik_Slovenije-precisceni_tekst_2012.pdf, претражено 21. 11. 2014. године

злоупотреба личних података види се да ово кривично дело у потпуности припада компјутерском криминалитету јер се врши преко интернета. Кривично дело чини свако ко улази или неовлашћено приступа компјутерској бази података о личности са циљем да себи или неком другом прибави одређене личне податке; ко путем интернета учини јавно доступним туђе личне податке а посебно о жртвама кривичних дела, жртвама кршења права и слобода заштићених сведока, лица који се налазе у судским списима судских поступака, као и заштићених личних досијеа о њима у вези са судским поступцима; ко преузме идентитет неке друге особе или неовлашћено обради њихове личне податке како би стекао имовинску корист или угрозио достојанство те особе.

У оквиру Главе XIX - **Кривична дела против сексуалног интегритета** (сло. Kazniva dejanja zoper spolno nedotakljivost) предвиђена су два кривична дела која се могу извршити уз помоћ информационо-комуникацијских техника: *врбовање особа млађих од 15 година за сексуалне намене* (чл. 173а – сло. pridobivanje oseb, mlajših od petnajst let, za spolne namene) и *презентација, производња, држање и стављање у порнографског материјала* (чл. 176 – сло. prikazovanje, izdelava, posest in posredovanje pornografskega gradiva).

Казненски законик прописује и кривична дела која се односе на заштиту ауторских и сродних права: ***повреда моралних права*** (чл. 147 – сло. kršitev moralnih avtorskih pravic), ***кршење новчаних права аутора*** (чл. 148 –сло. kršitev materialnih avtorskih pravic) и ***кршење ауторских и сродних права*** (чл. 149 – сло.kršitev avtorski sorodnih pravic).

2.2. Република Хрватска

Република Хрватска је Конвенцију бр. 185 потписала новембра 2001. године, ратификовала октобра 2002. године, а обавеза примене је настала од јула 2004. године. Одредбе Конвенције делимично су имплементиране у Казненом закону Републике Хрватске. **Казнени закон Републике Хрватске**[698]

[698] Казнени закон Републике Хрватске (пречишћен текст „Народне новине“, бр. 125/11, 144/12 и 56/15,61/15), доступно на http://www.zakon.hr/z/98/Kazneni-zakon , претражено 23. 07. 2015. године

у оквиру објашњења значења израза у закону (Глава VIII) дефинише појам рачунарског система, рачунарског податка и рачунарског програма.[699]

У посебној ***Глави XVI „Kазнена дјела против рачуналних сустава, програма и података“*** Казнени закон предвиђа низ кривичних дела која припадају компјутерском криминалитету, али садржи и у другим главама кривична дела која се по својим обележјима такође могу сматрати компјутерским криминалитетом. Најпре треба поменути чл. 142 *„повреда тајности писама и других пошиљки“* (***Глава XIV – Кривична дјела против приватности***) у коме је предвиђено да се неовлашћено отварање, повреда тајности, неовлашћено задржавање, прикривање, саопштавање, уништење или предаја другоме, може да изврши у у односу на електронску пошту. Тежи облик овог кривичног дела постоји уколико постоји намера код извршиоца да себи или другоме прибави имовинску корист или да другоме проузрокује штету или је извршилац службено лице у обављању службе или јавних овлашћења. Један број кривичних дела из ***Главе XVII (Казнена дјела сполног злостављања и искоришћавања дјетета)*** такође припада компјутерском криминалитету јер може бити извршен путем информацијко комуникацијских технологија. Таква кривична дела су *„искоришћавање дјеце за порнографију“* (чл. 163.); *„искоришћавање дјеце за пороногрфске представе“* (чл. 164), *„упознавање дјеце с порнографијом“* (чл. 165).[700] У ***Глави XXIV „Kазнена дјела против господарства“*** у опису кривичног дела *„злоупораба тржишта капитала“* (чл. 260) наводи се ширење информација путем медија, ***интернета*** или другим начином или средством који даје или би могао давати лажне или обмањујуће поруке у погледу финансијких инструмената, укључујући ширење гласина и

---

[699] *Рачунарски систем* се одређује као свака направа или скупина међусобно спојених повезаних направа, од којих једна или више њих на основу програма аутоматски обрађује податке, као и рачунарски подаци који су у њега унети, обрађени, учитани или пренесени за сврхе његовог рада, коришћења, заштите и одржавања (чл. 87 тач. 18). *Рачунарски податак* се дефинише у Казненом закону као свако исказивање чињеница, информација или замисли у облику прикладном за обраду у рачунарском систему (чл. 87 тач. 19). *Рачунарски програм* је скуп рачунарских података који су у стању да проузрокују да рачунарски систем изврши одређену функцију (чл. 87 тач. 20).

[700] У току 2011. године, у Републици Хрватској је 50 кривичних дела санкционисано као кривично дело дечије порнографије, 36 кривичних дела као кривично дело искоришћавање дјеце за порнографију и 16 кривичних дела као кривично дело упознаванја дјеце са порнографијом. *Видети:* Министарство унутрашњих послова Републике Хрватске, http://www.mup.hr/UserDocsImages/topvijesti/2012/lipanj/Zastitimo%20djecu%20na%20internetu.pdf, претражено 28. 09. 2015. године

лажних или обмањујућих вести, при ћему је особа која је проширила информацију знала или била дужна знати да је информација лажна или обмањујућа. У оквиру ***Главе XXX „Казнена дјела против јавног реда“*** предвиђено је кривично дело *„јавно потицање на насиље и мржњу“* које има неколико облика. Један облик овог кривичног дела постоји када неко путем „тиска, радија, телевизије, рачуналног сустава или мреже, на јавном скупу или на други начин јавно потиче или јавности учини доступним летке, слике или друге материјале којима позива на насиље или мржњу према скупини људи или припаднику скупине због њихове расне, вјерске, националне или етничке припадности, подрјетла, боје коже, спола, сполог опредељења, родног идентитета, инвалидитета или каквих других особина“. Кажњавање је предвиђено и за организатора, вођу групе и оног ко суделује у извршењу наведеног кривичног дела, као и за покушај извршења. Посебан облик овог кривичног дела постоји у случају јавног одобравања, порицања или знатног умањивања кривичног дела геноцида, злочина агресије, злочина против човечности или ратног злочина, усмерено према групи људи или припаднику групе због њихове расне, верске, националне или етничке припадности, порекла или боје коже, на начин који је прикладан да подстакне несиље или мржњу против такве групе или припадника те групе.

Кривична дела компјутерског криминалитета садржана су у ***Глави XXV – „Казнена дјела против рачуналних сустава, програма и података“*** обухватају: *неовлаштени приступ* (чл. 266), *ометање рада рачуналног сустава* (чл. 267), *оштећење рачуналних података* (чл. 268), *неовлаштено пресретање рачуналних података* (чл. 269), *рачунално кривотворење* (чл. 270), *рачунална пријевара* (чл. 271), *злоупораба направа* (чл. 272) и *тешка казнена дјела против рачуналних сустава, програма и података* (чл. 273). Иако у чл. 266 (неовлашћен приступ) није јасно дефинисан појам „неовлашћеног приступа“, несумњиво је да се ради о приступу кога није одобрио власник или друга овлашћена особа или приступ који је забрањен законом. У ову одредбу није имплементирана одредба Конвенције бр. 185 којом се санкционише неовлашћен приступ делу рачунарског система. Тежи облик постоји уколико је кривично дело извршено у односу на рачунарски систем или рачунарске податке тела државне власти, тела јединица локалне или регионалне самоуправе, јавне установе или трговачког друштва од посебног јавног интереса.

Одредбом чл. 267 (ометање рада рачунарског система) инкриминише се онемогућавање или отежавање рада или коришћења рачунарског система, рачунарских података или програма или отежавање рада или коришћења рачунарске комуникације. Код кривичног дела „оштећење рачунарских података“ (чл. 268) штити се интегритет и целовитост рачунарских података и програма. Радња извршења овог кривичног дела експлицитно је одређена као оштећење, измена, брисање, уништење, чињење неупотребљивим или недоступним или приказивање недоступним туђих рачунарских података или програма. Код кривичног дела „неовлаштено пресретање рачуналних података“ (чл. 269) санкционисано је пресретање или снимање нејавног преноса рачунарских података, укључујући и електромагнетску емисију рачунарског система или чињење другоме доступним тако прибављених података. Кривично дело „рачунално кривотворење“, према одредби чл. 270 КЗ РХ, постоји када неко лице изради, унесе, измени, избрише или учини неупотребљивим или недоступним рачунарске податке који имају вредност за правне односе, у намери да се они употребе као веродостојни или када неко такве податке употреби или набави ради употребе. Код овог кривичног дела кажњава се и за покушај, као код кривичног дела неовлашћено пресретање рачунарских података. Кривично дело „Рачунална пријевара“ (чл. 271), према опису радње извршења, постоји када нека особа са циљем да себи или другоме прибави протвправну имовинску корист, измени, избрише, оштети, учини неупотребљивим или недоступним рачунарске податке или омета рад рачунарског ситема и на тај начин проузрокује другоме штету. Тежи облик постоји када је прибављена знатна имовинска корист или проузрокована знатна штета. Код кривичног дела „злоупораба направа“ радња извршења је одређена као израда, набавка, продаја, поседовање или чињење другима доступним уређаје, рачунарске, програме, рачунарске податке, рачунарске лозинке, приступне шифре или друге податке уз чију се помоћ може приступити рачунарском систему са циљем да се употребе за вршење свих кривичних дела из Главе XXV.

Посебан члан Казненог закона предвиђа тешка кривична дела против рачунарских система, програма и података (чл. 273). Ова кривична дела се извршавају у односу на речунарски систем или рачунарске податке тела државне власти, тела јединице локалне или подручне (регионалне) самопуправе,

јавне установе или трговачка друштва од посебног јавног интереса. Строжије кажњавање је предвиђено уколико се кривична дела изврше средством намењеним за извршење напада на већи број рачунарских система или уколико се проузрокује знатна штета.

2.3. Федерација Босне и Херцеговине, Брчко Дистрикт и Република Српска

Босна и Херцеговина је Конвенцију бр. 185 потписала фебруара 2005. године, ратификовала маја 2006. године, а обавеза примене је настала од септембра 2009. године. Одредбе о компјутерском криминалитету садржане су у ентитетском законодавству: Кривичном закону Федерације Босне и Херцеговине и Кривичном закону Републике Српске. У Кривичним законима Федерације Босне и Херцеговине и Брчко Дистрикта на исти начин су нормирана и санкционисана кривична дела која припадају компјутерском криминалитету.

Кривични закон Босне и Херцеговине[701] не садржи посебне одредбе о компјутерском криминалитету јер су те одредбе садржане у ентитетском кривичном законодавству. Ипак, треба напоменути да се у оквиру Главе петнаесте „Кривична дјела против слободе и права човјека и грађанина“ нормира и санкционише неовлашћено прислушкивање или оптичко снимање (чл. 147а). Наведено кривично дело постоји када службено или одговорно лице у институцијама Босне и Херцеговине помоћу посебних направа без одобрења, прислушкује или звучно сними разговор или изјаву која му није намењена или омогући непозваном лицу да се упозна са разговором или изјавом која је неовлашћено прислушкивана или звучно снимљена или које неовлашћено прислушкује или сними туђе поруке у **комјутерском систему**. Осим тога, треба напоменути да је код кривичних дела која се односе на повреду ауторских права из Главе двадесет и прве, радња извршења тако широко постављена да може да обухвати и извршење ових кривичних дела употребом рачунарског система, иако то није изричито наведено.[702]

---

[701] Кривични закон Босне и Херцеговине („Службени гласник Босне и Херцеговине“ бр. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07,8/10, 47/14, 22/15, 40/15)

[702] Поробић, Миралем, Барјактаревић, Мирсад: „Cyber crime, pranje novca i finansijske istrage“,

Кривични закон Федерације Босне и Херцеговине[703] у Глави XXXII под називом ***„Кривична дјела против сустава електронске обраде података“*** (чл. 393 - 398) прописује следећа кривична дела из области компјутерског криминалитета: *оштећење рачуналних података и програма* (чл. 393), *рачунално кривотворење* (чл. 394), *рачунална пријевара* (чл. 395), *ометање рада и мреже електронске обраде података* (чл. 396), *неовлашћени приступ заштићеном систему и мрежи електронске обраде података* (чл. 397) и *рачунална саботажа* (чл. 398). Остала кривична дела која припадају компјутерском криминалитету садржана су у Глави XVII **„Кривична дјела против слободе и права човјека и грађанина“** (чл. 186 – *повреда тајности писма или друге пошиљке*, где је у ст. 2 предвиђено кажњавање уколико неко неовлашћено продре у компјутерску базу личних података или те податке неовлашћено користи или их учини доступним другој особи; тежи облици овог кривичног дела постоје уколико је дело учињено са циљем да се себи или другоме прибави корист или нанесе штета или је кривично дело извршило службено лице у обављању службе; чл. 188 – *неовлашћено прислушкивање или снимање туђих порука у рачунарском систему;* чл. 189 – *неовлашћено оптичко снимање*, које има тежи облик ако је жртва дете или малолетник) и Глави XIX **„Кривична дјела против сполне слободе и морала“** (чл. 211 – *искоришћавање дјетета или малољетника ради порнографије* и чл. 212 - *упознавање дјетета с порнографијом*).

Као што смо већ напоменули, у **Кривичном Закону Брчко дистрикта**[704] предвиђена су иста кривична дела из области компјутерског криминалитета као у Кривичном закону Федерације Босне и Херцеговине. Разлике не постоје ни у погледу санкционисања ових кривичних дела.

Кривични закон Републике Српске[705] у посебној Глави XXIV-а под називом **„Кривична дјела против безбједности рачунарских података“**

---

http://pravosudje.ba/vstv/faces/pdfservlet;jsessionid=d740751503b9f050afe655ea08e6d17ddc0412e00b660550df17d03959a09f65.e34TbxyRbNiRb40Qb34MahuLaNv0?p_id_doc=20568,претражено 24. 07. 2015. године

[703] Кривични закон Федерације Босне и Херцеговине (“Службене новине Ф БиХ бр. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14)

[704] Кривични закон Брчко Дистрикта Босне и Херцеговине (“Службени гласник БД БиХ бр. 10/03, 6/05, 21/10, 47/11, 52/11 и 9/13)

[705] Кривични закон Републике Српске (“Службени гласник РС бр. 49/03, 108/04, 37/06, 70/06, 73/10, 01/12 и 67/13)

предвиђа седам кривичних дела која се директно односе на компјутерски криминалитет: *оштећење рачунарских података и програма* (чл.292а), *рачунарска саботажа* (чл. 292б), *израда и уношење рачунарских вируса* (чл. 292в), *рачунарска превара* (чл. 292г), *неовлашћени приступ заштићеном рачунару, рачунарској мрежи, телекомуникационој мрежи и електронској обради података* (чл. 292д), *спречавање и ограничавање приступа јавној рачунарској мрежи* (чл. 292ђ) и *неовлашћено коришћење рачунара или рачунарске мреже* (чл. 292е). Остала кривична дела у вези са компјутерским криминалитетом предвиђена су у Глави XVII **„Кривична дјела против слобода и права грађана“** (чл. 176 - *неовлашћено коришћење личних података*, обухвата неовлашћено улажење у туђу заштићену компјутерску базу података са намером да се њиховим коришћењем за себе или другог прибави каква корист или да се другоме нанесе штета, тежи облик овог кривичног дела постоји када криивчно дело изврши службено лице злоупотребом положаја или овлашћења) и у Глави XIX **„Кривична дјела против полног интегритета** (чл. 199 – *искоришћавање деце и малољетних лица за порнографију*; чл. 200 – *производња, поседовање и приказивање дечје порнографије*, које има тежи облик ако је кривично дело извршено преко средстава јавног информисања или путем интернета). За разлику од других наведених закона, Кривични закон Републике Српске предвиђа кривично дело „производња, посједовање и приказивање дјечије пороногрфије“, као и строжије кажњавање за кривично дело „искоришћавање дјеце и малољетних лица за порнографију“.

2.4. Република Црна Гора

Република Црна Гора је Конвенцију бр. 185 потписала априла 2005. године у оквиру Државне заједнице Србије и Црне Горе, ратификовала је марта 2010. године, а обавеза примене је настала од јула 2010. године.

Кривични законик Црне Горе[706] у Глави XXVIII под називом **Кривична дела против безбедности рачунарских података** санкционише низ кривичних дела, која припадају компјутерском криминалитету. То су углавном

[706] Кривични законик Црне Горе („Службени лист РЦГ“, бр. 70/2003, 13/2004, 47/2006 и „Службени лист ЦГ“ бр. 40/2008, 25/2010, 32/2011, 40/2013 и 56/2013.)

иста кривична дела која се појављују и у другим кривичним законима бивших држава СФРЈ. Као и други кривични закони, Кривични законик Црне Горе издваја у посебну главу кривична дела која припадају искључиво компјутерском криминалитету, али такође у другим главама законика санкционисана су понашања везана за злоупотребу компјутера. Као и Казнени закон Републике Хрватске, Кривични законик Црне Горе дефинише неколико основних појмова која се односе на компјутерски криминалитет. У чл. 142 (Глава тринаеста „Значење израза") објашњава се значење „рачунарског система" (тач. 19), „рачунарског податка" (тач. 20.), „рачунарског програма" (тач. 21), „рачунарског вируса" (тач. 22) и „податка у рачунарском саобраћају" (тач. 23).[707]

У оквиру Главе петнаесте „Кривична дјела против слобода и права човјека и грађанина" инкриминисано је кривично дело „*повреда тајности писама и других пошиљки"* (чл. 172), у оквиру кога је наведена и повреда тајности електронске поште. Код кривичног дела „*дјечја порнографија*" (чл. 211 Глава осамнаеста „Кривична дјела против полне слободе") у опису радње извршења наведена је продаја, поклањање, приказивање, јавно излагање, чињење доступним слика, текстова, аудиовизуелних или других предмета пороногрофске садржине или приказивање порнографске представе детету *посредством информационо комуникационих технологије*, што квалификује ово кривично дело и као кривично дело које припада компјутерском криминалитету. У групи кривичних дела против полне слободе налази се и кривично дело „мамљење дјетета у циљу вршења кривичних дјела против полне слободе" (чл. 211б), које постоји када пунолетно лице у намери вршења кривичних дела против полне слободе предузме радње да дође до сусрета са дететом користећи средства информационо комуникационих технологија или на други начин.

---

[707] Под *рачунарским системом* подразумева се сваки уређај или група међусобно повезаних или условљених уређаја, од којих један или више њих, у зависности од програма, врши аутоматску обраду података; *рачунарски податак* је свако излагање чињеница, података или концепата у облику који је погодан за обраду у рачунарском систему, укључујући ту и програме помоћу којих рачунарски систем врши своје функције; *рачунарски програм* је скуп уређених рачунарских података на основу којих рачунарски систем врши своје функције; *рачунарски вирус* је рачунарски програм који угрожава или мења функције рачунарског система и мења, угрожава или неовлашћено користи рачунарске податке; *подаци у рачунарском саобраћају* су сви рачунарски подаци који генеришу рачунарски системи, који чине ланац комуникације између два рачунарска система који комуницирају укључујући и њих саме.

Кривична дела компјутерског криминалитета садржана су такође у одредбама Кривичног законика које се односе на интелектуалну својину. За разлику од већине законских решења у државама бивше СФРЈ, која, у оквиру заштите ауторских права, патента и интелектуалне својине, не помињу базу података, софтвер или електронску информацију, у Кривичном законику Црне горе у Глави двадесет првој „Кривична дјела против интелектуалне својине" предвиђено је кривично дело „*неовлашћено искоришћавање ауторског дјела или предмета сродног права*" (чл. 234), код кога се наводи *„база података"* као објект напада (неовлашћено објављивање, снимање, умножавање или на други начин јавно саопштавање или чињење доступним, у целини или делимично, ауторско дело, интерпретацију, фонограм, видеограм, емисију или *базу података* – ст.1, као и стављање у промет или држање неовлашћено умножене или неовлашћено стављене у промет ауторског дела, интерпретације, фонограма, видеограма, емисије или *базе података* – ст. 2). Посебно је предвиђено кривично дело „*неовлашћено уклањање или мијењање електронске информације о ауторском и сродним правима*" (чл. 236) које се састоји у неовлашћеном уклањању или измени електронске информације о ауторском и сродном праву или стављању у промет, увозу, емитовању или на други начин јавном саопштавању или чињењу доступним ауторског дела или предмета сродноправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена. Код оба крививична дела предвиђено је одузимање предмета извршења кривичних дела и предмета који су били употребљени или намењени за извршење кривичног дела и уништење предмета извршења.

Коришћење интернета приликом извршења кривичног дела наведено је код кривичног дела „*манипулација на тржишту хартија од вриједности или других финансијских инструмената*" (чл. 281а – Глава двадесет трећа „Кривична дјела против платног промета и привредног пословања"). Код наведеног кривичног дела санкционисано је ширење и преношење нетачних или обмањујућих информација које могу изазвати заблуду о хартијама од вредности или другим финансијским инструментима путем медија, *интернета* или на други начин. За постојање овог кривичног дела захтева се и знање извршиоца о томе да су информације нетачне, обмањујуће и да могу довести у заблуду корисника информација.

У посебној глави Кривичног законика предвиђено је неколико кривичних дела која припадају компјутерском криминалитету („Кривична дјела против безбједности рачунарских података" - Глава двадесет осма): оштећење рачунарских података и програма (чл. 394); ометање рачунарског система (чл. 350.); прављење и уношење рачунарских вируса (чл. 351); рачунарска превара (чл. 352); неовлашћени приступ рачунарском систему (чл. 353) и злоупотреба уређаја и програма (чл. 354).

Код кривичног дела *оштећења рачунарских података и програма* радња извршења се састоји у неовлашћеном брисању, измени, оштећењу, прикривању или на други начин чињењу неупотребљивим рачунарског податка или програма. Тежи облици овог кривичног дела постоје у случају проузроковања штете која прелази три хиљаде евра, односно тридесет хиљада евра.

Кривично дело *ометање рачунарског система* постоји када се унесе, уништи, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или рачунарски систем у намери да се омета рад рачунарског система. Предвиђен је тежи облик овог кривичног дела када се ради о подацима и програмима који су од знаћаја за државне органе, јавне службе, установе, привредна друштва или друге субјекте.

Рачунарска превара се састоји у уношењу, измени, брисању или пропуштању да се унесе тачан податак или на други начин прикривању или лажном приказивању рачунарског податка, као и у било каквом ометању рада рачунарског система, чиме се утиче на резултат електронске обраде, пренос података и функционисање рачунарског система. За постојање овог кривичног дела потребна је намера да се себи или другоме прибави противправна имовинска корист или се другоме проузрокује имовинска штета. Тежи облици се односе на оне случајеве када је прибављена имовинска корист која прелази износ од три хиљаде еура, односно износ од тридесет хиљада еура.

Кривично дело *неовлашћени приступ рачунарском систему* има пет облика: неовлашћен приступ рачунарском систему као целини или неком његовом делу; извршење дела уз кршење мера заштите рачунарског система или неовлашћен приступ рачунарском систему који је од значаја за државне органе, органе локалне самоуправе и установе којима је поверено вршење јавних овлашћења; неовлашћено пресретање рачунарских података, без обзира на начин њиховог преноса, који нису јавне природе ка рачунарском систему, од

њега или унутар самог система, укључујући и електромагнетну емисију; употреба рачунарског податка на начин предвиђен у претходим облицима; када услед употребе рачунарског податка на недозводен начин наступе тешке последице за другу особу.

Као посебно кривично дело инкриминисана су понашања која се односе на *злоупотребу уређаја и програма.* Кривично дело се састоји у производњи, продаји, набавци ради употребе, увозу, дистрибуцији или на други начин стављању на располагање: уређаја и рачунарских програма пројектованих или прилагођених првенствено у сврху извршења неког од наведених кривичних дела компјутерског криминалитета (чл. 349-353), као и рачунарске шифре или сличних података путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буде употребљен у сврху извршења неког од наведених кривичних дела компјутерског криминалитета (чл. 349-353).

ТАБЕЛАРНИ ПРИКАЗ ПРОПИСАНИХ КРИВИЧНИХ ДЕЛА

Компаративни преглед правног регулисања компјутерског криминаликтета у земљама бивше СФРЈ

Република Србија -члан КЗ -	Република Словенија -члан КЗ -	Република Хрватска -члан КЗ -	Федерација Босне и Херцеговине -члан КЗ -	Република Српска -члан КЗ -	Брчко Дистрикт -члан КЗ -	Црна Гора -члан КЗ -	БЈР Македонија -члан КЗ -	Косово -члан КЗ -
оштећење рачунарских података и програма (чл.298)	/	оштећење рачуналних података (чл.268)	оштећење рачуналних података и програма (чл.393)	оштећење рачунарских података и програма (чл.292а)	оштећење рачунарских података и програма (чл.387)	оштећење рачунарских података и програма (чл.349)	/	/
рачунарска саботажа (чл.299)	/	/	рачунална саботажа (чл.398)	рачунарска саботажа (чл.292б)	рачунарска саботажа (чл.392)	/	/	/
прављење и уношење рачунарских вируса (чл.300)	/	/	/	израда и уношење рачунарских вируса (чл.292в)	/	прављење и уношење рачунарских вируса (чл. 351)	правење и внесување на компјутерски вируси -прављење и уношење рачунарских вируса (чл.251 а)	/
рачунарска превара (чл.301)	/	рачунална пријевара (чл.271)	рачунална пријевара (чл.395)	рачунарска превара (чл.292г)	рачунарска превара (чл.389)	рачунарска превара (чл. 352)	компјутерска измама - рачунарска превара (чл.251 б)	/
неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302)	/	неовлаштени приступ (чл. 266)	неовлашћени приступ заштићеном суставу и мрежи електронске обраде података (чл.397)	неовлашћени приступ заштићеном рачунару, рачунарској мрежи, телекомуникационој мрежи и електронској обради података (чл.292д)	неовлашћени приступ заштићеном систему и мрежи електронске обраде података (чл.391)	неовлашћени приступ рачунарском систему (чл. 353) неовлашћени приступ заштићеном рачунару и рачунарској мрежи (чл.355) - брисан –	/	незаконит приступ информационим системима (Чл.64 Закона о услугама информатичког друштва Републике Косово)

Република Србија -члан КЗ -	Република Словенија -члан КЗ -	Република Хрватска -члан КЗ -	Федерација Босне и Херцеговине -члан КЗ -	Република Српска -члан КЗ -	Брчко Дистрикт -члан КЗ -	Црна Гора -члан КЗ -	БЈР Македонија -члан КЗ -	Косово -члан КЗ -
спречавање и ограничавање приступа јавној рачунарској мрежи (чл.303)	/	/	/	спријечавање и ограничавање приступа јавној рачунарској мрежи (чл.292ђ)	/	спрјечавање и ограничавање приступа јавној рачунарској мрежи (чл.356) - брисан -	/	/
неовлашћено коришћење рачунара или рачунарске мреже (чл.304)	/	/	/	неовлаштено кориштење рачунара и рачунарске мреже (чл.292е)	/	злоупотреба уређаја и програма (чл.354)	/	упад у рачунарске системе (чл. 339)
прављење, набављање и давање другом средства за извршење кривичних дела против безбедности рачунарских података (чл.304а)	/	злоупораба направа (чл.272)	/	/	/	/	/	/
приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл.185)	приказовање, изделава, посест ин посредовање порнографскега градива - презентација, производња, држање и стављање у порнографског материјала (чл.176)	искоришћавање дјеце за порнографију (чл. 163) искоришћавање дјеце за порнографске представе (чл.164)	искоришћавање дјетета или малољетника ради порнографије (чл.211)	Искоришћавање дјеце и малољетних лица за порнографију (чл.199)	Искоришћавање дјетета или малољетника ради порнографије (чл.208)	дјечја порно-графија (чл.211)	прикажување на порнографски материјал на малолетник - приказивање порнографског материјала малолетном лицу (чл. 193)	злоупотреба деце у порнографији (чл.238)

Република Србија -члан КЗ -	Република Словенија -члан КЗ -	Република Хрватска -члан КЗ -	Федерација Босне и Херцеговине -члан КЗ -	Република Српска -члан КЗ -	Брчко Дистрикт -члан КЗ -	Црна Гора -члан КЗ -	БЈР Македонија -члан КЗ -	Косово -члан КЗ -
искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл.185б)	придобивање осеб, млајших од петнајст лет, за сполне намене - врбовање особа млађих од 15 година за сексуалне намене (чл.173а)	/	/	/	/	/	/	/
/	/	упознавање дјеце с порнографијом (чл. 165)	упознавање дјетета с порнографијом (чл.212)	/	упознавање дјетета с порно-графијом (чл.209)	/	/	/
повреда моралних права аутора и интерпретатора (чл.198.)	кршитев моралних авторских правиц - повреда моралних права (чл.147)	/	/	/	/	повреда моралних права аутора и интерпретатора (чл.233)	/	повреда заштићених ауторских права (чл.296)
неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199.)	кршитев авторски сородних правиц - кршење ауторских и сродних права (чл. 149)	/	/	/	/	неовлашћено искоришћавање ауторског дјела или предмета сродног права (чл. 234)	/	/

Република Србија -члан КЗ -	Република Словенија -члан КЗ -	Република Хрватска -члан КЗ -	Федерација Босне и Херцеговине -члан КЗ -	Република Српска -члан КЗ -	Брчко Дистрикт -члан КЗ -	Црна Гора -члан КЗ -	БЈР Македонија -члан КЗ -	Косово -члан КЗ -
неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (чл. 200.)	/	/	/	/	/	неовлашћено уклањање или мијењање електронске информације о ауторском и сродним правима (чл.236)	/	/
повреда проналазачког права (чл. 201.) неовлашћено коришћење туђег дизајна (чл. 202.)	/	/	/	/	/	неовлашћено коришћење туђег патента (чл. 237) неовлашћено коришћење туђег дизајна (чл. 238)	/	/
неовлашћено фотографисање (чл.144) и неовлашћено објављивање и приказивање туђег списа, портрета или снимка (чл. 145) ***Не односе се посебно на интернет комуникацију.***	/	/	неовлашћено оптичко снимање (чл.189)	неовлашћено фотографисање (чл.175)	неовлашћено оптичко снимање (чл.186)	/	/	/

Република Србија -члан КЗ -	Република Словенија -члан КЗ -	Република Хрватска -члан КЗ -	Федерација Босне и Херцеговине -члан КЗ -	Република Српска -члан КЗ -	Брчко Дистрикт -члан КЗ -	Црна Гора -члан КЗ -	БЈР Македонија -члан КЗ -	Косово -члан КЗ -
фалсификовање новца (чл.223), фалсификовање хартија од вредности (чл.224), фалсификовање и злоупотреба платних картица (чл.225), фалсификовање знакова за вредност (чл.226), фалсификовање знакова за обележавање робе, мера и тегова (чл. 245), фалсификовање исправе (чл.355 и 356), фалсификовање службене исправе (чл.357). ***Не односе се посебно на рачунарско фалсификовање.***	/	рачунално кривотворење (чл.270)	рачунално кривотворење (чл.394)	/	рачунарско кривотворење (чл.388)	/	правење, набавување или отуѓување средства за фалсификување - израда, набављање или продаја средстава за фалсификување (чл.271)	производња, снабдевање, продаја, поседовање или набавка за употребу средстава за фалсификување (чл.304 став 3)

Република Србија -члан КЗ -	Република Словенија -члан КЗ -	Република Хрватска -члан КЗ -	Федерација Босне и Херцеговине -члан КЗ -	Република Српска -члан КЗ -	Брчко Дистрикт -члан КЗ -	Црна Гора -члан КЗ -	БЈР Македонија -члан КЗ -	Косово -члан КЗ -
повреда тајности писама и других пошиљки (чл.142)	кршитев тајности обчил - повреда тајности писама (чл.139)	повреда тајности писама и других пошиљака (чл.142)	повреда тајности писма или друге пошиљке (чл.186)	/	повреда тајности писма или друге пошиљке (чл.186)	повреда тајности писама и других пошиљки (чл. 172)	повреда на тајноста на писма или други пратки -повреда тајности писама и других пошиљки (чл. 147)	угрожавање приватности писма и рачунарских база података (чл.202)
/	/	ометање рада рачуналног сустава (чл.267)	ометање рада система и мреже електронске обраде података (чл.396)	/	ометање рада система и мреже електронске обраде података (чл.390)	ометање рачунарског система (чл. 350.)	/	/
/	/	/	/	Производња, посједовање и приказивање дјечије порнографије (чл.200)	/	/	производство и дистрибуција на детска порнографија - производња и дистрибуција дечије порнографије (чл.193а)	/
/	/	неовлаштено пресретање рачуналних података (чл.269)	/	/	/	/	/	/
/	/	тешка казнена дјела против рачуналних сустава, програма и података (чл.273)	/	/	/	/	/	/

Република Србија -члан КЗ -	**Република Словенија -члан КЗ -**	**Република Хрватска -члан КЗ -**	**Федерација Босне и Херцеговине -члан КЗ -**	**Република Српска -члан КЗ -**	**Брчко Дистрикт -члан КЗ -**	**Црна Гора -члан КЗ -**	**БЈР Македонија -члан КЗ -**	**Косово -члан КЗ -**
неовлашћено прикупљање личних података (чл.146) ***Не односе се посебно на интернет комуникацију.***	злораба осебних податков - злоупотреба личних података (чл.143)	недозвољена употреба особних података (чл.146)	/	неовлашћено коришћење личних података (чл. 176)	/	/	злоупотреба на личните податоци - злоупотреба личних података (чл. 149)	/
/	напад на информацијски систем - напад на информациони систем (чл.221)	/	/	/	/	/	/	/
/	кршитев материалних авторских правиц - кршење новчаних права аутора (чл.148)	/	/	/	/	/	/	/
/	/	/	/	/	/	мамљење дјетета у циљу вршења кривичних дјела против полне слободе (чл. 211б)	намамување на обљуба или друго полово дејствие на малолетник кој не наполнил 14 години - навођење на обљубу или другу сексуалну радњу малолетног лица млађег од 14 година (чл. 193 б)	/
/	/	/	/	/	/	/	изработка и употреба на лажна платежна картичка - израда и коришћење лажних платних картица (чл.274 б)	/

Република Србија -член КЗ -	Република Словенија -член КЗ -	Република Хрватска -член КЗ -	Федерација Босне и Херцеговине -член КЗ -	Република Српска -член КЗ -	Брчко Дистрикт -член КЗ -	Црна Гора -член КЗ -	БЈР Македонија -член КЗ -	Косово -член КЗ -
/	/	/	/	/	/	/	оштетување и неовластено навлегување во компјутерски систем - оштеќење и неовлашћен упад у компјутерски систем (чл.251)	/
/	/	/	/	/	/	/	повреда на права од индустриска сопственост и неовластена употреба на туѓа фирма - повреда права индустријске својине и неовлашћеног коришћења туђе фирме (чл.285)	/
/	/	/	/	/	/	/	ширење на расистички и ксенофобичен материјал по пат на компјутерски систем - ширење расистичког и ксенофобичног материјала преко рачунарских система (чл. 394 д)	/

Република Србија -члан КЗ -	**Република Словенија -члан КЗ -**	**Република Хрватска -члан КЗ -**	**Федерација Босне и Херцеговине -члан КЗ -**	**Република Српска -члан КЗ -**	**Брчко Дистрикт -члан КЗ -**	**Црна Гора -члан КЗ -**	**БЈР Македонија -члан КЗ -**	**Косово -члан КЗ -**
неовлашћено прислушкивање и снимање (чл.143) ***Не односи се посебно на интернет комуникацију.***	/	/	неовлашћено прислушкивање или снимање туђих порука у рачунарском систему (чл. 188)	неовлашћено прислушки-вање и тонско снимање (чл. 174)	неовлашћено прислушкивање или снимање туђих порука у рачунарском систему (чл. 188)	/	/	/
/	/	/	/	/	/	/	/	одавање технолошких мера (чл. 297)
/	/	злоупораба тржишта капитала (чл. 260)	/	/	/	манипулација на тржишту хартија од вриједности или других финансијских инструмената (чл. 281а)	/	/
/	/	/	**Кривични закон Босне и Херцеговине** не садржи посебне одредбе о компјутерском криминалитету јер су те одредбе садржане у ентитетском кривичном законодавству. Овај закон нормира и санкционише кривично дело неовлашћено прислушкивање или оптичко снимање (чл. 147а), док је код кривичних дела која се односе на повреду ауторских права из Главе XXI радња извршења тако широко постављена да може да обухвати и извршење ових кривичних дела употребом рачунарског система, иако то није изричито наведено.			/	/	/

2.5. Косово [708]

„Кривични законик Републике Косове“[709] садржи мали број кривичних дела која могу бити учињена коришћењем рачунарских система или опреме. Ова кривична дела нису обухваћена посебном главом Кривичног законика, већ се налазе у оквиру других глава КЗ.

У ***Глави XVII „Кривична дела против права и слобода лица”*** нормирано је је кривично дело *угрожавање приватности писма и рачунарских база података* (чл. 202 КЗ). Кривично дело има четири облика. Први облик кривичног дела постоји када неко лице без овлашћења отвори писмо, телеграм, факсимил, или други затворени документ, пакет или електронску комуникацију другог лица, или на било који други начин наруши приватност тих материјала, или, без овлашћења, задржи, прикрије, уништи или испоручи било ком лицу писмо, телеграм, факсимил, електронску комуникацију или други затворени документ или пакет другог лица. Радња другог облика кривичног дела састоји се у улажењу без овлашћења у рачунарску базу података другог лица или коришћење података добијених из те базе података или чињењу доступним другоме података из те базе. Уколико је кривично дело извршено ради прибављања имовинске користи за себе или друго лице или или у сврхе изазивања штете другом лицу постоји трећи облик овог кривичног дела. Најтежи облик постоји ако је кривично дело извршило овлашћено лице злоупотребљавајући своју позицију или овлашћење.

У Глави ***XX „Кривична дела против сексуалног интегритета“***, у чл. 238 прописано је кривично дело *злоупотреба деце у порнографији***,** при чему је у ставу 5 прецизирано да се кривичним делом сматра производња дечје

---

[708] Од завршетка рата на Косову и потписивања војно-техничког споразума у Куманову 1999. године, као и доношења Резолуције Савета безбедности ОУН 1244, Косово се налази под прелазном администрацијом УН (УНМИК), а од 2008. године и под Мисијом Европске Уније под називом ЕУЛЕКС. Република Србија сматра Косово делом своје територије (аутономна покрајина Косово и Метохија), док је Парламент Косова 2008. године донео одлуку о проглашењу независности од Србије, тако да на највећем делу територије са већинским албанским становништвом, функционише самопроглашена држава Република Косово.

[709] Привремени Кривични закон Косова ступио је на снагу 6. априла 2004. године на основу УНМИК Уредбе 2003/23, док је „Кривични законик Републике Косове“ бр. 04/2-082 објављен у „Службеном листу Републике Косова“ бр. 19/13 из јула 2012. године. Законик је ступио на снагу 01.01.2013. године.

порнографије или коришћење дете у прављењу или производњи представе уживо односно посредством средстава информационе и комуникационе технологије.

Кривично дело *одавање технолошких мера* (чл. 297) садржано у Глави XX „Кривична дела против економије" састоји се у одавању било којих технолошких мера које се користе или уклањање, склањање или промена информација из права о електронском управљању из Закона о заштити ауторских и сродних права. У оквиру исте главе садржано је и кривично дело *производња, снабдевање, продаја или набавка за употребу средстава за фалсификовање* (чл.304). Кривично дело има два облика. Код првог облика, радња извршења састоји се у производњи, продаји, примању, поседовању или набављању за употребу средства за фалсификовање новца, средстава обезбеђења или инструмената плаћања (ст. 1); док се код другог облика радња извршења састоји у производњи, снабдевању, примању, поседовању или набавци за употребу средства за фалсификовање фискалних, поштанских или других вредносних маркица, ознака за преварно обележавање или нетачних мера и тегова (ст. 2). У ст. 3 предвиђено је да „средства за фалсификовање" укључују инструменте, предмете, ***рачунарске програме*** и било која друга средства посебно намештена за фалсификовање или измену новца, средстава обезбеђења или плаћања, вредносних маркица, ознака за обележавање добара, мера и тегова, или холограма или друге компоненте новца, средстава обезбеђења или плаћања, које служе заштити од фалсификовања.

Кривично дело које се директно односи на рачунарске податке и рачунарске системе је кривично дело *упад у рачунарске системе (чл. 339**, Глава XXVII – Кривична дела против имовине***). Извршиоцем овог кривичног дела сматра се свако лице које које неовлашћено и са намером да прибави себи или другоме имовинску корист или да другоме изазове штету, измени, објави, избрише или уништи рачунарске податке или програме или на било који начин упадне у рачунарски систем. Друго кривично дело се односи на приватност писама и рачунарких база података.

Законик о кривичном поступку[710] предвиђа да државни тужилац може у поступку прикупљања доказа пре давања исказа у претходном поступку да добије све документоване доказе, који могу да подразумевају и електронска документа попут електронске поште, текстуалних порука и фотографија (чл. 121 став 1 тачка 1.7). За рачунарску анализу, рачунарску опрему, електронске медије за похрањивање или сличне уређаје, који су легално прибављени на основу судске наредбе или уз пристанак, државни тужилац може овластити полицијског службеника који има образовање, обуку или искуство у форензичкој рачунарској анализи и претраживању или вештака да испита, анализира и претражи информације или податке садржане у рачунарској опреми, електронским медијима за похрањивање или сличним уређајима (чл. 147). У извештају који доставља, овлашћени полицијски службеник или други стручњак наводе обавезно опис рачунарске опреме, опреме за похрањивање података или посебне рачунарске датотеке које је прегледао, укључујући и сва имена лице, бројеве или ознаке на доказним предметима који служе за идентификацију; опис места и начина на који је полиција прибавила рачунарску опрему, опрему за похрањивање података или посебну рачунарску датотеку; опис тока чувања рачунарске опреме, опреме за складиштење података или посебне рачунарске датотеке; опис одређене чињеничне информације за коју је био овлашћен да је претражи у рачунарској опреми, опреми за складиштење података или посебним рачунарским датотекама; опис корака предузетих у праћењу најновијих пракси у области рачунарске форензике како би се поуздано и прецизно обавило претраживање, укључујући али не ограничавајући се на кораке предузете за заштиту датотека од губитка, дешифровање датотека, враћање избрисаних датотека или добијање метаподатака о рачунарским датотекама или електронској пошти као и опис резултата претраживања и електронски примерак рачунарских датотека релевантних за претраживање. Овај Законик не даје дефиницију *електронског доказа* који би се појавио приликом вршења кривичних дела из области компјутерског криминалитета.

[710] Законик бр.04/L-123 о кривичном поступку Косова од 13. децембра 2012.године, „Службени лист Републике Косова“ бр. 37/28 из децембра 2012. године, доступно на: http://projuris.org/Zakoni_Kosova/Zakonik_o_krivicnom_postupku_2012.pdf, претражено 29. 07. 2015. године

Закон о услугама информатичког друштва[711] дефинише појам обраде личних података као сваку обраду, радњу или број радњи које се обављају у личним подацима, било аутоматским или неаутоматским средствима, као што могу бити: састанак, регистровање, организовање, чување, прилагођавање или исправка, кориговање, консултација, искоришћавање, преносна емисија, дистрибуција, или се омогућити увођење, ређање, комбиновање, блокирање, брисање или уништење података (чл. 2 тач. 1.33). У Поглављу XIV које се односи на заштиту информативног система информатичког друштва предвиђено је кривично дело ***незаконит приступ информационим системима*** (чл. 64). Незаконит приступ информационим системима подразумева намерни и бесправни приступ једном делу или читавом информационом систему када се врши против било ког дела информационог система, у циљу проузроковања штете физичком или правном лицу, у циљу економске користи, као и у случају прислушкивања података.[712] Под бесправном намерном радњом Закон подразумева запреку или озбиљан прекид функционисања информационог система упадајући, преносећи, оштећујући, бришући, кварећи, измењујући, куцајући или тумачећи неприступне компјутерске податке; као и брисање, квар, измену, куцање или тумачење неприступачних компјутерских података у информационом систему, када се то учини ради проузроковања штете физичком или правном лицу (чл. 64). Кажњиво је и намерно подстрекавање ради помагања или подстицања извршења овог кривичног дела (чл. 65). Тежи облик кривичног дела постоји уколико је кривично дело извршено у оквиру криминалне организације, ако је проузроковало знатну материјалну штету или непосредни или индиректан губитак, физичко оштећење физичког лица или знатно оштећење у делу критичне инфраструктуре Косова (чл. 66).

Закон о ауторском и сродном праву[713] у складу са чл. 10 Конвенције 185 о високотехнолошком криминалу пружа заштиту и електронској интелектуалној својини – компјутерским програмима, али само делимично.

---

[711] „Закон о услугама информатичког друштва Републике Косово“ – Закон бр. 04-L-094 од 02. 04. 2012. године, доступно на: http://www.kuvendikosoves.org/common/docs/ligjet/Zakon%20o%20uslugama%20informatickog%20drustva.pdf

[712] *Ibid.*

[713] Закон о ауторском и сродном праву Републике Косово – Закон бр. 04-L-065 од 18. 11. 2011. године, доступно на http://www.kuvendikosoves.org/common/docs/ligjet/Zakon%20o%20autorskom%20i%20srodnom%20pravu.pdf

Наиме, аутор компјутерског програма задржава сва ауторска права над програмом само уколико он није направљен у току испуњавања редовних радних задатака или према упутствима послодавца. У супротном, сва имовинска права и ауторска права над програмом без ограничења се преносе на послодавца односно наручиоца програма (чл. 120).

2.6. Република Македонија

Република Македонија потписала је Конвенцију бр. 185 новембра 2001. године, ратификовала је септембра 2004. године, а обавеза примене је настала од јануара 2005. године.

Кривичним законом[714] прописана су бројна кривична дела која се односе на безбедност и злоупотребу рачунарских система и рачунарских података, као и на тајност објављених података. Највећи број ових кривичних дела налази се у Глави XXV – **Кривична дела против јавних финансија, платног промета и економије** (мак. Кривични дела против јавните финансии, платниот промет и стопанството) и ту спадају: *израда, набављање или продаја средстава за фалсификовање* (чл. 271 – мак. правење, набавување или отуѓување средства за фалсификување), *израда и коришћење лажних платних картица* (чл. 274б – мак. изработка и употреба на лажна платежна картичка), *оштећење и неовлашћен упад у компјутерски систем* (чл. 251 – мак. оштетување и неовластено навлегување во компјутерски систем), *прављење и уношење рачунарских вируса* (чл. 251а – мак. правење и внесување на компјутерски вируси) и *рачунарска превара* (чл. 251б – мак. компјутерска измама).

У Глави XV – ***Кривична дела против слободе и права човека и грађанина*** (мак. кривични дела против слободите и правата на човекот и граганинот) предвиђена су, поред осталог, следећа кривична дела, која такође припадају компјутерском криминалитету: *повреда тајности писама и других пошиљки* (чл. 147 – мак. повреда на тајноста на писма или други пратки) и *злоупотреба личних података* (чл. 149 – мак. злоупотреба на личните податоци). Код кривичног дела повреде тајности писама и других пошиљки

[714] Кривичниот законик на Република Македонија („Службен весник на Република Македонија“ број 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7 /08, 139/08, 114/09, 51/11, 135/11, 185/2011, 142/2012, 166/2012, 55/2013)

писмо је изједначено са електронском поштом и за њено неовлашћено отварање предвиђена је санкција. Интересантно је да је покушај кривичног дела *злоупотреба личних података* такође кажњив.

Као кривична дела компјутерског криминалитета могу се навести и нека кривична дела из Главе XIX – ***Кривична дела против полне слободе и сексуалног морала*** (мак. кривични дела против половата слобода и половиот морал). То су: *приказивање порнографског материјала малолетном лицу* (чл. 193 – мак. прикажување на порнографски материјал на малолетник), *производња и дистрибуција дечије порнографије* (чл. 193а – мак. производство и дистрибуција на детска порнографија) и *навођење на обљубу или другу сексуалну радњу малолетног лица млађег од 14 година* (чл. 193б – мак. намамување на обљуба или друго полово дејствие на малолетник кој не наполнил 14 години). Један облик радње извршења кривичног дела *навођење на обљубу или другу сексуалну радњу малолетног лица млађег од 14 година* постоји када неко лице коришћењем компјутерских комуникација закаже састанак са лицем млађим од 14 година или га на други начин намами на сексуални однос, друге сексуалне активности или производњу дечије порнографије.

У македонском КЗ предвиђено је кривично дело које не познају други законски прописи земаља бивше СФРЈ. То је кривично дело *ширење расистичког и ксенофобичног материјала преко рачунарских система* (чл. 394д – мак. ширење на расистички и ксенофобичен материјал по пат на компјутерски систем) предвиђено у Глави XXXIII – **Кривична дела против јавног реда** (мак. кривични дела против јавниот ред). Према одредби закона ово кривично дело врши свако ко користи компјутерски систем ради јавног ширења расистичког и ксенофобичног писаног материјала, слика или идеје која помаже, промовише или подстиче мржњу, дискриминацију или насиље против било ког лица или групе на основу расе, боје коже, националног или етничког порекла, верских уверења. Кривично дело има тежи облик ако је реч о лицу које дело врши злоупотребом положаја или овлашћења.

Треба напоменути да у домену процесног права, македонско законодавство садржи неколико битних одредби које су везане за компјутерски криминалитет. **Закон о кривичном поступку *(мак. Законот на кривичната***

постапка)[715] прописује *поступак за претрагу рачунарског система и рачунарских података* (чл. 184). На захтев овлашћеног лица, лице које користи рачунар или му има приступ у обавези је да овлашћеном лицу омогући приступ и претрагу података, као и да предузме хитне мере и спречи уништење или измену података. У чл. 252 овог Закона као посебна истражна мера предвиђа претраживање и *омогућавање увида у рачунарски систем,* као и *праћење и снимање телефонских и других електронских комуникација* (чл. 251 ст. 1).

Македонија је такође уложила напоре да образује јак институционални оквир за борбу против високотехнолошког криминалитета. При Министарству унутрашњих послова, у оквиру Одељења за организован криминал, јануара 2005. године је основано Одељење за кибернетички криминал и фалсификате, септембра 2008. године ово Одељење је прерасло у Јединицу за компјутерски криминал, док је октобра 2013. године добило своје коначно устројство као Сектор за компјутерски криминал и дигиталну форензику.

[715] Законот на кривичната постапка („Службен весник на Република Македонија“ број 150/2010, 100/2012)

3. Законодавни и институционални оквир за супротстављање компјутерском криминалитету у Републици Србији

Потписивањем Конвенције о високотехнолошком криминалу 185 и Додатног протокола (2005. године), а посебно ратификовањем (2009. године), Република Србија је преузела обавезу да створи нормативне и институционалне претпоставке за успешно супротстављање компјутерском криминалитету. Због тога је донето више прописа (закона и подзаконских аката) у којима су имплементиране поједине одредбе Конвенције и на основу којих је створен институционални оквир за њихово спровођење. Најважнији међу њима су следећи закони: Кривични законик Републике Србије,[716] Законик о кривичном поступку Републике Србије, [717] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала,[718] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима,[719] Закон о ауторским и сродним правима[720] и Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине.[721] Поред наведених закона који се односе и на компјутерски криминалитет, треба поменути и законе којима се регулише електронско пословање и који предвиђају прекршајну одговорност за поједина недозвољена понашања. То су: Закон о електронском потпису,[722] Закон о електронској трговини,[723] Закон о електронском документу[724] и Закон о оптичким дисковима.[725]

Институционални оквир за спровођење одредби закона који се односе на високотехнолошки криминалитет обухвата посебне организационе јединице

---

[716] Кривични законик Републике Србије („Службени гласник РС” бр.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 и 104/2013)
[717] Законик о кривичном поступку („Службени гласник РС” бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014)
[718] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС” бр.61/2005 и 104/2009)
[719] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима („Службени гласник РС” бр.32/2013)
[720] Закон о ауторским и сродним правима („Службени гласник РС“ бр. 104/2009, 99/2011 и 119/2012).
[721] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине („Службени гласника РС“ бр. 46/2006, 104/2009 – др. закони)
[722] Закон о електронском потпису („Службени гласник РС” бр.135/2004)
[723] Закон о електронској трговини („Службени гласник РС“ 41/2009 и 95/2013)
[724] Закон о електронском документу („Службени гласник РС“ 51/2009)
[725] Закон о оптичким дисковима („Службени гласник РС“ 52/2011)

постојећих државних органа, чије деловање доприноси бољој заштити од копјутерског криминалитета и спровођењу превентивних и репресивних мера. Специјализација државних органа за борбу против компјутерског криминалитета неопходна је због сложености и посебних карактеристика компјутерског криминалитета, као и због сталног праћења развоја савремених компјутерских технологија.

Поред посебних организационих јединица у државним органима, значајну улогу у овој област имају Министарство трговине, туризма и комуникацијама,[726] Републичка агенција за електронске комуникације (РАТЕЛ) и Републичка радиодифузна агенција (РРА).[727]

3.1. Кривични законик Републике Србије и кривична дела компјутерског криминалитета

Кривични законик Републике Србије (у даљем тексту: КЗ РС) садржи прописе материјалноправног карактера који се односе на компјутерски криминалитет на тај начин што у оквиру Главе XXVII предвиђа *кривична дела против безбедности рачунарских података*, али и друга кривична дела која се на основу Конвенције о високотехнолошком криминалу и позитивноправних законских прописа сматрају кривичним делима компјутерског криминалитета. У том смислу, кривична дела компјутерског криминалитета предвиђена КЗ РС могу се сврстати у три групе: (1) сва кривична дела која за групни заштитни објекат имају безбедност рачунарских података; (2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала

[726] Министарство трговина, туризма и телекомуникација обавља, поред осталог, државне послове који се односе на област телекомуникација и информатичког друштва, који се односе на предлагање политике и стратегија развоја информационог друштва, припрему закона, других прописа, стандарда и мера у области електронског пословања, развоја и примене информационо комуникационих технологија, заштиту података и информациону безбедност, међународне послове у области информационог друштва и сл. *Наведено према* Закону о министарствима „Службени гласник Републике Србије бр. 44/2014, 14/2005 и 52/2015.

[727] *Видети*: Регулаторна агенција за електронске комуникације и поштанске услуге, www.ratel.rs, претражено 25. 08. 2015. године и Регулаторно тело за електронске медије, http://www.rra.org.rs/cirilica, претражено 25. 08. 2015. године

материјална штета прелази износ од милион динара и (3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира, уставног уређења и безбедности Републике Србије, која због начина извршења или употребљених средстава несумњиво припадају компјутерском криминалитету.[728]

Одредбе које се односе на област компјутерског криминалитета садржане су пре свега у општем делу Кривичног законика који се односи на „значење израза“ (чл.112 тач. 16-20 и 33-34 КЗ). Дефинисани су појмови *рачунарског податка* (представљена информација, знање, чињеница, концепт или наредба који се уносе, обрађују или памте или су унети, обрађени или запамћени у рачунару или рачунарској мрежи), *рачунарске мреже* (скуп међусобно повезаних рачунара који комуницирају размењујући податке), *рачунарског програма* (уређени скуп наредби који служи за управљање радом рачунара или за решавање одређеног задатка помоћу рачунара), *рачунарског вируса* (рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу, који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података), *рачунара* (сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке) и *рачунарског система* (сваки уређај или група међусобо повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података).

3.1.1. Кривична дела против безбедности рачунарских података

Прва група кривичних дела компјутерског криминалитета односи се на безбедност рачунарских података (Глава XXVII) и она су углавном садржана и у Конвенцији о високотехнолошком криминалу, што показује да је Србија у највећем делу прихватила предлоге дате у Конвенцији у погледу инкриминисања појединих кривичних дела. У складу са одредбама чл. 4, 5, 6, 7 и 8 Конвенције, у Кривичном законику су предвиђена следећа кривична дела:

[728] Чл. 3 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала.

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), неовлашћено коришћење рачунара или рачунарске мреже (чл. 304) и прављење, набављање и давање другом средства за извршење кривичних дела против безбедности рачунарских података (чл. 304а).

Оштећење рачунарских података и програма састоји се у неовлашћеном брисању, измени, оштећењу, прикривању или чињењу неупотребљивим рачунарског податка или програма. Ово је основни облик кривичног дела, а квалификовани облици постоје када штета проузрокована кривичним делом прелази одређени новчани износ. За правилну квалификацију овог кривичног дела неопходно је утврдити да ли је извршилац поступао неовлашћено и да ли је последица дела неупотребљивост рачунарског податка или програма. С обзиром на радњу извршења овог кривичног дела, често је отежано прикупљање доказа због чега каснији повраћај података не представља околност која елиминише постојање кривичног дела.[729]

Под *рачунарском саботажом* подразумева се дело уношења, уништавања, брисања, измене, оштећења, прикривања или на други начин чињења неупотребљивим рачунарског податка или програма или уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. Ово кривично дело се разликује од претходног по тежини последица које су проузроковане јер се код рачунарске саботаже појављује као радња извршења и уношење податка у рачунар што доводи до

[729] Најчешћи вид извршења овог кривичног дела је рушење веб сајтова. Хакери нападају најчешће само део сајта, на пример насловну страну која се промени и на њој се остави хакерски „потпис“ , порука или поздрав. Слаба заштита веб сајтова и недовољна информисаност о опасностима које могу доћи са интернета погодују вршењу ових кривичних дела. Извршиоце је врло тешко открити јер они користе алате за скривање који онемогућавају утврђивање места са кога је напад дошао. *Видети више:* Николић Комлен, Лидија, Гвозденовић, Радоје, Радуловић, Саша, Милосављевић, Александар, Јерковић, Ранко, Живковић, Владан, Живановић, Саша, Рељановић Марио; Алексић Иван: „Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу“, *op.cit.,* 2010, стр. 91

неупотребљивости рачунарског податка или програма, односно уништења или оштећења рачунара. Осим тога, ради се о подацима који су значајни за државне органе, јавне службе, установе, предузећа или друге субјекте, што такође повећава друштвену опасност овог кривичног дела.

Кривично дело *прављење и уношење рачунарских вируса* има два облика: прављење рачунарског вируса у намери његовог уношења у туђ рачунар или рачунарску мрежу и уношење рачунарског вируса у туђ рачунар или рачунарску мрежу при чему је настала штета. Рачунарски вируси се веома лако шире глобалном рачунарском мрежом, електронском поштом, програмима за размену порука и системима за дељење података. Такође се могу пренети посетом одређеним веб сајтовима или преузимањем садржаја са интернета. Штетне последице које остављају рачунарски вируси огледају се у отежаној приватној и пословној комуникацији, неконтролисаном слању приватних података корисника, трајно брисање података, непланирано гашење рачунара, онеспособљавање оперативног система рачунара или оштећење хардвера. Поред вируса посебна врста злонамерних програма су „црви“ („мрежни црви“) који се крећу кроз рачунарску мрежу и могу да продру у рачунарски систем. „Црви“ се брзо умножавају, шире се без помоћи корисника и сами дистрибуирају сопствене копије широм мрежа. Деловањем рачунарских вируса могу се угрозити објекти инфраструктуре, нуклеарна постројења, системи одбране и сл. Код овог кривичног дела поред казне предвиђено је одузимање уређаја и средстава којима је кривично дело учињено.

Рачунарска превара се може извршити уношењем нетачног податка, пропуштањем уношења тачног податка, прикривањем или лажним приказивањем податка, чиме извршилац утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету. Тежи облици овог кривичног дела постоје у два случаја: када износ прибављене противправне имовинске користи прелази износ од четиристотине педесет хиљада динара и када износ прелази милион петсто хиљада динара. Ово кривично дело има привилегован облик када је дело извршено само у намери да се другоме причини штета. За правилну квалификацију кривичног дела и доказивање рачунарске преваре потребно је, поред осталог, тачно утврдити радњу која је

предузета, начин уношења неистинитог податка, у чему се неистинитост огледа и какав је био утицај на резултат електронске обраде и преноса података. С обзиром на то да је у данашње време електронско пословање између привредних субјеката постало неопходан начин пословања, ово кривично дело се може извршити на штету свих привредних субјеката.[730]

Кривично дело *рачунарске преваре* треба разликовати од класичног кривчног дела *преваре* (чл. 208 КЗ РС) које припада имовинском криминалитету, односно групи кривичних дела против имовине. Иако у закону није изричито наглашено, кривично дело преваре може бити извршено коришћењем рачунарских технологија, када извршилац у намери да себи или другоме прибави противправну имовинску корист лажним приказивањем неких чињеница или њихвим прикривањем оштећеног доведе у заблуду или га одржава у заблуди и тиме га наведе да на штету своје или туђе имовине нешто учини или не учини. Појава интернета отворила је широке могућности за вршење кривичног дела преваре, повећала број потенцијалних жртава и скоро сасвим отклонила трошкове потребне за извршење кривичног дела. Начини извршења превара коришћењем компјутера и интернета су различити, извршиоци су потпуно анонимни, а жртва може да постане свако ко користи рачунарску технологију.[731]

Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података састоји се у кршењу мера заштите неовлашћеним укључивањем у рачунар или рачунарску мрежу или у

---

[730] У домаћој судској пракси забележено је неколико случајева процесуирања кривичног дела рачунарске преваре. Тужилаштво за борбу против високотехнолошког криминала покренуло је истрагу против осумњиченог Ч.А. због основане сумње да је током 2007. и 2008. године у два наврата користећи рачунар улазио у системе банака у Аустралији и Швајцарској и издавао лажне налоге за трансфер средстава, чиме је прибавио противправну имовинску корист у износу од 51.990 CHF, односно да је покушао да из једне швајцарске банке неовлашћено изврши трансфер средстава у износу од 19.000 USD. Такође је забележено више случајева злоупотребе рачунарских система рачунарских мрежа у спортским кладионицама. Извршиоци на различите начине покушавају да утичу на резултат електронске обраде података и користећи софтверска решења фалсификују одигране тикете. *Више о томе:* Николић Комлен, Лидија, Гвозденовић, Радоје, Радуловић, Саша, Милосављевић, Александар, Јерковић, Ранко, Живковић, Владан, Живановић, Саша, Рељановић Марио; Алексић Иван: „Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу“, *op.cit.,* 2010, стр. 102 и 103 *и* Прља, Драган, Ивановић, Звонимир, Рељановић, Марио: „Кривична дела високотехнолошког криминала“, Институт за упоредно право, Београд, 2011, стр. 173

[731] Најпознатији пример за начине преваре путем интернета је тзв. „нигеријско писмо“, које представља синоним за лажне e-mail поруке. Више о овој појави видети на стр. 192 рада.

неовлашћеном приступу електронској обради података, као и у употреби података добијених на овај начин.

Посебан тежи облик овог кривичног дела постоји уколико је услед извршења наведених радњи дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице. Ово кривично дело је према начину извршења слично кривичном делу *шпијунаже (чл.315 КЗ)*, које припада групи кривичних дела против уставног уређења и безбедности Републике Србије. Због тога је приликом квалификације кривичног дела неопходно да се са сигурношћу утврди да ли је упадом у рачунарски систем извршилац дошао до војних, економских или службених података или докумената који су законом, другим прописом или одлуком надлежног органа донетом на основу закона, проглашени тајним; да ли је одавање таквих података проузроковало штетне последице за безбедност, одбрану или за политикче, војне или економске интересе земље и какав је умишљај учиниоца.

Спречавање и ограничавање приступа јавној рачунарској мрежи постоји када се неовлашћено спречава или омета приступ јавној рачунарској мрежи, док тежи облик овог дела постоји уколико је дело учинило службено лице у вршењу службе. Рачунарске мреже су доступне великом броју лица, користе се у свакодневном животу за информације, обављање финансијских трансакција, електонске трговине или одржавање друштвених контаката и изложене су неовлашћеном спречавању или ометању приступа. Овим кривичним делом се забрањује управо овакав неовлашћен приступ јер он може да доведе до потпуног онемогућавања или отежавања приступа јавној рачунарској мрежи. Доказивање овог кривичног дела је веома тешко због немогућности идентификовања идентитета извршилаца напада, великог броја „заражених“ рачунара чији корисници нису ни свесни да им је рачунар злоупотребљен.[732]

---

[732] Најчешћи су DDoS (Distributed Denial of Sevice) напади, када се помоћу одређеног малициозног софтвера остварује контрола над великим бројем рачунара. Пример за ове нападе је напад на интернет сајт Православне цркве и обарање интернет презентације радиоемисије „Печшаник“. *Видети*: Николић Комлен, Лидија, Гвозденовић, Радоје, Радуловић, Саша, Милосављевић, Александар, Јерковић, Ранко, Живковић, Владан, Живановић, Саша, Рељановић Марио; Алексић Иван: „Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу“, *op.cit.,* 2010, стр. 108. Cyber секција Народноосободилачког фронта преузела је пуну одговорност за напад на хрватски Телеком, који

Неовлашћено коришћење рачунара или рачунарске мреже извршава особа која неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист. За разлику од претходних кривичних дела, за ово кривично дело гоњење се предузима по приватној тужби. Неовлашћено коришћење рачунара и рачунарске мреже може се појавити приликом извршења кривичних дела против части и угледа (Глава XVII КЗ Србије), посебно кривичних дела увреде (чл. 170), изношење личних и породичних прилика (чл. 172) и повреда угледа због расне, верске, националне или друге припадности (чл. 174). Ипак, у Кривичном законику код наведених кривичних дела није инкриминисан као начин извршења неовлашћено коришћење рачунарских услуга или рачунарске мреже.

Кривично дело *Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података* постоји када извршилац поседује, прави, набавља, продаје или даје другом на употребу рачунаре, рачунарске системе, рачунарске податке и програме ради извршења једног од кривичних дела *против безбедности рачунарских података* (Глава XXVII КЗ РС). Предвиђање наведеног кривичног дела у Кривичном законику у складу је са чл. 6 Конвенције о високотехнолошком криминалу, који под *злоупотребом уређаја* подразумева производњу, продају, набављање ради употребе, увоз, дистрибуцију и друге облике стављања на располагање уређаја, укључујући и рачунарски програм ради извршења дела прописаних Конвенцијом.

У случају извршења овог кривичног дела, предмети који су коришћени за извршење (рачунари, рачунарски системи, рачунарски подаци и програми) биће одузети од извршилаца.

За наведена кривична дела у Кривичном законику предвиђене су одређене кривичне санкције. Према Конвенцији о високотехнолошком криминалу (чл. 13) свака држава уговорница треба да усвоји законодавне и друге мере неопходне да би се обезбедило да кривична дела која припадају

се догодио у току ноћи 21.и 22. 09. 2015. године, тврди да су напад извели јер се боре против капитализма и за успостављање самоуправног социјалистичког друштва. Али и на Twitteru KuNaNeT стоји порука како су они извршили DdoS напад, тако да није познато да ли су те две групе хакера повезане. *Видети:* Јутарњи лист, www.jutarnji.hr, претражено 22. 09. 2015. године.

вискотехнолошком криминалу подлежу делотворним, пропорционалним и одвраћајућим санкцијама, које укључују и лишавање слободе. У том смислу Кривични законик је предвидео за сваки облик кривичног дела посебну кривичну санкцију и то: новчану казну или затвор до 3 месеца (чл. 304); новчану казну или затвор до 6 месеци (чл. 300/1, чл. 301/4, чл. 302/1); новчану казну или затвор до једне године (чл. 298/1 и 303/1); новчану казну или затвор до две године (чл. 302/2); затвор три месеца до три године (чл. 298/2), затвор три месеца до пет година (чл. 298/3); затвор шест месеци до три године (чл. 304а/1); затвор шест месеци до пет година (чл. 299); затвор до две године (чл. 300/2); затвор до три године (чл. 301/1, 302/3, 303/2); затвор од једне до осам година (чл. 301/2) и затвор од две до десет година (чл. 301/3). Уколико дође до измене Кривичног законика требало би, на основу судске праксе, размотрити да ли су ове предвиђене санкције биле делотворне, пропорционалне и одвраћајуће од вршења ових кривичних дела, како је одређено Конвенцијом о високотехнолошком криминалу.

3.1.2. Остала кривична дела која припадају компјутерском криминалитету

Поред кривичних дела прописаних у Глави XXVII Кривичног законика Републике Србије која се односе на дела против безбедности рачунарских података, КЗ РС у оквиру Главе XVIII која се односи на *кривична дела против полне слободе* предвиђа кривична дела у вези са дечијом порнографијом, што у потпуности одговара чл. 9 Конвенције о високотехнолошком криминалу и Конвенцији о заштити деце од сексуалне експлоатације и сексуалног злостављања. Неопходност предвиђања и санкционисања ових кривичних дела у Кривичном законику произилази из чињенице да је, уз злоупотребу платних картица и пиратерију, злоупотреба малолетника и деце за порнографију најчешћи појавни облик високотехнолошког криминалитета. Педофилске веб странице и форуме веома је тешко открити јер су сајтови заштићени шифрама, имају више нивоа приступа, а заинтересоване особе морају саме понудити материјал како би постали чланови. Због отежаног откривања и процесуирања, у борбу против педофилије на интернету укључен је велики број људи,

удружења грађана која помажу жртвама, међународних организација, посебних полицијских јединица, тужилаштва и судова.[733] Кривична дела у вези са дечијом порнографијом предвиђена су пре свега због заштите психофизичког и полног интегритета малолетника и деце јер су они жртве ових кривичних дела.

Кривично дело *приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл.185 КЗ РС)* има четири облика с обзиром на радње извршења овог кривичног дела: (1) продаја, приказивање, чињење доступним јавним излагањем или на други начин текстова, слика, аудиовизуелних или других предмета порнографске садржине или приказивање порнографске представе малолетнику (према чл. 112 тач. 9 КЗ РС то је лице које је навршило 14 а није навршило 18 година); (2) искоришћавање малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу; (3) извршење оба облика кривичних дела према детету (према чл. 112 тач. 8 КЗ РС дететом се сматра лице које није навршило 14 година) и ово је тежи облик кривичног дела; (4) прибављање за себе или другог, поседовање, продаја, приказивање, јавно излагање или *електронски* или на други начин чињење доступним слике, аудио визуелног или другог предмета порнографске садржине настале искоришћавањем малолетног лица. Код последњег облика овог кривичног дела, које може бити извршено само према пунолетном лицу (ако је извршено према малолетнику, дело се квалификује према ст. 1 овог члана) изричито се наводи као радња извршења чињење доступним слике, аудио визуелног или другог предмета порнографске садржине настале искоришћавањем малолетног лица електронским путем, што значи, поред осталог, и коришћењем компјутера и интернета. Код овог кривичног дела предвиђено је и одузимање предмета порнографске садржине који се искоришћавају или настану на овакакв начин.

---

[733] Ангажовање грађана од стране МУП-а Србије и Вишег јавног тужилаштва у Београду у акцији "Армагедон", која је покренута 2010. године ради сузбијања дечије порнографије показала се веома успешном. Грађани су давали информације и помагали полицијским органима да се идентификују „интернет предатори". Према подацима из дневне штампе у току 2011. године ухапшено је 23 лица из различитих градова Србије (Београд, Горњи Милановац, Зајечар, Нови Сад, Сомбор, Бор), што је било дупловише него 2010. године. У току 2015. ухапшене су чак 32 особе код којих је пронађена већа колићина материјала са дечијом пороографијом. Међу ухапшеним особама било је разних професија и образовања: свештеници, директори, адвокати, наставници. *Видети:* Србија данас Магазин, www.srbijadanas.com/clanak/akcija-argmagedon-uhapseni-osumnjiceni-za-distribuciju-dečije-pornografije-12-05-2015,
Новости магазин, www.novosti.rs/.../aktuelno291.html., претражено 01. 12. 2015. године

Законом није дефинисано шта се сматра порнографским материјалом, што значи да се ово питање разматра у сваком конкретном случају. Такође треба истаћи да је неопходно код ових кривичних дела водити рачуна о психофизичким својствима деце и малолетника, који се налазе у процесу развоја и сазревања, поготово што се они могу појавити као оштећени, оштећени као сведоци, па чак и као извршиоци ових кривичних дела.[734]

У основном и тежем облику кривичног дела *навођење малолетног лица на присуствовање полним радњама* (чл. 185а ст. 1 навођење малолетника да присуствује силовању, обљуби или са њом изједначеним чином или другој полној радњи; тежи облик чл. 185а ст.2 дело учињено употребом силе, претње или према детету) није изричито предвиђено да кривично дело постоји и у случају „посредног присуства", односно када се путем Интернет конекције оваква радња прикаже малолетнику или детету. Ипак, у чл. 185б ст. 1 КЗ РС наведено је да и ово кривично дело може бити извршено искоришћавањем рачунарске мреже или комуникације другим техничким средствима. Приликом доказивања овог кривичног дела важно је обезбедити доказе о сексуаланим радњама којима је малолетник присуствовао, као и трагове који се могу повезати са његовим праћењем таквог материјала. Због тога је неопходно у току увиђаја прегледати рачунаре и податке садржане у њима.

Кривичним делом *искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл.185б КЗ РС)* санкционисано је коришћење рачунарске мреже или комуникације другим техничким средствима у намери извршења кривичних дела против полне слободе према малолетном лицу или детету договарањем састанка и појављивањем на договореном месту ради састанка. Први облик овог кривичног дела састоји се у коришћењу рачунарске мреже или комуникације другим техничким средствима за договарање састанка и појевљивање на договореном месту ради састанка у намери извршења кривичног дела *силовања* (чл. 178 ст. 4), *обљубе над немоћним лицем* (чл. 180 ст. 1 и 2), *обљубе са дететом* (чл. 180 ст. 1 и 2), *обљубе злоупотребом положаја*

[734] Постоје такви облици криминаних понашања које закон не предвиђа и који се односе на случајеве када су малолетници и жртве и извршиоци код тзв. секстинга. Више о томе видети на стр. 145 овог рада.

(чл. 181 ст. 2 и 3), *недозвољене полне радње* (чл. 182 ст. 1), *подвођење и омогућавање вршења полног односа* (чл. 183 ст. 2), *посредовање у вршењу проституције* (чл. 184 ст. 2), *коришћење малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу* (чл. 185 ст. 2.) и *навођење малолетног лица на присуствовање полним радњама* (чл. 185а). Тежи облик овог кривичог дела постоји када је кривично дело учињено према детету. Висина предвиђене казне зависи од облика извршеног кривичног дела: за основни облик предвиђена је казна затвора од шест месеци до пет година и новчана казна, док је за тежи облик предвиђена казна затвора од једне до осам година.

Друга група кривичних дела која, у складу са Конвенцијом о високотехнолошком криминалу (чл. 10), припадају компјутерском криминалитету односе се на кршење ауторских и њима сличних права и обухватају репродуковање и дистрибуцију неауторизованих примерака дела кроз компјутерске системе. Кривични законик Републике Србије у оквиру Главе XX (*кривична дела против интелектуалне својине*) предвиђа следећа кривична дела: повреда моралних права аутора и интерпретатора (чл.198), неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199), неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (чл. 200), повреда проналазачког права (чл. 201) и неовлашћено коришћење туђег дизајна (чл. 202). Код свих наведених кривичних дела није изричито наведено да могу бити извршена злоупотребом Интернета, електронске технологије и комуникације (осим код кривичног дела из чл. 200, када се неовлашћено уклања или мења електронска информација о ауторском или сродом праву), али из одредби Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала произилази да се овај Закон примењује на кривична дела против интелектуалне својине код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику (чл. 3 Закона). Кривична дела која су највише повезана са коришћењем интернета и друштвених мрежа су повреда моралних права аутора и интерпретатора (чл.198), неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199),

неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (чл. 200).

Повреда моралних права аутора и интерпретатора постоји: (1) када неко лице под својим именом или именом другог лица у целини или делимично објави, стави у промет примерке туђег ауторског дела или интерпретације или на други начин јавно саопшти туђе ауторско дело или интерпретацију; (2) када се без дозволе аутора измени или преради туђе ауторско дело или туђа снимљена интерпретација; (3) када се стави у промет примерак туђег ауторског дела или интерпретације на начин којим се вређа част или углед аутора или извођача. Сви наведени појавни облици овог кривичног дела могу бити извршени коришћењем електронске технологије и комуникације. Многобројни текстови који се објављују на интернету доступни су великом броју корисника, што представља идеалну подлогу за објављивање туђих дела под својим именом и без дозволе аутора. Посебно распрострањен облик су плагијати научних и стручних радова.

Кривично дело *неовлашћено искоришћавање ауторског дела или предмета сродног права,* као и предходно, има неколико појавних облика. Први облик се састоји у неовлашћеном објављивању, снимању, умножавању или на други начин јавном саопштавању у целини или делимично ауторског дела, интерпретације, фонограма, видеограма, емисије, рачунарског програма или базе података. Други облик обухвата стављање у промет или у намери стављања у промет држање неовлашћено умножених или неовлашћено стављених у промет примерака ауторских дела. Трећи облик је тежи јер се наведене радње предузимају у намери прибављања имовинске користи за себе или другог. Посебан, четврти облик овог кривичног дела постоји када дође до производње, увоза, стављања у промет, продаје, давања у закуп, рекламирања у циљу продаје или давања у закуп или држања у комерцијалне сврхе уређаја или средстава чија је основна или претежна намена уклањање, заобилажење или осујећивање технолошких мера намењених спречавању повреда ауторских и сродних права, или коришћење таквих уређаја или средстава у циљу повреде ауторског или сродног права. Овим последњим обликом инкриминисане су припремне радње за извршење свих осталих облика овог кривичног дела. У свим овим случајевима ради се о *пиратерији*, која је појавом модерних информационих

технологија и рачунарских мрежа доживела експанзију тако да данас готово сваки филм, музички албум, компјутерски програм, видео игра, поред легалног има и „пиратско“ издање. Пиратски садржаји се могу преностити и путем друштвених мрежа што значајно доприноси масовности ове појаве. Откривање пиратерије је веома отежано јер извршилац може бити било које лице, било ког узраста и образовања, а пиратске копије се тешко проналазе код извршилаца јер се веома брзо дистрибуирају. Популаран начин размене фајлова који се злоупотребљавају за пиратерију је коришћење програма којима се остварује директна веза између два компјутера ради размене података између корисника. На овај начин се најчешће размењују велики видео фајлови, музичка дела и софтвер. Материјална штета од пиратерије огромна је и за државу (ненаплаћена пореска потраживања) и за појединце (неостварена добит, гашење појединих делатности и сл.), док је извршиоцима пиратерије гарантовано остварење великих прихода. Ради се о веома уносном послу јер приход од продаје пиратских садржаја знатно превазилази износ уложених средстава.

Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима постоји када дође до неовлашћеног уклањања или измене електронске информације о ауторском или сродном праву, или стављању у промет, увозу, извозу, емитовању или на други начин јавном саопштавању ауторског дела или предмета сроднoправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена. Објект овог кривичног дела је електронска информација о правима интелектуалне својине, која представља облик заштите права интелектуалне својине. Доказивање овог кривичног дела је веома комплексно, треба обратити пажњу на средства којима је дело извршено, на постојање одређене заштите ауторског и сродног права у облику електронске информације, на везу између извршиоца са уклањањем информације, као и на чињеницу да се уклањање врши неовлашћено.[735]

Конвенција о високотехнолошком криминалу у чл.7 став 1 препоручује националним законодавствима да предвиде *кривично дело фалсификовања које је у вези са компјутерима***.** Радње извршења овог кривичног дела, према тексту

[735] Прља Драган, Рељановић Марио, Ивановић Звонимир: „Интернет право”, Институт за упоредно право, Београд, 2012, стр. 50

Конвенције, састоје се сваком умишљајно учињеном делу уношења, мењања, брисања или прикривања компјутерских података који могу да доведу до стварања података који су неистинити, а у намери да се они сматрају за аутентичне и истините и да се са њима поступа као да су аутентични. Кривични законик Републике Србије не познаје овако дефинисано кривично дело фалсификовања које је у вези са употребом компјутера и интернета, већ инкриминише: у Глави XXII као *кривична дела против привреде* фалсификовање новца (чл.223), фалсификовање хартија од вредности (чл.224), фалсификовање и злоупотреба платних картица (чл.225), фалсификовање знакова за вредност (чл.226), фалсификовање знакова за обележавање робе, мера и тегова (чл. 245), и у Глави XXXII као *кривична дела против правног саобраћаја* фалсификовање исправе (чл.355) и посебни случајеви фалсификовања исправе (чл.356), фалсификовање службене исправе (чл.357).

У Кривичном законику Републике Србије постоји велики број кривичних дела чије инкриминације треба прилагодити одредбама Конвенције о високотехнолошком криминалу. То се пре свега односи на кривична дела против слобода и права човека и грађанина, части и угледа, човечности и других добара заштићених међународним правом (расна и друга дискриминација, трговина људима), кривична дела против живота и тела (навођење на самоубиство и помагање у самоубиству), која могу бити извршена и у виртуелном простору уз коришћење компјутера, интернета и друштвених мрежа. Позитивно кривично законодавство не садржи одредбе којима би се корисници друштвених мрежа заштитили од узнемиравања, сексуалног узнемиравања, сајбер мобинга, вршњачког злостављања – булинга, лажног представљања, стварања лажног идентитета, интернет превара и сл.

3.2. Законик о кривичном поступку и процесне одредбе о компјутерском криминалитету

Законик о кривичном поступку Републике Србије (у даљем тексту ЗКП) садржи одребе процесноправног карактера које се односе на процесне механизме и овлашћења учесника у кривичном поступку, откривање учинилаца кривичих дела, прикупљање доказа, процесуирање и суђење. ЗКП не садржи посебне одредбе које се односе на прикупљање и обезбеђивање доказа за

кривична дела која припадају компјутерском криминалитету нити дефинише електронски доказ, који има исту вредност као сви други материјални докази. У одредбама које се односе на значење израза у закону (чл. 2) дефинисани су „електронски запис“, „електронска адреса“, „електронски документ“, „електронски потпис“, али није дефинсан електронски доказ, који од компјутерског криминалитета има посебан значај. За разлику од Конвенције о високотехнолошком криминалу која указује на специфичност и значај електронског доказа (информација или податак значајан за истрагу, смештен у рачунару или предат путем рачунара), ЗКП не издваја посебно и не препознаје значај електронског доказа у процесу доказивања кривичних дела компјутерског криминалитета.

Ипак, ЗКП садржи неколико одредби које би могле бити релевантне за остваривање приступа и увида у садржај похрањених рачунарских података. У чл. 152 ст. 3 ЗКП предвиђено је да предмет претресања (претресање стана и других просторија или лица) могу да буду и уређаји за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи. За разлику од претресања стана и других просторија или лица, који се могу извршити у одређеним случајевима и без одлуке суда, за претресање уређаја и опреме то није могућа, те се може закључити да је у сваком случају неопходна судска наредба. То значи да орган поступка када пронађе рачунар са подацима у вези са извршењем кривичног дела компјутерског криминалитета, може само да предузме мере обезбеђења, односно да уз помоћ стручног лица предузима и проналази, обазбеђује или описује трагове, али не и да изврши претресање рачунара док не добије одлуку суда.[736] Друге одредбе ЗКП-а односе се на привремено одузимање предмета (чл. 147). У предмете који се могу привремено одузети и послужити као доказ у кривичном поступку спадају и уређаји за аутоматску обраду података и уређаји и опрема на којој се чувају или се могу чувати електронски записи.[737] Законик није предвидео сходну примену ових правила на рачунарске податке, али, с обзиром на то да се рачунарски подаци сматрају исправом уколико су подобни или одређени да служе као доказ

[736] Видети више: Писарић, Милана: „Претресање рачунара ради проналажења електронских доказа“, Зборник радова Правног факултета у Новом Саду, 1/2015, стр. 233

[737] Кнежевић, Саша: „Кривично процесно право: општи део“, Ниш: Правни факултет, Центар за публикације, Ниш, 2015, стр. 318

чињенице која се утврђује у поступку, они би се такође могли привремено одузети.

ЗКП предвиђа примену посебних доказних радњи (чл. 161)[738] за одређена кривична дела међу којима су и поједина кривична дела компјутерског криминалитета: неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199 КЗ РС), оштећење рачунарских података и програма (чл. 298 ст. 3 КЗ РС), рачунарска саботажа (чл. 299 КЗ РС), рачунарска превара (чл. 301 ст. 3 КЗ РС) и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302 КЗ РС), Према лицу за које постоје основи сумње да је учинило неко од наведених кривична дела или да припрема извршење неког од наведених кривичних дела, може се, на образложени предлог јавног тужиоца, одредити тајни надзор комуникације, уколико се на други начин не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано. Изузетно, ова посебна доказна радња се може одредити и у случају постојања основа сумње да се припрема неко од наведених кривичних дела, а околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност. Тајни надзор и снимање комуникације односи се на комуникацију која се обавља путем телефона или других техничких средстава или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки. Поред услова за одређивање

---

[738] Посебне доказне радње које предвиђа ЗКП (чл. 161 - 187) су: тајни надзор комуникације, тајно праћење и снимање, симуловани послови, рачунарско претраживање података, контролисана испорука, прикривени иследник (само за кривична дела за која је законом одређено да поступа јавно тужилаштво посебне надлежности). Посебне доказне радње се могу одредити према лицу закоје постоје основи сумње да је учинио неко од кривичних дела наведених у чл. 162 ЗКП, а на други начин се не могу прикупити докази за кривично дело или би њихово прикупљање било знатно отежано. Такође, посебне доказне радње се могу изузетно одредити када постоје основи сумње да се припрема неко од наведених кривичних дела уколико околности случаја указују да се на други начин кривично дело не би моло открити, спречити или доказати или би то изазвало несраземерне тешкоће или велику опасност. За најтеже облике компјутерског криминалитета може да буде значајна посебне доказне радња online прикривеног иследника и сајбер патролирање, које се не наводи у ЗКП, али лпке могу значајно да допринесу борби против компутерског криминалитета. *Више о томе видети:* Драговић, Свјетлана, Милијевић, Драгана; Вишњић Дражен: „Мјесто и улога прикривеног истражитеља у спречавању и сузбијању кривичних дјела из области вискотехмолошког криминалитета", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године, стр. 254

тајног надзора комуникације, Законом су одређени начин одређивања (наредба о тајном надзору комуникације – чл. 167), спровођење ове посебне доказне радње (чл.168), проширење тајног надзора комуникације (чл. 169), достављање извештаја и материјала (чл.170).

У чл. 162 ст. 1 наведена су и кривична дела која могу да буду у вези са употребом компјутера и компјутерске технологије: приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетних лица за порнографију (чл. 185 ст. 2 и 3 КЗ), изазивање националне, расне и верске мржње и нетрпељивости (чл. 317 КЗ), трговина људима (чл. 388 КЗ) и кривично дело из чл. 98 ст. 3 до 5. Закона о тајности података[739] У односу на наведена кривична дела такође могу да буду одређене посебне доказне радње под условима предвиђеним ЗКП.

Међу посебним доказним радњама треба поменути рачунарско претраживање података (чл. 178 - 180 ЗКП), када се компјутерска технологија користи у поступку прикупљања доказа. Предвиђено је да суд може под условима предвиђеним ЗКП на образложени предлог јавног тужиоца одредити рачунарско претраживање већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело. Наредбу о спровођењу рачунарског претраживања података извршава полиција, везбедносно-информативна агенција, Војнобезбедносна агенција, царинске, пореске или друге службе или други државни органи, односно правно лице које на основу закона врши јавна овлашћења.

3.3. Закон о организацији и надлежности државних органа за борбу против високотехнолшког криминала

Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала успоставља се организација и одређује надлежност државних органа у борби против високотехнолошког криминалитета. Овим законом је уређено образовање, организација, надлежност

[739] У чл. 98 Закона о тајности података ("Службени гласник РС" бр. 104/2009) предвиђено је кажњавање казном затвора за кривично дело неовлашћеног саопштавања, предаје или чињење доступним података или докумената који су поверени и представљају тајне податке са ознаком „државна тајна" непознатом лицу, затим ако је део учињено из користољубља или ради објављивање или коришћење тајних података или је извршено за време ратног или ванредног стања или је дело учињено из нехата.

и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела високотехнолошког криминала (чл.1). Под високотехнолошким криминалом се подразумева вршење кривичних дела код којих се као објект или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику – рачунарски програми и ауторска дела која се могу употребити у електронском облику (чл. 2).

Закон у чл. 3 прецизира да се његове одредбе примењују ради откривања, кривичног гоњења и суђења за 1) кривична дела против безбедности рачунарских података одређена Кривичним закоником; 2) кривична 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 2000 примерака или настала материјална штета прелази износ од 1.000.000 динара; и за 3) кривична 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 кривичним делима високотехнолошког криминала.

За поступање по кривичним делима вискотехнолошког криминалитета надлежно је Више јавно тужилаштво у Београду за територију Републике Србије. *Посебно одељење за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду* („Посебно тужилаштво"),[740] док је у Вишем суду у Београду формирано *Веће за борбу против високотехнолошког криминала*, а у оквиру Министарства унутрашњих послова основана је посебна служба ради обављања послова органа унутрашњих послова у вези са кривичним делима високотехнолошког криминалитета.[741] Наведени органи

[740] Посебно тужилаштво је основано је 20. фебруара 2007. године као посебно одељење Окружног јавног тужилаштва у Београду. Посебног тужиоца поставља републички јавни тужилац.. Предност при постављењу иамју они тужиоци, односно заменици, који поседују посебна знања из области информатичких и радиодифузних технологија.

[741] Служба за борбу против високотехнолошког криминала („Служба") је специјализована полицијска служба која је формирана као Одељење за за борбу против високотехнолошког

имају територијалну надлежност на целој територији Републике Србије. Оваквим законским решењем успостављен је адекватан правно институционални оквир за поступање правосудних и полицијских органа у овој области, који пружа добар основ за успешну борбу против високотехнолошког криминалитета. Пре измена Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, до којих је дошло 2009. године, био је споран начин формулисања стварне надлежности поменутих органа.[742] Због тога је предложено проширивање стварне надлежности ових органа за сва кривична дела која по начину, средствима и објекту извршења представљају дела из области високотехнолошког криминалитета.[743] Измене закона на основу којих је дошло до проширивања стварне надлежности и на кривична дела против привреде, слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије према Закону о изменама и допунама Закона о надлежности државних органа за борбу против високотехнолошког криминалитета ступиле су на снагу 01. 01. 2010. године.

При Окружном суду у Београду образовано је Веће за борбу против високотехнолошког криминала, кога чине судије овог суда које поседују

криминала. Међу кривичним пријавама које је у току 2008. и 2009. године ово Одељење поднело Посебном тужилаштву за кривична дела високотехнолошког криминала по бројности се издвајају кривичне пријаве поднете због крађу идентитета и злоупотребу налога на друштвеним мрежама, а посебно на друштвеној мрежи Facebook – *видети више о овоме код* Урошевић, Владимир, Уљанов, Сергеј, Вуковић, Радоје: „Полиција и високотехнилошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије“, Министарство унутрашњих послова Републике Србије, http://www.singipedia.singidunum.ac.rs/attachment.php?attachmentid=1042&d=1278689423, претражено 12. 10. 2015.године.
У току 2011.године пред овим тужилаштвом покренути су кривични поступци против 46 особа због пиратских радио и телевизијских станица, против 39 особа због малолетничке порнографије, против 21 особе за угрожавање сигурности колико је покренуто и за рачунарске преваре, а против 11 особа за бављење нелегалним копирањем филмова и музике. *Видети:* Sajber kriminal u porastu, http://www.novimagazin.rs/vesti/sajber-kriminal-u-porastu/ , претражено 10. 02. 2014. године

[742] У чл. 3 Закона наведена су кривична дела за које је установљена надлежност посебних органа. Међутим,овако формулисана стварна надлежност не обухвата сва кривична дела која припадају компјутерском криминалитету. Тако, на пример, нису обухваћена следећа кривична дела.: приказивање, прибављање, и поседовање порнографског материјала, и искоришћавање малолетног лица за порнографију – чл..185 КЗ РС и кривично дело фалсификовање и злоупотреба платних картица – чл. 225 КЗ. *Цит према* Бејатовић, Станко, *op.cit.* , стр. 24

[743] Николић Комлен, Лидија и др. *op cit.*, стр. 278

посебна знања из области информатичких технологија.[744] У Министарству унутрашњх послова формиран је Одсек за сузбијање компјутерског криминала у оквиру Службе за борбу против организованог криминала Управе криминалистичке полиције (СБПОК).

Одељење за борбу против високотехнолошког криминала сарађује са другим организационим целинама Службе за сузбијање организованог криминала, посебно а Одсеком за прикупљање и обраду дигиталних доказа у оквиру Службе за специјалне истражне методе, као и са осталим организационим јединицама Дирекције полиције и појединим службама безбедности републике Србије (БИА, ВБА). Сагласно Конвенцији о високотехнолошком криминалу, сарадња је успостављена и са службама у иностранству у чијој је надлежности откривање, праћење и пресецање делатности организација и појединаца који врше кривична дела компјутерског криминалитета. С обзиром на то да компјутерски криминалитет има транснационални карактер, сарадња је успостављена и са Националним централним бироом Интерпола Београд.

Поред наведених посебних организационих јединица у државним органима, значајну улогу у овој област имају Министарство трговине, туризма и комуникацијама,[745] Републичка агенција за електронске комуникације (РАТЕЛ) и Републичка радиодифузна агенција (РРА).[746]

3.4. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима

Законом о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима (тзв. „Маријин закон") прописане су посебне мере које се спроводе према учиниоцима кривичних дела против полне слободе извршених према малолетним лицима одређених законом

---

[744] Приликом постављања судија предност имају судије које имају искуства у борби против високотехнолошког криминалитета и они који су укључени у тзв. РАСО програм (Пројекат за борбу против економског криминала у Републици Србији).

[745] Министарство трговина, туризма и телекомуникација обавља, поред осталог, државне послове који се односе на област телекомуникација и информатичког друштва, који се односе на предлагање политике и стратегија развоја информационог друштва, припрему закона, других прописа, стандарда и мера у области електронског пословања, развоја и примене информационо комуникационих технологија, заштиту података и информациону безбедност, међународне послове у области информационог друштва и сл. *Наведено према* Закону о министарствима „Службени гласник Републике Србије бр. 44/2014, 14/2005 и 52/2015.

[746] Регулаторна агенција за електронске комуникације и поштанске услуге, www.ratel.rs, претражено 25. 08. 2015. године и Регулаторно тело за електронске медије, http://www.rra.org.rs/cirilica, претражено 25. 08. 2015. године

и уређује вођење посебне евиденције лица осуђених за та кривична дела. Сврха закона је спречавање сексуалне делинквенције према малолетним лицима. Подручје примене закона обухвата тачно одређена кривична дела извршена према малолетним лицима, међу којима су кривична дела компјутерског криминалитета и то приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185 КЗ) и искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл. 185б КЗ). Посебне мере предвиђене законом примењују се према учиниоцу наведених кривичних дела после издржане казне затвора и оне се састоје у обавезном јављању надлежном органу полиције и Управе за извршење кривичних санкција; забрани посећивања места на којима се окупљају малолетна лица (вртићи, школе и сл.); обавезном посећивању професионалних саветовалишта и установа; обавезном обавештавању о промени пребивалишта, боравишта или радног места; обавезном обавештавању о путу у иностранство. Посебно је важна одредба чл. 5 ст. 3 Закона којом је предвиђено да кривично гоњење и извршење казне не застаревају за кривична дела против полне слободе извршена према малолетним лицима. На основу наведених одредби, као и одредби Кривичног законика, може се закључити да су у нашем законодавству усвојене законодавне и друге мере предвиђене у чл. 9 Конвенције о високотехнолошком криминалу у погледу кривичних дела у вези са дечијом порнографијом.

3.5. Закон о ауторским и сродним правима

Закон о ауторским и сродним правима садржи казнене одредбе којима се одређује прекршајна одговорност и одговорност за привредне преступе у вези са ауторским правима, као и грађанско-правне односе у области права интелектуалне својине. У чл. 2 Закона се одређује шта се сматра ауторским делом и као ауторко дело се, у оквиру писаних дела, одређују рачунарски програми у било којем облику његовог изражавања, укључујући и припремни материјал за њихову израду. У Закону су установљени основни елементи општег режима заштите ауторских дела од недозвољеног емитовања, који се односе и на писана дела, односно рачунарске програме (чл. 28 - 30). Такође,

Закон је аутору дао право да другоме забрани или дозволи да његовоо дело, које је забележено на носачу звука, односо носачу слике (компакт диск, аудио касета, видео касета, филмска трака, оптички диск, дијапозитив) јавно саопштава уз помоћ техничких уређаја за репродуковање звука односно слике (чл. 33). Иако није изричито наведено, свакако да се ово право аутора односи и на електронско емитовање.

У Закону не постоје посебне одредбе које се односе само на рачунарске програме, осим што је у чл. 47 предвиђено да лице које је на законити начин прибавило примерак рачунарског програма, може, ради сопственог уобичајеног наменског коришћења програма, без дозволе аутора и без плаћања ауторске накнаде, поред осталог да: смешта програм у меморију рачунара и пушта програм у рад; отклања грешке у програму, као и да врши друге неопходне измене у њему које су у складу са његовом сврхом, ако уговором није друкчије предвиђено; начини један разервни примерак програма на трајном телесном носачу и изврши декомпилацију програма искључиво ради прибављања неопходних података за постизање интероперабилности тог програма са другим независно створеним програмом или одређеном рачунарском опремом, под условом да тај податак није био на други начин доступан и да је декомпилација ограничена само на онај део програма који је неопходан за постизање интероперабилности. Уколико је податак добијен последњом описаном радњом постоји забрана да се тај податак саопштава другоме или користи за друге сврхе, посебно за пласман другог рачунарског програма којим би се повредило ауторско право на првом.

У оквиру казнених одредби (чл. 215) Закон, поред осталог, предвиђа кажњавање привредног друштва или другог правног лица новчаном казном за привредни преступ уколико произведе, увезе, стави у промет, прода, да у закуп, рекламира у циљу продаје или давања у закуп или држи у комерцијалне сврхе уређаје, производе, саставне делове, рачунарске програме, који су превасходно конструисани, произведени или прилагођени да омогуће или олакшају заобилажење било које ефикасне технолошке мере, или који немају другу значајнију сврху осим наведене.

3.6. Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине

Законом о посебним овлашћењима ради ефикасне заштите права интелектуалне својине се уређују посебна овлашћења органа државне управе и организација које врше јавна овлашћења ради ефикасне заштите права интелектуалне својине у складу са прописима којима се уређује право интелектуалне својине (чл. 1). Закон предвиђа да је роба којом се повређују права интелектуалне својине, поред осталог, нарочито пиратски примерак ауторског дела или предмета сродног права, укључујући и рачунарске програме, који се дефинише као примерак заштићеног ауторског дела или предмета сродног права, односно роба која садржи ауторско дело или предмет сродног права, која је израђена без сагласности носиоца права.

Казненим одредбама (чл. 39 и чл. 40) утврђена је прекршајна одговорност и одговорност за привредне преступе правног лица и одговорног лица за неовлашћену производњу, увоз, извоз, нуђење ради стављања у промет, складиштење или коришћење у комерцијалне сврхе производа или поступка заштићеног патентом. Такође је одређено да ће се предмети извршења привредног преступа и предмета употребљених за извршење привредног преступа бити одузети, а предмети извршења привредног преступа уништени.

3.7. Закон о електронском потпису

У Закону о електронском потпису електронски документ се дефинише као документ у електронском облику који се користи у правним пословима и другим правним радњама, као и у управном, судском и другом поступку пред државним органом (чл. 2 ст. 1 тач. 1), а електронски потпис као скуп података у електронском облику који су придружени или су логички повезани са електронским документом и који служе за идентификацију потписника (чл. 2 ст.1 тачка 2). На овај начин, изједначено је правно важење докумената у папирном и у електронском облику који се користе свим правним пословима и правним радњама. Томе иде у прилог и одредба да се електронска документа која су електронски потписана морају чувати онолико времена колико се чувају сами документи. Електронском документу се не може оспоравати пуноважностили доказна снага само зато што је у електронском облику, осим у

случајевима када закон захтева својеручан потпис. Закон садржи казнене одредбе којима се утврђује кажњавање за прекршај новчаном казном корисника - правног лица/предузетника/одговорног лица у правном лицу, државног органа, органа територијалне аутономије, органа локалне самоуправе, физичког лица и сертификационог тела за низ радњи, као што су, поред осталог: нечување од неовлашћеог приступа средстава и података за формирање електронског потписа; употреба и коришћење супротно одредбама закона, недостављање сертификационом телу потребних података и информација о променама које утичу или могу утицати на тачност утврђивања идентитета потписника итд.

3.8. Закон о електронској трговини

Законом о електронској трговини уређују се услови и начин пружања услуга информационог друштва, обевезе информисања корисника услуга, комерцијална порука, правила у вези са закључењем уговора у електронском облику, одговорност пружаоца услуга информационог друштва, надзор и прекршаји. У закону су дефинисани поједини изрази, као што су: услуга информационог друштва, пружалац услуге информационог друштва, корисник услуге, потрошач, уговор у електронском облику, комерцијална порука. Овим законом је створен правни основ за изједначавање електронских облика пословања са класичним непосредним облицима јер се уводи уговор у електронском облику, чији су садржина и форма идентични уговорима закљученим у писаној форми. Уговор у електронском облику се разликује од уговора закључених у писаној форми по начину закључења, овај уговор се закључује искључиво коришћењем средстава електронске комуникације.

Закон о електронској трговини садржи казнене одредбе. До кажњавања новчаном казном за прекршај физичког лица или одговорног лица у правном лицу, предузетика или пружаоца услуга може да дође уколико: не пруже прописане информације надлежним државним органима; пошаљу нетражену комерцијалну поруку без претходног пристанка лица коме је таква порука била намењена; потенцијалном кориснику услуга, пре закључења уговора, не обезбеди на разумљив и недвосмислен начин прописане податке и обавештења; не обавести надлежни државни орган о недопуштеним активностима или подацима корисника његове услуге или не предочи све податке, сагласно

одговарајућем судском, односно управаном акту и уколико не омогући приступ рачунарској опреми и уређајима и ако без одлагања не покаже или не достави потребне податке или документа ради вршења надзора.

3.9. Закон о електронском документу

Закон о електронском документу дефинише процедуру поступања са електронским документом, пријем таквог документа, издавање потврде о пријему, као и начин чувања дупликата. Према тексту Закона, електронски документ је скуп података састављен од слова, бројева, симбола, графичких, звучних и видео записа садржаних у поднеску, писмену, решењу, исправи или било ком другом акту који сачине правна и физичка лица или органи власти ради коришћења у правном промету или у управном, судском или другом поступку пред органима власти, ако је електронски израђен, дигитализован, послат, примљен, сачуван или архивиран на електронском, магнетном, оптичком или другом медију (чл. 2).

У правном промету класична и електронска форма имају исту важност, ипак, у Закону су наведени правни послови када се не може употребити електронски документ (чл. 4 Закона: пренос права својине на непокретности, уговори из области наследног права, уговори о утврђивању имовинских односа између брачних другова, уговори о располагању имовином лица којима је одузета пословна способност, уговори о поклону, други правни послови или радње за које је посебним законом или на основу закона донетих прописа, изричито одређена употреба својеручног потписа у документима на папиру или овера својеручног потписа).

У Закону о електронском документу садржане су и одредбе о временском жигу који представља званично време придружено електронском документу, којим се потврђује садржај електронског документа у то време, односно садржај сваког документа у групи. У Закону је садржана казнена одредба, којом је предвиђено кажњавање новчаном казном за прекршај издаваоца временског жига уколико се пре почетка обављања послова издавања временског жига не региструје; ако формира временски жиг који не садржи писане податке; уколико не чува на безбедан начин и у прописаном року податке о издатим временским жиговима и уколико не омогући инспектору за

електронски потпис приступ у пословне просторије и увид у податке о пословању и пословну документацију, као и приступ систему за формирање временског жига, рачунарској опреми и уређајима (чл. 23).

3.10. Закон о оптичким дисковима

Законом о оптичким дисковима уређују се услови за производњу оптичких дискова и производних делова, увоз и извоз производних делова и опреме, која се користи за производњу оптичких дискова, као и комерцијално умножавање, увоз, извоз и промет оптичких дискова. У оквиру казнених одредби одређено је кажњавање за прекршај новчаном казном правног лица, предузетника, физичког лица или одговорног лица у правном лицу, које производи, складишти, ставља у промет, увози и/или извози оптичке дискове, односно производне дискове (стампер) супротно одредбама Закона о оптичким дисковима или не поштује обавезе обележавања, чувања и вођења евиденције прописане законом.

ГЛАВА IV

ПРЕВЕНЦИЈА И МЕРЕ ЗАШТИТЕ ОД КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

1. Стратешке концепције, стратешка опредељења и препоруке

Супротстављање компјутерском криминалитету обухвата два механизма: превентивно и репресивно деловање, одвраћање од злоупотребе компјутера и стварање услова за брзо откривање и доказивање у случајевима када је злоупотреба извршена. Превентивне мере се односе на установљавање стратегија заштите информационих система и њихову имплементацију, као и унапређивање законске регулативе на глобалном и националном нивоу. На глобалном плану ОУН се активно укључује у превентивно деловање кроз рад својих специјализованих тела и радних група, као што су на пример Међународна телекомуникациона унија (International Telecommunication Union – ITU), Канцеларија УН за контролу наркотика и превенцију криминала (United Nations Office on Drugs and Crime – UNDOC) и Канцеларија УН за послове разоружања (Office for Disarmament Affairs – UNODA). Проучавање превенције високотехнолошког криминалитета у оквиру различитих нивоа безбедности спада у делокруг рада НАТО организације (North Atlatnic Treaty Organization), пре свега Комитета науке за мир и безбедност (The Science for Peace and Security Committee) и Техничког Центра за брзе реакције на компјутерске инциденте (NATO Computer Incident Response Capability-Technical Centre).[747]

Значајан допринос глобалним напорима за стратешко супротстављање компјутерском криминалитету дају регионалне међувладине организације, као што је Организација за европску безбедност и сарадњу – ОЕБС (Organization for Security and Co-operation in Europe –OSCE), у оквиру које је оформљена Радна група за безбедност информација и приватност. Треба поменути и друге

[747] Бошковић, Горан, Ивановић, Звонимир: „Стратешке концепције у супротстављању високотехнолошком криминалу", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 80 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године

европске институције које својим радом значајно доприносе превентивном деловању и супротстављању компјутерском криминалитету, од којих су најзначајније: Европски институт телекомуникационих стандарда (European Telecommunications Standards Institute – ETSI), Европски комитет за стандардизацију (European Committee for Standardization – CEN), Одбор за информационе и комуникационе стандарде (Information and Communications Technologies Standards Board – ICTSB). Координацију сузбијања безбедносних претњи од стране компјутерског криминалитета врше Европске јединице тимова за брзе реакције на компјутерске инциденте (European Task Force on on Comuter Security Incident Response Teams - TF-CSIRT) и Еурополов Центар за високотехнолошки криминал.[748]

За изградњу превентивног система заштите од компјутерског криминалитета посебно су важне Препорука Савета министара Европског савета[749], које се односе се на: побољшање техничких могућности за аутентификацију корисника података; побољшање техничких могућности праћења комуникација преко интернета и посебно на друштвеним мрежама, како би се заштитила приватност корисника и спречило непотребно и неовлашћено прикупљање личних података о корисницима; побољшање мера заштите од злоупотребе анонимности на интернету, на пример. увођење цертификата који би у одређеним случајевима злоупотребе могли да открију име и локацију са које одређени корисник који се крије иза своје анонимности чини неко кривично или противправно дело; побољшање технологија којима би се заштитиле новчане трансакције преко интернета као и ауторска права.

У Препорукама Савета министара Европског савета наводи се да је компјутерско образовање и основно упознавање са информационим технологијама неопходно како би се: законодавци упозорили у којим је то областима неопходно проширити прописивање кажњивих дела како би се утицало на превенцију злоупотребе рачунара, интернета и друштвених мрежа; подигла свест корисника да Интернет треба искључиво да служи као медиј за

[748] Ibid.
[749] Recommendations to the European Council Europe and the global information society, http://channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, претражено 04.12.2014.године

едукацију и учење а не као место на коме ће се вршити различита кривична дела; створила средина која погодује лаком и доступном коришћењу интернета поготово када је реч о најмлађим генерацијама корисника, како би они у току свог школовања могли да на наднационалном нивоу размењују своја знања и искуства; едуковали корисници о правима и обавезама које имају приликом коришћења виртуелних комуникационих мрежа (нпр. коришћењу програма за филтрирање, правилима понашања у циљу заштите личних података, начину зашптите права интелектуалне својине на интернету и сл.); едуковали корисници које све потенцијалне опасности вребају на друштвеним мрежама, које су друштвене мреже „опасне“, које треба избегавати, као и како заштитити личне податке приликом комуникације на друштвеним мрежама.

Препоруке су такође усмерене на индустрију која се бави информационим и комуникационим технологијама, којој се саветује да: повећа степен сигурности корисника на свим интернет локацијама и друштвеним мрежама, као и саму сигурност рачунарских система; саветује кориснике и интернет провајдере како да безбедно користе рачунарске системе и информационе технологије и процедуре; побољша сарадњу са владиним агенцијама и званичним телима која се баве информационим технологијама и питању безбедности података на њима; утврде правила понашања на тај начин што би се прописало који садржај се сматра противправним и који је као такав санкционисан; створи међународну мрежу контаката на којој би стално на располагању као упозорење била база противправних садржаја и њихових аутора, како би корисници знали да са њима не ступају у контакте а интернет провајдери да им, у складу са законом, онемогуће приступ интернету и друштвеним мрежама; у сарадњи са специјалним одељењима у полицији и са тужилаштвима створи протоколе и процедуре, ради проналажења извршилаца и откривања кривичних дела компјутерског криминалитета.

У Препорукама Савета министара Европског савета предлаже се и предузимање одређених правних мера превенције и заштите од компјутерског криминалитета, које се односе на измене правних регулатива на међународном нивоу. Стварање међународног правног оквира је веома битно како би се спречило вршење кривичних дела компјутерског криминалитета, открили и процесуирали извршиоци ових кривичних дела и како би се створили механизми помоћу којих би се жртвама ових дела надокнадила претрпљена

штета. Такође се предвиђа јачање међународноправних механизама за борбу против кривичних дела компјутерског криминалитета, стварање листе минималних правила и процедура које свака земља мора да примењује (нпр. за дела попут упада у рачунаре и рачунарске системе, компјутерску шпијунажу, компјутерску превару, повреде ауторских права и сл.) и процесуирање и санкционисање објављивања противправних и незаконитих садржаја на интернету, нпр. дечија порнографија, дискриминаторско понашање, глорификција насиља и аката насиља, говор мржње и сл.

Препоруке се такође односе на формирање одговарајућих правних механизама којима би се дефинисала одговорност интернет провајдера за садржаје који се објављују а имају неадекватан или незаконит садржај; доношење адекватних националних закона којима би се обезбедили кривично-процесни механизми за ефикасно процесуирање извршилаца кривичних дела која припадају компјутерском криминалитету. У свакој земљи треба да се створе одговарајући механизми заштите од могуће злоупотребе анонимности у виртуелном простору, како би се у случајевима злоупотребе или извршења кривичног дела, открио идентитет извршиоца, уз обавезну правну заштиту корисниковог права на приватност (нпр. захтевати судски налог за откривање одређених електронских података и њихово прослеђивање органима надлежним за процесуирање). Уколико се ради о међународним случајевима извршења кривичних дела компјутерског криминалитета или неодговарајућих понашања на Интернету, потребно је: побољшати механизме међународне правне помоћи, подстицати јачање сарадње између полиција различитих држава, како би се првенствено обезбедило правовремено и хитно обезбеђење и чување електронских података који служе као докази постојања кривичног дела; детаљно уредити питања надлежности за кривична дела са елементом иностраности и за кривична дела која су учињена на територијама више држава; едуковати полицијске тимове шта је то компјутерски криминалитет, који су његови појавни облици и начин гоњења учинилаца ових кривичних дела.

У оквиру међународних стандарда треба поменути ISO/IEC 2700 серије стандарда и њихову имплементацију у информациони систем. Сврха ових стандарда је да пруже помоћ организацијама свих врста и величина да развију и примене систем управљања безбедношћу сопствених инфомација и да се

припреме за независно и непристрасно оцењивање (сертификацију) тог система примењеног на заштиту информација.[750]

Поред законских и институционалних мера које треба да створе успешан механизам заштите од компјутерског криминалитета, у Србији је донета Стратегија развоја информационог друштва у Републици Србији до 2020. године[751], која као једну од области приоритета одређује информациону безбедност, а посебно унапређење правног и институционалног оквира за информациону безбедност, заштиту критичне инфраструктуре, борбу против високотехнолошког криминала и научно-истраживачки и развојни рад у области информационе безбедности. Поред тога што Стратегија предвиђа да ће до 2020. године бити уређени сви аспекти информационе безбедности и формирани одговарајући институционални оквири, један од циљева је да се развојем информационе безбедности створи поверење корисника у безбедно функционисање информационих система, поверење грађана у заштићеност података о личности у информационим системима, ширење свести о неопходности спровођења мера информационе безбедности, заштита података, информационих и телекомуникационих система, безбедност електронских трансакција и да се створе ефикасни механизми заштите и остваривање права у процесима електронског пословања и електронске размене података.

Стратегија такође предвиђа доношење одговарајућих прописа из области информационе безбедности, којима ће се додатно уредити стандарди информационе безбедности, подручја информационе безбедности, као и надлежности и задаци појединих институција у овој области, као и формирање институције која ће у области информационе безбедности обављати послове верификације и сертификације метода, софтверских апликација, уређаја и система, истраживања и развоја и надзирати примену стандарда информационе безбедности у државним органима.

---

[750] Више о томе видети код Поповић, Драган, Вучановић, Драган, Лазаревић, Ристо: "Имплементација стандарда серије ISO/IEC 27000 као мјера сузбијања високотехнолошког криминала", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 159, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године

[751] Стратегија развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС" бр. 51/2010)

Основ борбе против високотехнолошког криминалитета, према тексту Стратегије су одредбе Кривичног законика Републике Србије, Закона о кривичном поступку, Закона о организацији и надлежности органа за борбу против високотехнолошког криминала и Закону о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, као и формирање посебног Одељења за борбу против високотехнолошког криминала при вишем јавном тужилаштву у Београду и Службе за борбу против високотехнолошког криминала у оквиру Министарства унутрашњих послова.

2. Заштита информационих система и заштита приватности на друштвеним мрежама

Заштита информационих система представља примарни, базични ниво заштите и односи се на заштиту информационих система, информација и информационих мрежа у приватном власништву грађана и у битним државним и приватним организацијама.[752] Заштитне мере је неопходно спроводити на више нивоа, међу којима су најзначајнији: *оперативни ниво* (примена најсавремнијих средстава за заштиту података, ћеста тестирања ових система и отклањање уочених безбедносних проблема), *производни ниво* (контрола произвођача информатичких средстава, тестирања хардвера и софтвера информационих система на безбедносне пропусте), *државни ниво* (физички, технички, организациони, кадровски, нормативни). Ипак, у свком случају, први корак у заштити информационих система је постављање физичке и софтверске заштите. Физичким мерама се мора осигурати заштита од случајних оштећења опреме (непосредним путем или путем телефонске линије) и неовлашћене уградње делова опреме или програма. Софтверска заштита подразумева предузимање мера заштите оперативног система, спречавање неовлашћеног улажења у поједине корисничке програме (лозинке, кључне речи), регисторвање

[752] Путник, Ненад: „Сајбер простор и безбедносни изазови“, Факултет безбедности, Београд, 2009, стр. 334, цит према Путник, Ненад, Гаврић, Невена: “Мере и стратегије заштите информациониг+х система од високотехнолошког криминала”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 218 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године

свих активности у компјутеру и шифрирање података који се преносе од једног до другог корисника у систему.[753]

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.

Повреде приватности је веома тешко доказати а извршиоце је готово немогуће открити. Неки од проблема доказивања повреде приватности корисника друштвених мрежа су:

- трагови који остају су специфични, а огледају се у променама електронских записа који су настали у софтверском делу рачунара,
- анонимност извршиоца кривичног дела и тешко проналажење трагова које иза себе оставља,
- проналажење трагова најчешће и само представља неовлашћено продирање у туђе компјутерске системе и базе података,
- ИП адреса није увек поуздано средство за праћење извршиоца дела, зато што и њоме може да се манипулише,
- откривање, тумачење и доказно коришћење промена насталих у софтверу захтева изузетну стручност и ангажовање компјутерских експерата високог нивоа,
- различито место и време деловања извршиоца кривичних дела.

Да би се смањио број злоупотреба на друштвеним мрежама и угрожавање права на приватност корисника друштвених мрежа, 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

[753] Компутерски криминал/ИПФ-радна база, http://promocije.net/proba/krivicno-pravo/materijalno-krivicno-pravo/kompjuterski-kriminal/, претражено 19.02.2016. године

криминалитета“ и остварило боље превентивно деловање, препознавање и праћење оваквих дела као и превазилажење проблема непријављивања ових кривичних дела. Што пре би требало да се уједначе и унификују дефиниције појединих облика злоупотребе друштвених мрежа, да се аналитички прате поједини случајеви и да се јавност упознаје са могућим начинима злоупотребе. На појединачном плану кориснике друштвених мрежа треба упознати са могућим ризицима и начинима за избегавање виктимизације. У том смислу, у литератури постоје неки општи савети за заштиту корисника од могућих злоупотреба и интернет насиља. [754]

Већина корисника друштвених мрежа прави основну грешку јер не чита политику приватности пре него што се придружи одређеној друштвеној мрежи. Политика приватности обично садржи објашњења на који начин друштвена мрежа сакупља податке о својим корисницима и како их и за шта касније користи.

Свако од корисника интернета, а посебно корисника друштвених мрежа, може да допринесе борби против компјутерског криминалитета тако што ће и сам ***поштовати одређена правила понашања у виртуелном свету интернета***. Пре свега, значајан је избор људи са којима се ступа у контакт, избор сајтова, линкова и интернет страница са којих стижу поруке са друштвених мрежа. Сајтови треба да буду изабрани са посебном пажњом уз претходно прикупљање информација о њима. Друштвене мреже није пожељно користити на радном месту јер увек постоји могућност да више корисника користи један рачунар и да може доћи до злоупотребе налога. Коко не би дошло до уношења вируса, потребно је обавезно проверити скенирањем антивирусним програмом, који мора да увек буде ажуриран.

Ризично је за лозинку постављати датум рођења, име града, надимак, иницијале корисника и сл. јер се ови подаци лако сазнају и могу да се искористе за крађу идентитета, компјутерске преваре и друге злоупотребе. Такође, лозинке за електронске налоге никада не треба чувати аутоматски у пољима за унос. Уколико постоји било каква сумња о томе ко је послао поруку, треба свакако проверити ко је то учинио ступањем у контакт са познатим корисницима.

[754] Microsoft Safety & Security Center, http://www.microsoft.com/security/online-privacy/social-networking.aspx, претражено 17.08.2013. године

„Пријатељи“ на друштвеној мрежи треба да буду пажљиво изабрани јер „крадљивци идентитета“ могу да отварају лажне профиле и да се лажно представљају како би на тај начин лакше приступили туђим личним подацима и информацијама.

Заштита приватности се може остварити пажљивим избором друштвене мреже којој ће корисник приступити. Због тога је неопходно да се пажљиво прочита какву „политику приватности“ (енгл. Privacy policy) има друштвена мрежа, да ли администратори друштвене мреже контролишу информације које се објављују и да ли постоји могућност блокирања неприкладног садржаја.

Посебну пажњу треба посветити избору података који ће се наћи на интернету. Корисник друштвене мреже треба да зна да је сваки податак који објави на друштвеној мрежи доступан свима и остаје трајно забележен. Чак и уколико одлучи да обрише кориснички налог и уништи информације које су објављене, корисник не може да буде сигуран да неко већ није одштампао податке или фотографије. Најбоље је у циљу заштите приватности никако не објављују превише лични подаци и фотографије које се могу показати само најближим пријатељима. Посебно је важно да се на интернету не остављају фотографије деце. За родитеље је веома важно да разговарају са децом о опасностима са друштвених мрежа и да деци помогну да на сигуран начин приступају друштвеној мрежи.

Једна од опасности друштвених мрежа је свакако и анонимност иза које корисници могу да се сакрију јер увек постоји дилема ко се заправо крије иза одређеног профила и имена. Због тога је веома битно научити како да се препознају људи који се у виртуелном простору лажно представљају, тј. како препознати да ли је нечији профил на друштвеној мрежи прави или лажан. Поглед на „зид” (енгл. Wall, Timeline) корисника доста говори о томе да ли је профил заиста прави: уобичајено је да се на „зиду” налазе различита размишљања, слике са пријатељима, коментари које пријатељи остављају или у њима учествују, постови у којима се корисник помиње. Уколико на зиду неког корисника ничега од наведеног нема, постоји могућност да тај корисник није онај за кога се представља.

У случају било каквог облика злостављања преко друштвене мреже или интернета, не треба одговарати на насилне, претеће или било које друге сумњиве поруке и позиве; не треба брисати поруке или слике јер могу

послужити као доказ; а пожељно је да се обавести полиција ако поруке садрже претње насиљем, ухођење, напастовање, дечију порнографију или ако све већ предузете мере нису дале резултате. Уколико је извршилац дела особа чији је идентитет или електронска адреса позната кориснику друштвене мреже, о делу које је извршено треба обавестити полицију, мобилне операторе и Интернет провајдера.

На друштвеним мрежама (форуму или ћаскању) постоји опција „Ignore" или „Block" којом је могуће спречити поруке одређених корисника. То је такође могуће контактирањем администратора мреже,[755] који ће онемогућити долазак порука одређених корисника од којих су пре долазиле неугодне или насилне поруке. Администратори и модератори друштвених мрежа (форума или ћаскања) читају све теме и дискусије и пазе да не буде вређања, претњи, објављивања приватних података и кршења права корисника. Администратор ће избрисати такав запис, упозорити корисника или му забранити даљи приступ ако се то понови.

Такође, постоје препоруке да треба раздвојити приватне и пословне (службене) корисничке профиле. Пословни профили морају да буду прављени на тај начин да привуку пословне контакте да их виде, а не свакога ко може да злоупотреби податак који је нашао на профилу.

Уколико корисник на интернету пронађе неистините податке о себи, мора да брзо реагује. Уколико корисник види да су објављени подаци који могу да му наруше послови или лични углед, мора одмах да на одговарајући начин замоли особу која јке податак објавила да га уклони са интернета или да исправи грешку која је начињена. Уколико онај ко је податак објавио не жели да склони или исправи објављене податке, корисник увек може да се обрати администратору интернет странице или друштвене мреже да уклони нетачне податке.

Корисници интернета који желе да приступе некој друштвеној мрежи треба пажљиво да размисле која би то друштвена мрежа била, јер постоје друштвене мреже различитих садржаја за повезивање корисника различитих интересовања. Такође, неопходно је пре приступања друштвеној мрежи

[755] Лице које мрежу одржава и које води рачуна о заштити права корисника, прим.аут.

прочитати какву политику приватности друштвена мрежа нуди, да ли администратори друштвене мреже надгледају све информације које корисници објављују и да ли постоји могућност блокирања неприкладног и увредљивог садржаја.

Уколико узмемо у обзир шта приватност представља и колико је исправно нечије приватне податке и информације делити са другима, намеће се питање: на који начин популарне друштвене мреже морају да поштују императив морално одговорном понашања а на који начин сами корисници морају да воде рачуна о заштити своје приватности. Најлакши начин за спречавање злоупотребе личних података је утицање на саме кориснике да ограниче право приступа својим подацима, док би основни принцип друштвених мрежа морао да буде посвећен борби против неовлашћеног преузимања личних података корисника.

Корисници друштвених мрежа могу извршити једноставну проверу како би били сигурни да се нигде не манипулише њиховим подацима или да се ти подаци не злоупотребљавају. Посетом страници Google (www.google.com) и уписивањем свог имена и презимена у поље претраживања, Google ће пронаћи све интернет странице на којима се тражено име спомиње, а исти тест може да се направи и уношењем броја телефона, е-маил адресе или корисничког имена на друштвеној мрежи. Google такође даје могућност да се направи и „Google Alert" - аларм који ће кориснику послати информацију на е-маил сваки пут када се на интернету помене његово име или неки од личних података.

Увођењем у Кривични законик Републике Србије кривичних дела против безбедности рачунарских података, свакако је постигнут напредак у репресивним мерама за сузбијање компјутерског криминалитета. Ипак, предвиђањем ових кривичних дела није покривена цела област злоупотребе рачунарских технологија и рачунарских система, поготово нису сагледане злоупотребе које се дешавају коришћењем друштвених мрежа. Успешна превенција злоупотребе друштвених мрежа изузетно је значајна јер овај облик компјутерског криминалитета доводи до тешких, често неотклоњивих последица. Детаљно законско регулисање, откривање и санкционисање свих облика злоупотреба друштвених мрежа уз повећану пажњу, стално праћење и контролу од стране администратора и корисника су најзначајнији облици превентивног деловања. Свакодневни развој интернета и друштвених мрежа

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.

3. „On line“ активности за безбедан интернет

Дан безбедног интернета (Safe Internet Day SID) обележава се сваке године другог дана друге недеље фебруара почев од 2004. године у организацији европске мреже INSAFE (www.safeinternet.org). Ова мрежа је успостављена у оквиру Програма за безбеднији интернет, који је осмислила Европска комисија. У Србији се овај дан обележава низом манифестација, пре свега у основним и средњим школама. Циљ обележавања Дана безбедног интернета је промовисање безбедног и одговарајућег коришћења on-line технологије и мобилног интернета, нарочито међу децом и младима у читавом свету. Паралелно се организују догађаји у стотинак земаља да би се подигла свест људи о проблемима и ризицима којима су изложена деца на интернету.

Од 2011. године уз финансијску помоћ организације Save the Children и ОАК Фондације, Фондација „Фонд Б92“ реализован је пројекат „Свеобухватни приступ заштити деце од злостављања и искоришћавања на интернету“, што је представљало припремну фазу за оснивање Центра за безбедни интернет. Центар за безбедни интернет „Кликни безбедно“ је пројекат, који од 2013. године спроводи Фондација „Фонд Б92“ у сарадњи са партнерима, Министарством трговине, туризма и телекомуникација и Министарством унутрашњих послова Републике Србије. Циљ пројекта и рада Центра за безбедни интернет је едукација и информисање грађана, посебно деце и младих, њихових родитеља, наставника и других интернет корисника о предности и ризицима употребе информационих и комуникационих технологија путем едукативних активности (трибина, радионица, обука за вршњачке едукаторе, надметања у знању и едукативним играма), као и заштита грађана од непримереног, недозвољеног и штетног садржаја и понашања на интернету обезбеђивањем релевантних информација о безбедној употреби интернета и

информационо-комуникационих технологије. Саветодавни одбор и Дечији савет обезбеђују реализацију активности Центра, а радом Центра руководе, подржавају га и помажу Фонд Б92, Министарство трговине, туризма и телекомуникација и министарство унутрашњих послова.[756]

У оквиру Центра за безбедни интернет постоји електронски механизам за пријаву нелегалоног, штетног и непримереног садржаја и понашања на интернету „Нет патрола“ у оквиру које едуковани оператери примају, обрађују и прослеђују пријаве надлежним службама. „Нет патрола“ је од новембра 2013. године члан INHOPE (Inhoup) Међународног удружења оператера интернет механизама за пријаве, који окупља оператере интернет механизама за пријаву штетног, недозвољеног и нелегалног садржаја на интернету, са циљем сузбијања ширења узнемирујућег материјала, посебно оног који садржи призоре и виртуелна представљања сексуалне злоупотребе деце, сексуалног искоришћавања и физичкох и психолошких напада на децу. Основни циљ рада „Нет патроле“ је да се спречи ширења материјала, који садржи призоре сексуалне злоупотребе деце, сексуално искоришћавање и физичке и психичке нападе на децу, али се такође могу пријављивати и материјали који садрже говор мржње, садржај расистичке и ксенофобичне природе, али и све друге непримерене садржаје и облике понашања на интернету. Сви садржаји се могу пријавити потпуно анонимно, попуњавањем онлајн формулара за пријаву на сајту www.netpatrola.rs или слањем пријаве путем електронске поште. Посебно едуковани оператери примају, обрађују и прослеђују пријаве грађана Јединици за високотехнолошки криминал МУП-а Србије и другим надлежним службама и организацијама у складу са утврђеном оперативном процедуром.

Током првих пет месеци рада у току 2013. године, „Нет патрола“ је примила 378 пријава, на основу којих су уклоњени следећи онлајн садржаји: блог са стотинама непримерених фотографија дечака, оглас за који је процењено да представља ризик од контактирања и узнемиравања деце у сврхе сексуалног искоришћавања (тзв. груминг), две странице са десетинама фотографија са експлицитним приказима сексуалне злоупотребе и искоришћавања деце, 6 интернет страница у оквиру једног форума које су

[756] Кликни безбедно, http:/kliknibezbedno.rs/sr/centar-za-bezbedni-internet.1.51.html, претражено 02.02.2016. године

садржале бројне линкове ка фотографијама и видео материјалима са експлицитним представама искоришћавања и злоупотребе деце у сексуалне сврхе, као и две странице на друштвеној мрежи Facebook. Пријаве које су се односиле на сексуалну злоупотребу деце су прослеђене Одељењу за високотехнолошки криминал МУП-а Србије на даљу истрагу и поступање, а шест пријава је упућено међународним електронским механизмима за пријаву штетног и недозвољеног садржаја (у Аустралији, Сједињеним Америчким Државама, Русији, Јапану и Швајцарској).

„Нет патрола“ је током 2014. и у првој половини 2015. година примила и обрадила 1690 пријава: 378 пријава садрже представе сексуалне злоупотребе малолетних особа, 85 пријава садрже еротске или друге облике неприкладних представа деце, 6 пријава груминга деце, 19 пријава расизма и ксенофобије, 417 пријава легалних, али штетних садржаја (нпр. малтретирања у виртуелном свету, екстремно насилна порнографија и сл.).[757] Од свих ових пријава, 252 пријаве су прослеђене на деловање Одељењу за високотехнолошки криминал при МУП-у Србије, 469 INHOPE мрежи, а 14 власницима садржаја. Пријављено је и 340 „спам“ порука. У 2015. години посредством партнера у INHOPE мрежи примљена је и прва пријава за уклањање нелегалног садржаја који је хостован унутар званичне територије Републике Србије, тачније на Косову, која је прослеђена међународним институцијама.

Интересантна апликација постоји од 28.09.2013. године на интернет порталу Министарства унутрашњих послова Републике Хрватске, под називом „Red Button“. Наиме, ова апликација је намењена свим интернет корисницима, али је посебно прилагођена деци и омогућује (1) пријављивање садржаја на Интернету за који се сумња да је незаконит или (2) различите облике искоришћавања или злостављања деце. За пријаву садржаја на Интернету, довољно је у апликацију унети адресу интернет странице и корисничко име починитеља. Апликација дозвољава да се пријава злостављања поднесе и за Интернет и за реално злостављање, а може да је поднесе како сама жртва тако и пријатељ жртве. Уколико се злостављање или узнемиравање догодило на

[757] Годишњи извештај о раду Центра за безбедни интернет – Србија у 2014.-2015. години, http://kliknibezbedno.rs/files/materijali/Klikni-bezbedno-publikacija-2015_1440332559.pdf, претражено 01.10.2015.године

Интернету, подносилац пријаве мора да унесе податке о интернет адреси и корисничком имену које злостављач користи, па се овај податак директно прослеђује на даљу обраду криминалистичкој полицији, и по потреби Центру за социјални рад, тужилаштву и сл. Од почетка пуштања у рад апликације па до 31.12.2014.године поднето је укупно 1241 пријава од којих је поступано у 333. Највише пријава се односило на странице на друштвеној мрежи Facebook, спам поруке и поруке са порнографским садржајем.[758]

[758] Министарство унутрашњих послова Републике Хрватске, http://mup.hr/169020.aspx, претражено 28.09.2015.године; Протрка, Никола, Грубер, Кристијан, Салопек, Данко, *op.cit.,* 2015, str. 653

ГЛАВА V

РЕЗУЛТАТИ ЕМПИРИЈСКОГ ИСТРАЖИВАЊА

1. Предмет, циљ и метод истраживања

Предмет истраживања било је сазнавање ставова корисника различитих друштвених мрежа о могућности злоупотребе права на приватност путем друштвених мрежа, коришћења/некоришћења одређене заштите, као и утврђивање најсигурнијих метода превентивног деловања и спречавања виктимизације корисника друштвених мрежа. Основни циљеви истраживања били су: утврђивање учесталости коришћења појединих друштвених мрежа од стране испитаника/испитаница и њихове активности на друштвеним мрежама; добијање података о препознавању насиља на друштвеним мрежама и могућностима заштите; утврђивање изложености испитаника/испитаница различитм облицима виктимизације и могућности за правовремену заштиту права на приватност.

Истраживање је имало карактер пилот или пробног истраживања и рађено је на пригодном намерно одабраном узорку. Реализација истраживања трајала је од јануара 2014. године до априла 2014. године и резултати истраживања су омогућили разраду ваљане хипотетичке основе за нова, шира и продубљенија истраживања. Истраживање је спроведено у две фазе. У првој фази су анкетирани одабрани корисници друштвених мрежа, којих је било укупно 612. Један део испитаника чинили су ученици одабраних основних школа, средњих школа и факултета, а други део испитаника чинили су активни корисници друштвених мрежа одабрани слањем упитника на одређене e-mail adrese. Ученици и студенти су упитнике попуњавали на часовима, а затим их предавали наставницима/професорима. Корисници друштвених мрежа су анкету попуњавали преко интернета (on line), тако што су одговори директно били прослеђивани у базу података која је након тога обрађивана и анализирана.

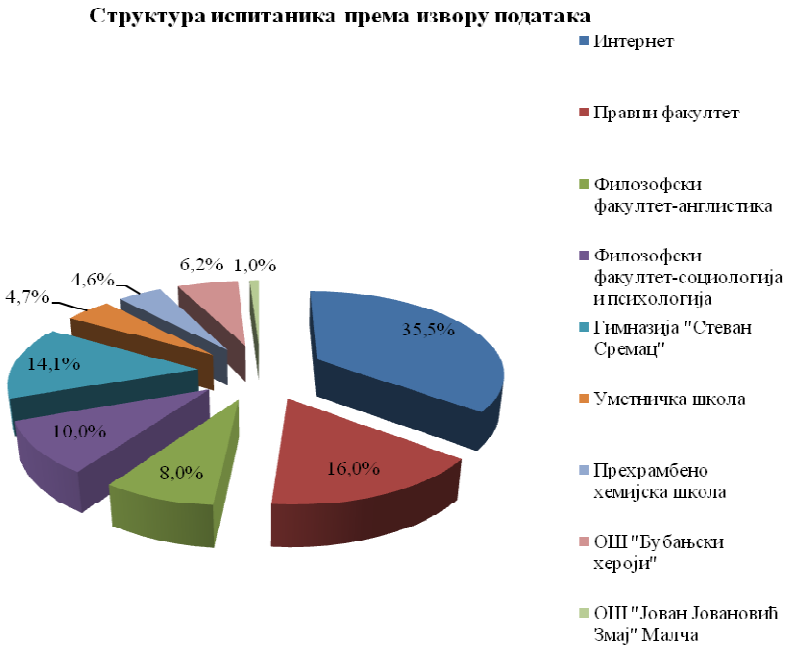
У другој фази истраживања, прикупљени подаци су селектовани и статистички обрађени, а након тога уследила је анализа и интерпретација података, чији су резултати презентовани у докторској тези.

За потребе истраживања сачињен је посебан упитник који је садржао општа питања везана за независне варијабле: пол, године старости, образовање, пребивалиште. Друга врста питања односила се на: учесталост коришћења интернета и комуникације преко друштвених мрежа, податке који се најчешће саопштавају непознатим и познатим особама преко друштвених мрежа, могуће видове злоупотребе и повреде права на приватност у контактима преко друштвених мрежа, облике заштите које је могуће применити и предлоге мера за спречавање злоупотребе права на приватност путем друштвених мрежа.

Подаци добијени истраживањем су шифрирани и унесени у матрицу. У анализи је коришћен хи-квадрат тест како би се утврдила статистичка значајност уочених разлика између укрштених обележја. Обрада података је рађена у програму СПСС.

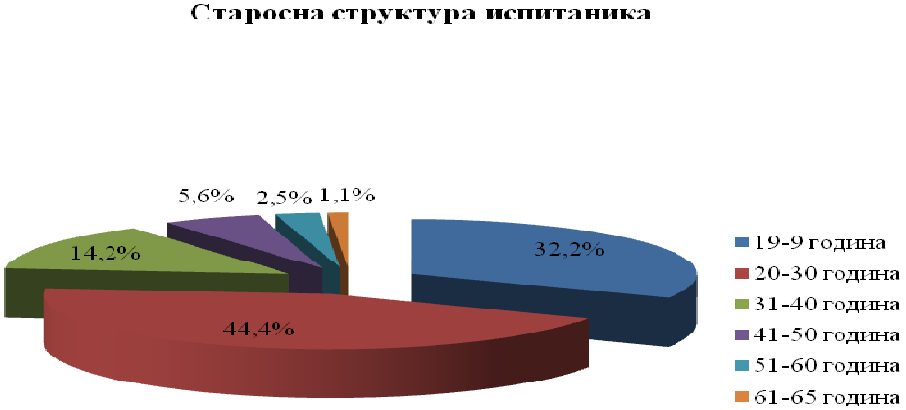
2. Структура узорка

С обзиром на различиту структуру корисника друштвених мрежа, да би се постигла репрезентативност, анкета је спроведена на тај начин што су анкетни упитници упућивани на случајно одабране e-mail адресе или преко друштвених мрежа (217 корисника или 35.5%), док је већи број испитаника (395 или 64.5%) случајно одабран из популације студената/студенткиња (Правни факултет, Филозофски факултет, департмани: Англистика, Социологија и Психологија), ученика средњих (гимназија „Стеван Сремац“, Уметничка школа, Прехрамбено хемијска школа) и основних школа („Бубањски хероји“, „Јован Јовановић Змај“ Малча).



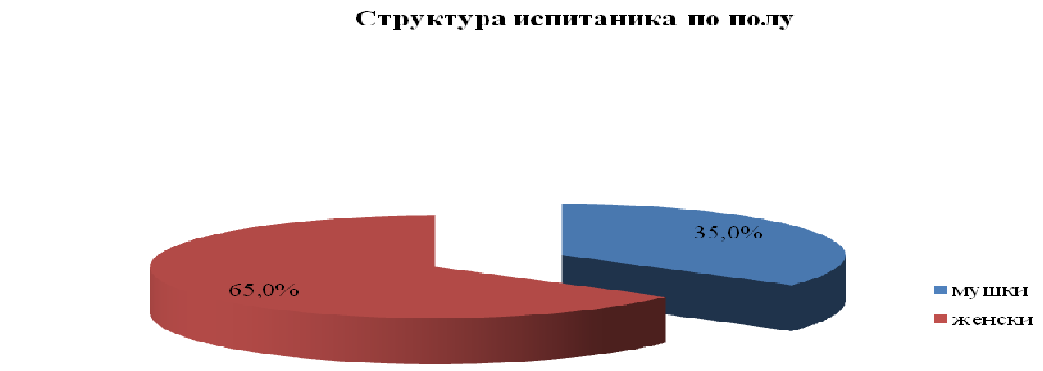
Графикон 1.

Анкетирани испитаници/испитанице су били различитог узраста (графикон 2.). Преовлађује узраст од 20-30 година (271 или 44.4%), што је разумљиво јер је највећи број активних корисника/корисница душтвених мрежа управо тих година. Прилично је заступљен и узраст од 9-19 година (197 или 32.2%), док је најмање заступљен узраст од 51-60 година (15 или 2.5%) и 61-65 година (7 или 1.1%). Оваква структура испитаника/испитаница према узрасту упоређена са бројем корисника/корисница друштвених мрежа показује да су корисници/кориснице друштвених мрежа углавном млађег узраста.



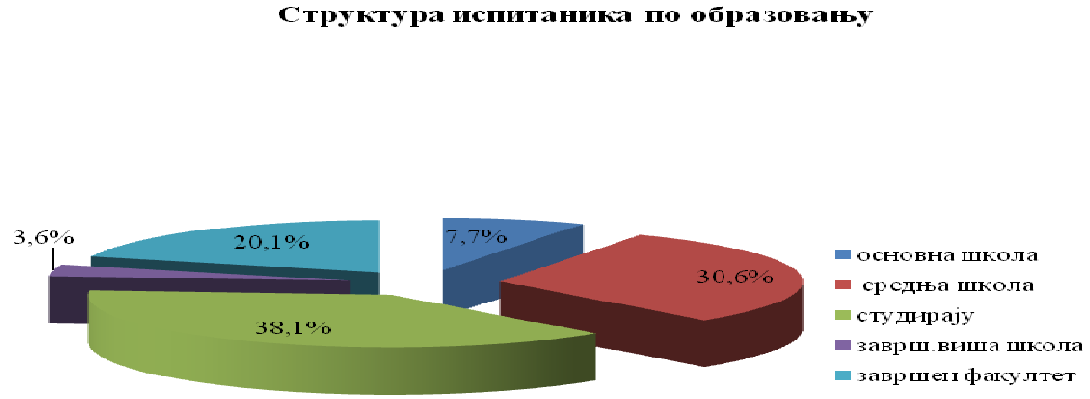
Графикон 2.

Дистрибуција испитаника према полу (графикон 3) показује знатну бројчану предност испитаника женског пола (398 или 65.0%) у односу на испитанике мушког пола (214 или 35%), што је разумљиво јер су жене бројчано заступљеније међу корисницима друштвених мрежа С обзиром на то да истраживање није обухватило упоређивање пола испитаника са учесталошћу коришћења друштвених мрежа, ове процентуалне разлике по полу, нису статистички значајне.



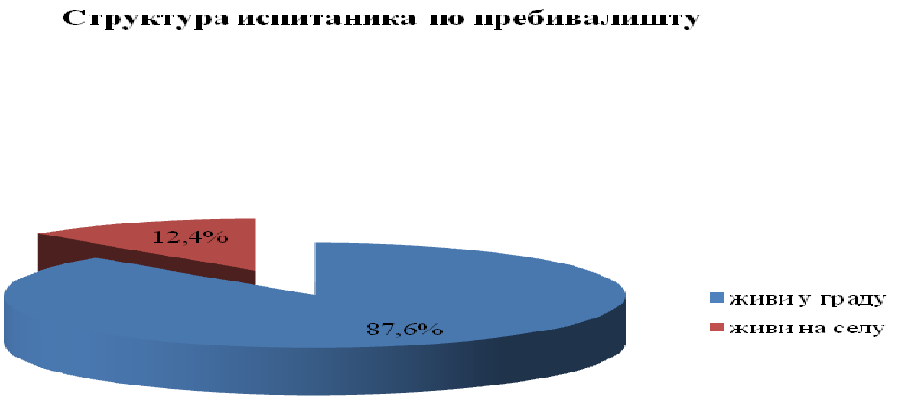
Графикон 3.

Испитаници/испитанице у узорку су различитог образовања (графикон 4). Преовлађују студенти/студенткиње (38.1%), затим испитаници/испитанице са завршеном средњом школом (30.5%) и завршеним факултетом (20.1%).



Графикон 4.

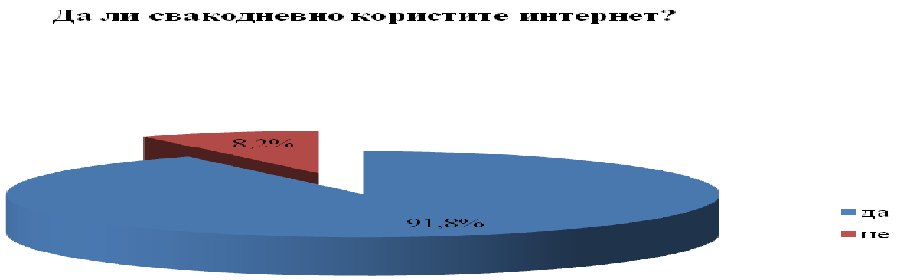
У погледу пребивалишта (графикон 5), већина испитаника/испитаница има пребивалишта у граду - 87.6%, док у руралној средини живи знатно мање испитаника/испитаница – 12.4%.



Графикон 5.

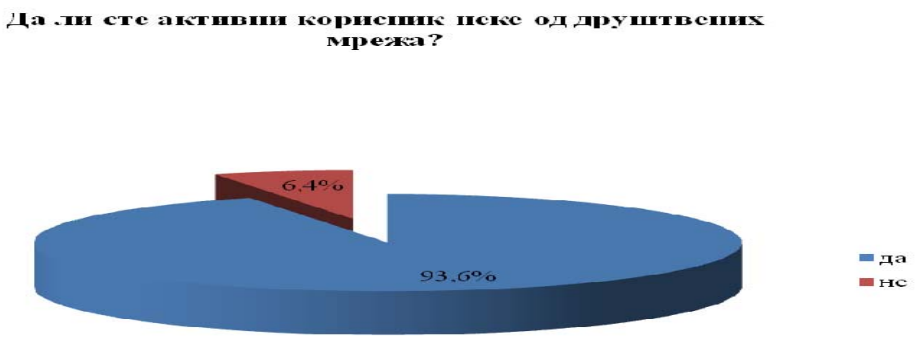
3. Анализа резултата истраживања

Да би се утврдила учесталост коришћења интернета, испитаницима /испитаницама је постављено питање да ли свакодневно користе интернет. Како се могло претпоставити велики проценат испитаника/испитаница свакодневно користи интернет – 91. 8%, само 8.2% не користи свакодневно интернет (графикон 6).



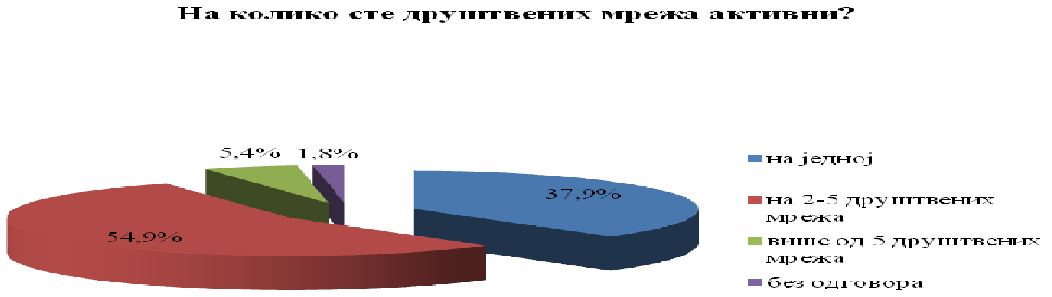
Графикон 6

У погледу активног коришћења друштвених мрежа такође је испољена велика учесталост корисника/корисница јер се чак 93.6% испитаника /испитаница изјаснило да активно користи друштвене мреже, а само 6.4% корисника/корисница није активно на друштвеним мрежама (графикон 7.)



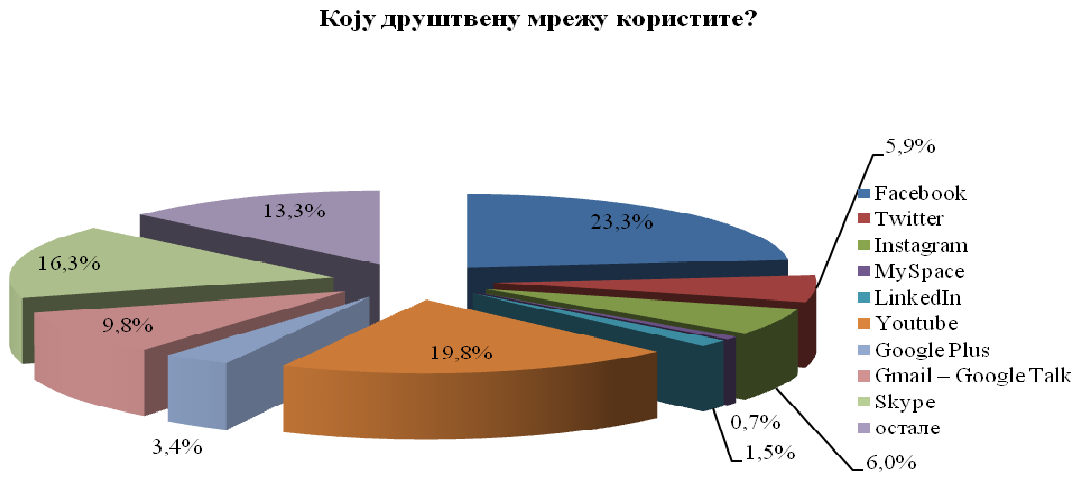
Графикон 7

Испитаници/испитанице не користе само једну већ више друштвених мрежа. Већи проценат испитаника/испитаница активан је на две до пет друштвених мрежа 54.9% или на једној 37.9%, док је на више од пет друштвених мрежа активно 5.4% испитаника/испитаница (графикон 8.). Овај резултат се не разликује од података везаних за општу популацију који показују да већина корисника/корисница друштвених мрежа користе већи број друштвених мрежа, што је такође индикатор већих могућности за злоупотребу њихове приватности.



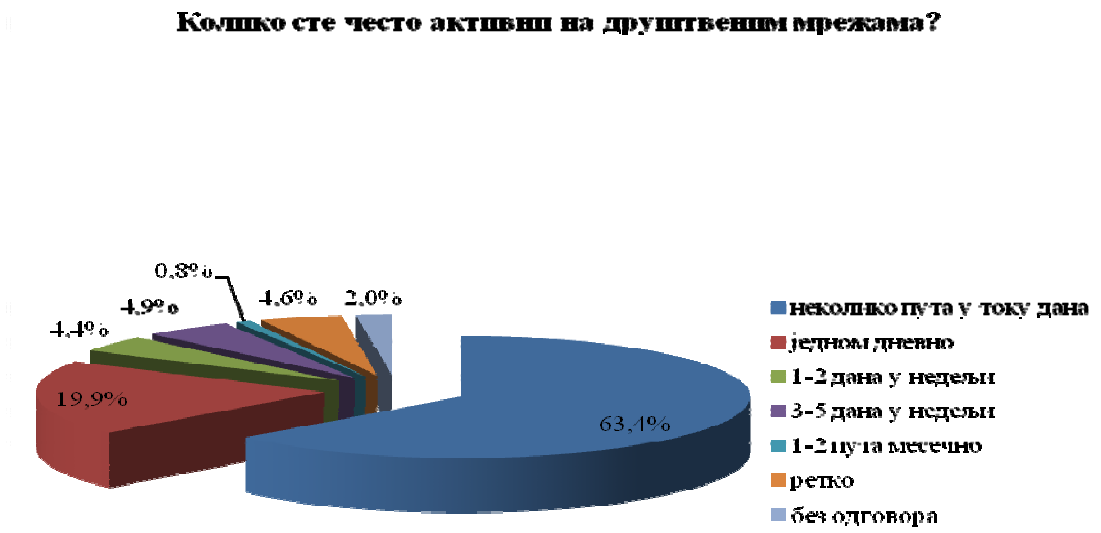
Графикон 8.

Испитаници/испитанице, који користе друштвене мреже, испољавају различито интересовање за поједине друштвене мреже. Највећи проценат испитаника/испитаница користи друштвену мрежу Facebook (23.3%), затим Youtube (19.8%), Skype (16%), Gmail Google Talk (9.8%). Само 0.7% испитаника/испитаница користи MySpace (графикон 9).



Графикон 9.

Активност на друштвеним мрежама испитаника/испитаница се, према њиховим одговорима, одвија у различитим временским интервалима. Највише испитаника/испитаница користи друштвене мреже неколико пута у току дана 63.4% и једном дневно 19.9%. Најмањи проценат испитаника (0.8%) користи друштвене мреже један до два пута месечно, што показује да су испитаници/испитанице у току дана веома активни на друштвеним мрежама (графикон 10).



Графикон 10.

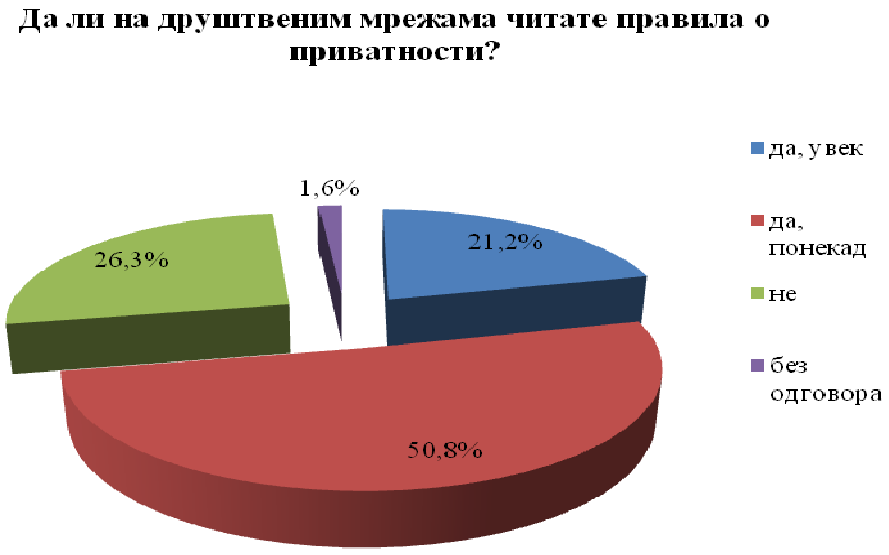
Корисници/корисице друштвених мрежа могу и умеју да заштите свој Facebook профил и да на тај начин сами превенирају могуће злоупотребе њихове приватности. Због тога је највећи проценат испитаника/испитаника

одговорио да је њихов Facebook профил приватни и да смо њихови пријатељи могу да се упознају са садржајем профила – 55.4%, али није занемарљив проценат испитаника/испитаница који су се изјаснили да је њихов Facebook профил могу да виде сви корисници друштвене мреже – 10.0% или да је њихов Facebook профил делимично приватан – 23.0% (табела 1).

Табела 1. - Какав је у погледу заштите Ваш Facebook профил?

	Број	***Проценат***
јавни (сви корисници друштвене мреже могу да виде садржај профила)	**61**	**10 %**
делимично приватни	**141**	**23 %**
приватни (само пријатељи могу да виде садржај профила)	**339**	**55.4 %**
не знам	**47**	**7.7 %**
нема facebook профил	**23**	**3.8 %**
без одговора	**1**	**0.2 %**
укупно	**612**	**100 %**

Приликом одговора на питање да ли на друштвеним мрежама читају правила о приватности, већина испитаника/испитаница је одговорила да то чини само понекад 50.8% или да уопште не чита правила о приватности – 26.3%, што показује да овај облик примарне превентивне заштите испитаници/испитанице недовољно примењују (графикон 11). Само 21.2% испитаника/испитаница увек чита правила о приватности на друштвеним мрежама.



Графикон 11.

Неопрезност у навођењу личних података на Facebook профилу види се и у одговору на питање да ли профил садржи податке о узрасту испитаника /испитаница. Велика већина испитаника/испитаница је одговорила да на њиховом Facebook профилу пише колико имају година – 60.9% и да овај податак постоји на неким профилима – 10.0%. Много мање испитаника /испитаница не наводи овај податак – 27.0% (табела 2).

Табела 2. - Да ли на Вашим профилима пише колико година имате?

	Број	*Проценат*
да	**373**	**60.9 %**
не	**165**	**27 %**
не на свим профилима	**61**	**10 %**
без одговора	**13**	**2.1 %**
укупно	**612**	**100 %**

Мало већу опрезност показали су испитаници/испитанице када је у питању коришћење истог компјутера на радном месту/школи/факултету приликом приступа интернету и друштвеним мрежама. Већи проценат испитаника/испитаница одговорио је да не користи исти компјутер – 50.7%, али је такође висок проценат оних који заједнички користе исти компјутер приликом приступа интернету и друштвеним мрежама – 48.2% (табела 3).

Табела 3. - Да ли на радном месту/школи/факултету више вас користи исти компјутер да приступате интернету и друштвеним мрежама?

	Број	*Проценат*
да	**295**	**48.2 %**
не	**310**	**50.7 %**
без одговора	**7**	**1.1 %**
укупно	**612**	**100 %**

Анкета је показала да испитаници/испитанице у највећем проценту на друштвене мреже постављају слике/видео снимке на којима су са својим пријатељима – 59.6% или где су сами – 25.0%. Само 13.6% испитаника /испитаница не поставља своје слике или видео снимке на друштвене мреже. Ово такође показује да међу испитаницима/испитаницама није довољо развијен систем самозаштите приватних података (табела 4).

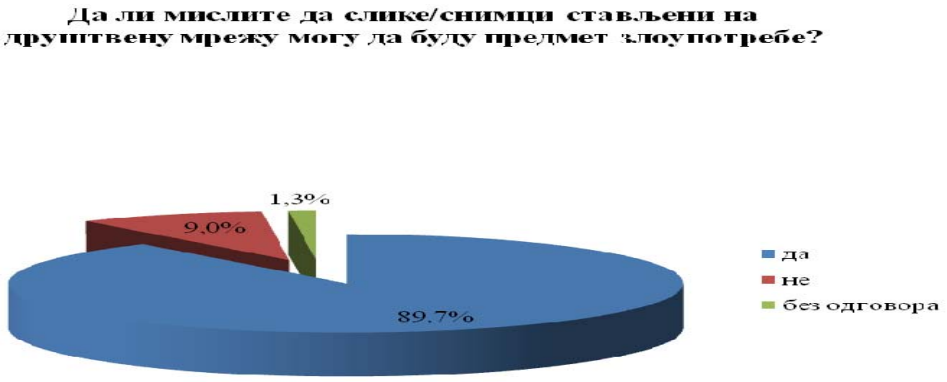
Табела 4. - Да ли на друштвене мреже постављате своје слике или видео снимке?

	Број	*Проценат*
да, постављам слике/снимке где сам сам/сама	**153**	**25 %**
да, постављам слике/снимке на којима сам са својим пријатељима	**365**	**59.6 %**
не, никада	**83**	**13.6 %**
без одговора	**11**	**1.8 %**
укупно	**612**	**100 %**

За разлику од одговора на претходно питање, када су испитаници /испитанице показали неопрезност у погледу заштите својих личних података, када се ради по сликама или видео снимцима других људи, 65.5% испитаника /испитаница никада то не чини без сагласности оних чије се слике или видео снимци постављају на друштвене мреже. Само 3.9% испитаника/испитаница поставља на друштвене мреже слике и видео снимке других људи без њихове претходне сагласности (графикон 12).

Графикон 12.

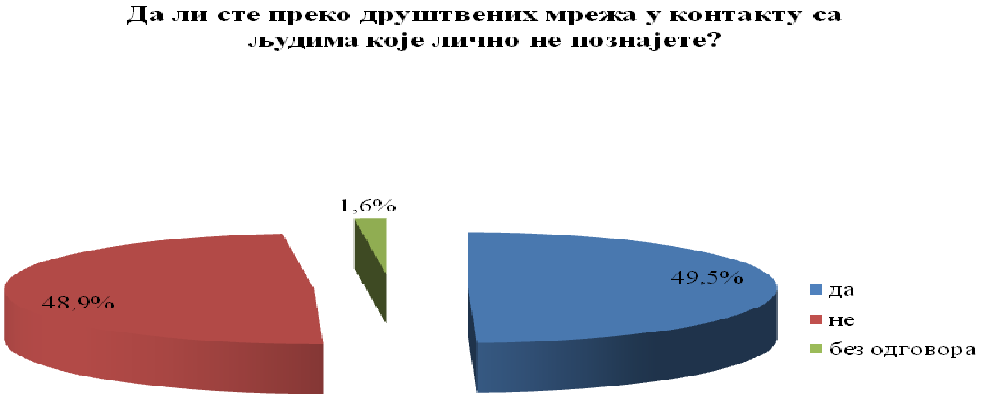
Разлог за врло ретко постављање слика и видео снимака на друштвене мреже код већине испитаника/испитаника – 89.7% је њихово уверење да слике/снимци могу да буду предмет злоупотребе (графикон 13). Много мање испитаника/испитаница – 9.0 сматра да до злоупотребе слика/снимака неће доћи. Овај налаз показује да су испитаници/испитанице у великој мери упознати са повећаним ризиком од злоупотребе приватности уколико слике/видео снимке поставе на друштвену мрежу коју користе.



Графикон 13.

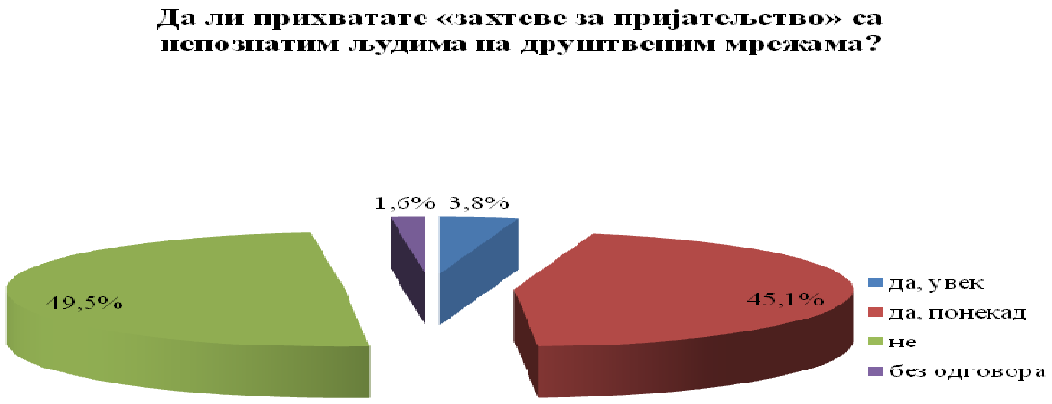
Испитаницима/испитаницама је постављено питање на који начин могу да слике/снимци стављени на друштвене могу да буду искоришћени у погрешне сврхе. Као могуће видове злоупотребе испитаници/испитанице су навели: крађу идентитета и преваре; манипулација сликом или подацима са друштвене мреже; коришћење слике у циљу сексуалне експлоатације, порнографије и педофилије; сексуално узнемиравање; ради уцене, праћења, подсмеха итд.

Интересантно је да приближан проценат испитаника/испитаница јесте (49.5%) и није (48.9%) у контакту преко друштвених мрежа са људима које лично не познају (графикон 14).



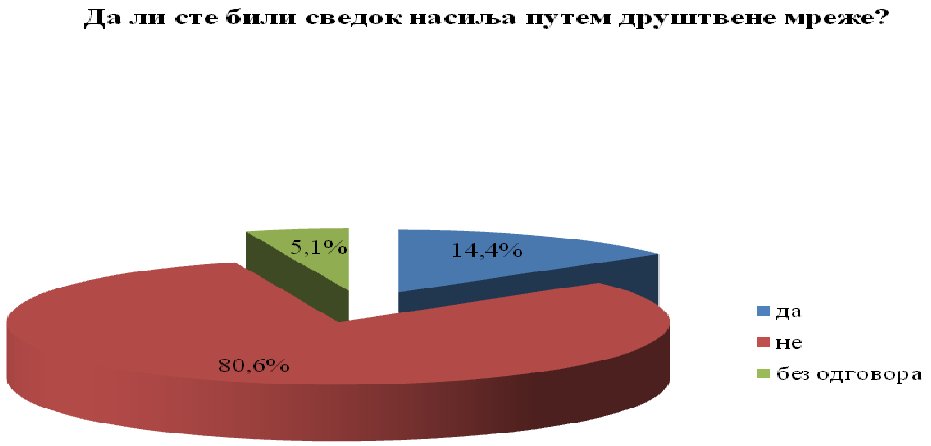
Графикон 14.

Велику неопрезност испитаници/испитанице показују када се ради о „захтеву за пријатељство“ са непознатим људима на друштвеним мрежама. И у овом случају се скоро подједнак проценат испитаника/испитаница који су одговорили да оваква пријатељства не прихватају – 49.5% у односу оне који такве захтеве увек прихватају и понекад прихватају – 48.9% (графикон 15).



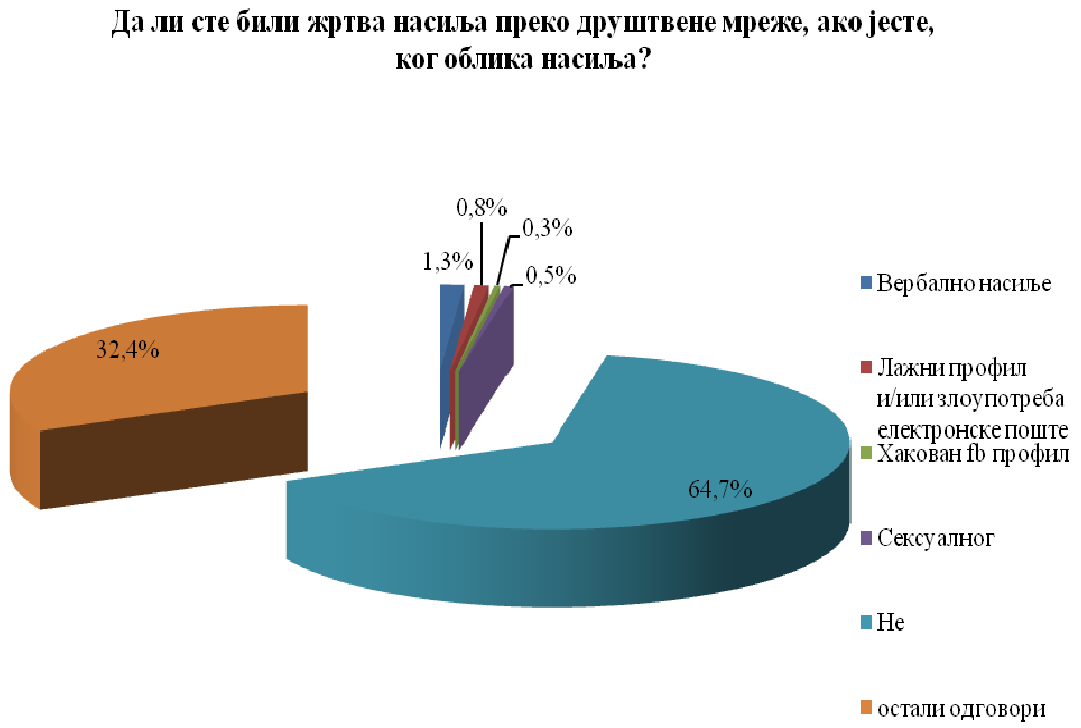
Графикон 15.

Неопрезност испитаника/испитаница приликом коришћења друштвених мрежа исказана приликом одговора на претходна питања свакако је резултат несуочавања са насиљем које се испољава преко друштвених мрежа. Само 14.4% испитаника је одговорило да су били сведоци насиља путем друштвених мрежа. Знатно већи проценат испитаника/испитаница – 80.6% се није суочио са насиљем преко друштвених мрежа (графикон 16).



Графикон 16.

Испитаници/испитанице који су одговорили да су били сведоци насиља путем друштвених мрежа у највећем проценту су се изјаснили да нису реаговали – 52.1%. Они који су реаговали на сазнање о насиљу, учинили су то најчешће пријавом администратору мреже – 3.6%, блокирањем корисника – 2.3% и подношењем кривичне пријаве – 0.8%. Описујући облик насиља коме су били изложени испитаници/испитанице су навели да се најчешће радило о вербалном насиљу, затим о лажном профилу и/или злоупотреби електронске поште, хакованом Facebook профилу и сексуалном насиљу (графикон 17).



Графикон 17

Анкета је показала да највећи проценат испитаника/испитаница – 88.7% није никада био жртве прогањања или сексуалног узнемиравања преко друштвене мреже. Мањи број испитаника/испитаница – 57 (9.3%) одговорио је да су једном или више пута били жртве прогањања или сексуалног узнемиравања (табела 5).

Табела 5. - Да ли сте некада били жртва прогањања или сексуалног узнемиравања преко друштвене мреже?

	Број	***Проценат***
да , једном	**37**	**6.0 %**
да, више пута	**20**	**3.3%**
не	**543**	**88.7%**
без одговора	**12**	**2.0%**
укупно	**612**	**100 %**

Исто тако, највећи број испитаника/испитаница је одговорио да нису били жртве преваре или крађе преко друштвене мреже – 533 или 87.1%. Жртава овог облика криминалитета у испитиваном узорку било је само 38 и то 33 или 5.4% испитаника/испитаница је једном имало такво искуство, док је 5 или 0.8% више пута било жртва преваре или крађе преко друштвене мреже (табела 6).

Табела 6. - Да ли сте некада били жртва преваре или крађе преко друштвене мреже?

	Број	*Проценат*
да , једном	**33**	**5.4%**
да, више пута	**5**	**0.8%**
не	**533**	**87.1%**
без одговора	**41**	**6.7%**
укупно	**612**	**100 %**

Иако већина испитаника/испитаница нису били жртве насиља преко друштвене мреже у својим одговорима су наводили шта, по њиховом мишљењу; може да буде разлог насиља било које врсте преко друштвене мреже. Према мишљењу испитаника/испитаница то може да буде: психички проблем или фрустрација (135 или 22.1%), већа слобода и храброст у виртуелном свету него у реалном јер постоји анонимност (50 или 8.2%), досада или забава (37 или 6%), превелика отвореност у комуникацији и непотребно стављање на друштвену мрежу много приватних података (11 или 1.8%), одсуство санкција (5 или 0.8%), доступност података о личности (5 или 0.8%).

Графикон 18.

На питање „да ли се осећате сигурним/сигурном када користите друштвену мрежу?“ само 2 (0.3%) испитаника/испитаница није дало одговор. Већина испитаника/испитаница је одговорила да се: осећају сигурним приликом

коришћења друштвених мрежа (116 или 17.3%); да се осећају сигурним јер нису никада имали било какве непријатности на друштвеним мрежама (192 или 28.6%); да се осећају сигурним јер су увек када се деси проблем успевају да га сами реше (61 или 9.1%); да се углавном осећају сигурним јер знају да постоје они који су имали лоша искуства (187 или 27.8%); да се углавном оећају сигурним јер су имали лоша искуства из којих су научии да буду опрезни (22 или 3.3%). Поједини испитаници/испитанице су веома опрезни приликом коришћења друштвених мрежа и одговорили су да се никада не осећају сигурним јер „опасност увек вреба“ (92 или 13.7%).

Испитаници/испитанице су уочили да су корисници/кориснице приликом коришћења друштвених мрежа изложени различитим претњама. Као најчешће су наведене: злоупотреба фотографије (362 или 17.0%); ширење говора мржње (342 или 16.1%); слање претњи (305 или 14.3%)); узнемиравање или малтретирање од стране пријатеља или познаника (280 или 13.2%); неовлашћено сликање или коришћење фотографије (278 или 13.1%); сексуално узнемиравање у причаоницама, преко друштвене мреже или електронске поште (196 или 9.2%); затрпавање нежељеним сексуалним садржајима (195 или 9.2%); прогањање и присиљавање на нежељену комуникацију преко интернета (169 или 7.9%).

Поједини испитаници/испитанице имали су негативно искуство са наведеним претњама преко друштвених мрежа. Приличан број испитаника /испитаница 142 или 18.7% није хтео да одговори на питање о томе да ли су приликом коришћења друштвених мрежа били изложени некој претњи, док је 42 или 5.5% испитаника/испитаница одговорило да нису били изложени никаквим претњама. Најчешће претње биле су: ширење говора мржње, које обухвата сваку комуникацију која омаловажава особу или групу на основу карактеристика, као што су раса, боја коже, етничка или национална припадност, пол, сексуална оријентација, религија (142 или 18.7%); затрпавање нежељеним сексуалним садржајима (110 или 14.5%); узнемиравање или малтретирање од стране пријатеља или познаника (67 или 8.8%); злоупотреба фотографије (65 или 8.6%); слање претњи (51 или 6.7%); неовлашћено сликање и коришћење фотографије (43 или 5.7%); прогањање или присиљавање на нежељену комуникацију преко интернета (39 или 5.1%) и сексуално узнемиравање у причаоницама, преко друштвене мрежа или електронске поште (33 или 4.3%).

Према одговорима испитаника/испитаница, којима се догодило да буду изложени претњама преко друштвених мрежа, најнебезбеднија у том погледу је друштвена мрежа Facebook. Ипак, с обзиром на то да велики број

испитаника/испитаница - 222 (36.3%) није одговорио на питање на којој друштвеној мрежи су највише били изложени претњама, добијени резултати нису статистички значајни (табела 7).

Табела 7. - Уколико Вам се догодило нешто од наведеног, упишите о којој је друштвеној мрежи/друштвеним мрежама реч?

	Број	*Проценат*
Facebook	**236**	**38.6%**
Twitter	**11**	**1.8%**
Skype	**12**	**2.0%**
Није ми се десило	**95**	**15.5%**
Instagram	**5**	**0.8%**
Остале мреже	**30**	**4.9%**
Без одговора	**222**	**36.3%**
укупно	**611**	**100.0%**

Уколико се догоди нека од наведених претњи испитаници/испитанице се најчешће обраћају једном или неколицини пријатеља (355 или 29.3%), затим полицији (316 или 26.1%); родитељима/старатељима (284 или 23.5%), суду (103 или 8.5%); невладиној опрганизацији (80 или 6.6%); наставнику/професору (58 или 4.8%), док се 14 или 1.2% испитаника никоме не обраћа за помоћ.

С обзиром на то да су испитаници/испитанице били изложени различитим претњама приликом коришћења друштвених мрежа постављено им је низ питања да би се сазнала њихова реакција и мере које су предузели да се на наки начин заштите. Велики број испитаника/испитаница је обрисао некога са списка контаката – 524 или 85.6% , само 57 или 9.3% испитаника нису обрисали никога са списка контаката (табела 8). Своје име са слике коју је неко други поставио обрисало је 362 или 59.2% испитаника/испитаница, али приличан број испитаника/испитаница – 208 или 34% то није учинио, док 42 или 6.9% испитаника/испитаница није одговорило на ово питање (табела 9). Коментар који је неко написао обрисало је 376 или 61.4% испитаника /испитаница, такав коменетар није обрисало 189 или 30.9% испитаника /испитаница, није одговорило 47 или 7.7% испитаника/испитаница (табела 10). Већи број испитаника/испитаница – 447 или 73% је обрисао или изменио нешто што је објавио, 121 или 19.8% то није учинио, док 44 или 7.2% испитаника/испитаница није одговорило на питање „да ли сте до сада обрисали или изменили нешто што сте објавили?“ (табела 11).

Табела 8. - Да ли сте до сада обрисали некога са списка контаката?

	Број	*Проценат*
да	**524**	**85.6 %**
не	**57**	**9.3 %**
без одговора	**31**	**5.1 %**
укупно	**612**	**100 %**

Табела 9. - Да ли сте до сада обрисали своје име са слике коју је неко други поставио?

	Број	*Проценат*
да	**362**	**59.2 %**
не	**208**	**34 %**
без одговора	**42**	**6.9 %**
укупно	**612**	**100 %**

Табела 10. - Да ли сте до сада обрисали коментар који вам је неко написао?

	Број	*Проценат*
да	**376**	**61.4 %**
не	**189**	**30.9 %**
без одговора	**47**	**7.7 %**
укупно	**612**	**100 %**

Табела 11. - Да ли сте до сада обрисали или изменили нешто што сте објавили?

	Број	*Проценат*
да	**447**	**73 %**
не	**121**	**19.8 %**
без одговора	**44**	**7.2 %**
укупно	**612**	**100 %**

Да испитаници/испитанице пазе шта објављују види се из одговора на питање „да ли сте до сада објавили нешто од чега вас је касније било срамота?“. Највећи број – 405 или 66.2% одговорио је да то није учинио; 143 или 23.4% испитаника/испитаница је одговорило да су објавили нешто од чега их је касније било срамота, а 64 или 10.5% није одговорило на ово питање (табела 12)

Табела 12.

	Број	Проценат
да	143	23.4 %
не	405	66.2 %
без одговора	64	10.5 %
укупно	612	100 %

Опрезност/неопрезност испитаника приликом коришћења друштвених мрежа и тачност/ нетачност података који стављају на друштвене мреже, сагледава се приликом одговора на следећа питања:

- да ли сте до сада свој профил учинили јавним да свако може да му приступи (437 или 71.4% то није учинило; 114 или 18.6% јесте; 61 или 10% није одговорило – табела 13);

Табела 13.

	Број	Проценат
да	114	18.6 %
не	437	71.4 %
без одговора	61	10 %
укупно	612	100 %

- да ли сте на свом профилу написали адресу становања (505 или 82.5% то није учинило; 41 или 6.7% јесте, 66 или 10.8% није одговорило - табела 14);

Табела 14.

	Број	Проценат
да	41	6.7 %
не	505	82.5 %
без одговора	66	10.8 %
укупно	612	100 %

- да ли сте до сада блокирали неку особу да не може да вас више контактира (398 или 65% је то учинило; 168 или 27.5% није, 46 или 7.5% није одговорило – табела 15);

Табела 15.

	Број	*Проценат*
да	**398**	**65 %**
не	**168**	**27.5 %**
без одговора	**46**	**7.5 %**
укупно	**612**	**100 %**

- да ли сте до сада некада обрисали или деактивирали ваш профил на друштвеној мрежи (326 или 53.3% то није учинило, 232 или 37.9% је обрисало или деактивирало свој профил на друштвеној мрежи, 54 или 8.8% није одговорило – табела 16);

Табела 16.

	Број	*Проценат*
да	**232**	**37.9 %**
не	**326**	**53.3 %**
без одговора	**54**	**8.8 %**
укупно	**612**	**100 %**

- да ли сте приликом комуникације на друштвеним мрежама дали нетачан податак у погледу свог узраста (438 или 71.6% није дало нетачан податак у погледу узраста, 116 или 19% је то учинило, 58 или 9.5% није одговорило – табела 17);

Табела 17.

	Број	*Проценат*
да	**116**	**19 %**
не	**438**	**71.6 %**
без одговора	**58**	**9.5 %**
укупно	**612**	**100 %**

- колико пута сте до сада додали непознато лице на листу контаката (206 или 33.7% то никада није учинило, 197 или 32.2% је то учинило 1-5 пута, више од 5 пута 152 или 24.8%; увек то чини 30 или 4.9%, без одговора је 27 или 4.4%; значи, већи је проценат испитаника

/испитаница 61,9% који су додавали непознато лице на листу контаката од оних који то нису чинили – 33.7% - табела 18);

Табела 18.

	Број	*Проценат*
никада	**206**	**33.7 %**
1-5 пута	**197**	**32.2 %**
више од 5 пута	**152**	**24.8 %**
увек	**30**	**4.9 %**
без одговора	**27**	**4.4%**
укупно	**612**	**100%**

- колико пута сте до сада разговарали телефоном са особом коју сте упознали преко друштвене мреже (402 или 65.7% никада није разговарало телефоном са особом коју су упознали преко друштвене мреже, 132 или 21.6% је то учинило 1-5 пута, 38 или 6.2% више од 5 пута; увек то чини 12 или 2% испитаника/испитаница, 28 или 4.6% је без одговора на ово питање – табела 19);

Табела 19.

	Број	*Проценат*
никада	**402**	**65.7 %**
1-5 пута	**132**	**21.6 %**
више од 5 пута	**38**	**6.2 %**
увек	**12**	**2 %**
без одговора	**28**	**4.6 %**
укупно	**612**	**100 %**

- колико пута сте до сада упознали лично особу коју сте најпре упознали преко друштвене мреже (највећи број 309 или 50.5% никада није лично упознало особу коју је најпре упознало преко друштвене мреже, 197 или 32.2% је то учинило 1-5 пута; више од 5 пута – 63 или 10.3%, увек то чини 18 или 2.9% испитаника, без одговора је 25 или 4.1% - табела 20);

Табела 20.

	Број	Проценат
никада	309	50.5 %
1-5 пута	197	32.2 %
више од 5 пута	63	10.3 %
увек	18	2.9 %
без одговора	25	4.1 %
укупно	612	100 %

- информације о имену и презимену преко друштвене мреже непознатим људима дало је чак 372 испитаника/испитаница (60.8%), што показује да су испитаници/испитанице прилично искрени у саопштавању својих података. Информације о имену и презимену није дало никада 205 (33.5%) испитаника /испитаница, док 35 (5.7%) није одговорило на ово питање (табела 21).

Табела 21.

	Број	Проценат
никада	205	33.5 %
да, увек	372	60.8 %
без одговора	35	5.7 %
укупно	612	100 %

- да ли сте преко друштвених мрежа непознатим људима дали информацију о томе где радите или студирате (никада – 287 или 46.9%; да, увек – 284 или 46.4%; без одговора – 41 или 6.7% (табела 22);

Табела 22.

	Број	Проценат
никада	287	46.9 %
да, увек	284	46.4 %
без одговора	41	6.7 %
укупно	612	100 %

- да ли сте преко друштвених мрежа непознатим људима дали информацију о томе где обично идете са пријатељима (462 или 75.5% никада није дало ову информацију, 108 или 17.6% увек даје ову информацију, без одговора је 42 или 6.9% - табела 23);

Табела 23.

	Број	*Проценат*
никада	**462**	**75.5 %**
да, увек	**108**	**17.6 %**
без одговора	**42**	**6.9 %**
укупно	**612**	**100 %**

- да ли сте преко друштвених мрежа непознатим људима послали личне фотографије и фотографије блиских људи (380 или 62.1% испитаника/испитаница никада није послало личне фотографије и фотографије блиских људи, 188 или 30.7% увек то чини, без одговора је 44 или 7.2% - табела 24);

Табела 24.

	Број	*Проценат*
никада	**380**	**62.1 %**
да, увек	**188**	**30.7 %**
без одговора	**44**	**7.2 %**
укупно	**612**	**100 %**

- да ли сте преко друштвених мрежа непознатим људима послали e-mail адресу (417 или 68.1% није никада послало e-mail адресу, 154 или 25.2% увек то чини, 41 или 6.7% је без оговора на ово питање – табела 25);

Табела 25.

	Број	*Проценат*
никада	**417**	**68.1 %**
да, увек	**154**	**25.2 %**
без одговора	**41**	**6.7 %**
укупно	**612**	**100 %**

- да ли сте преко друштвених мрежа непознатим људима дали информацију о својој адреси становања (546% или 89.2% никада није дало адресу становања, 24 или 3.9% увек даје адресу становања, 42 или 6.9% није одговорило – табела 26);

Табела 26.

	Број	*Проценат*
никада	**546**	**89.2 %**
да, увек	**24**	**3.9 %**
без одговора	**42**	**6.9 %**
укупно	**612**	**100 %**

- да ли сте преко друштвених мрежа непознатим људима дали информацију о свом броју телефона (486 или 79.4% никада то није учинило, 79 или 12.9% увек даје информацију о броју телефона, без одговора је 47 или 7.7% испитаника/испитаница – табела 27).

Табела 27.

	Број	*Проценат*
никада	**486**	**79.4 %**
да, увек	**79**	**12.9 %**
без одговора	**47**	**7.7 %**
укупно	**612**	**100 %**

Испитаници/испитанице су показали велику опрезност приликом ћаскања на друштвеној мрежи или телефонског разговора о сексуалним темама са особом коју су упознали преко друштвене мреже. Велики број испитаника 494 (80.7%) никада није о овим темама ћаскао или разговарао са особом коју су упознали преко друштвене мреже, 58 (9.5%) је разговарало 1-5 пута, више од пет пута је разговарао 21 (3.4%) испитаника/испитаница, увек то чини 13 (2.1%) испитаника/испитаница, без одговора је 26 (4.2%) упитника (табела 28).

Табела 28.

	Број	Проценат
никада	494	80.7 %
1-5 пута	58	9.5 %
више од 5 пута	21	3.4 %
увек	13	2.1 %
без одговора	26	4.2 %
укупно	612	100 %

О чувању приватности на друштвеној мрежи (енгл. privacy settings) већина испитаника/испитаница се изјаснила да су правила о чувању приватности ефикасна, али недовољна – 221 (36.1%) и да нису ефикасна у довољној мери да заштите кориснике – 175 (28.6%). Мањи број испитаника – 111 (18.1%) зна да ова правила постоје, али их никада не читају, док 38 (6.2%) не знају да ова правила постоје. Само 56 (9.2%) испитаника/испитаница се изјаснио да су правила о заштити приватности на друштвеним мрежама у потпуности ефикасна(табела 29).

Табела 29.

	Број	Проценат
не знам да ово постоји	38	6.2 %
знам да постоје, али их никада не цитам	111	18.1 %
мислим да нису ефикасна у довољној мери да заштите кориснике	175	28.6 %
мислим да су ефикасна, али недовољна	221	36.1 %
мислим да су у потпуности ефикасна	56	9.2 %
без одговора	11	1.8 %
укупно	612	100 %

Слично познавање правила о заштити приватности испитаници/ испитанице су показали и приликом одговора на питање о могућностима за пријављивања насиља или узнемиравања на друштвеној мрежи (report abuse buttons). Већина испитаника/испитаница, зна да постоје правила за

пријављивање насиља или узнемиравања на друштвеној мрежи, али их никада не читају – 195 (31.9%), нешто мањи број сматра да ова правила нису ефикасна у довољној мери да заштите кориснике – 143 (23.4%) или да су ефикасна, али недовољна – 137 (22.4%). Да су правила о пријављивању насиља или узнемиравања на друштвеној мрежи потпуно ефикасна проценило је само 33 испитаника/испитаница (5.4%), а 91 (14.9%) уопште не зна да постоји могућност за пријављивање насиља или узнемиравања на друштвеној мрежи (табела 30).

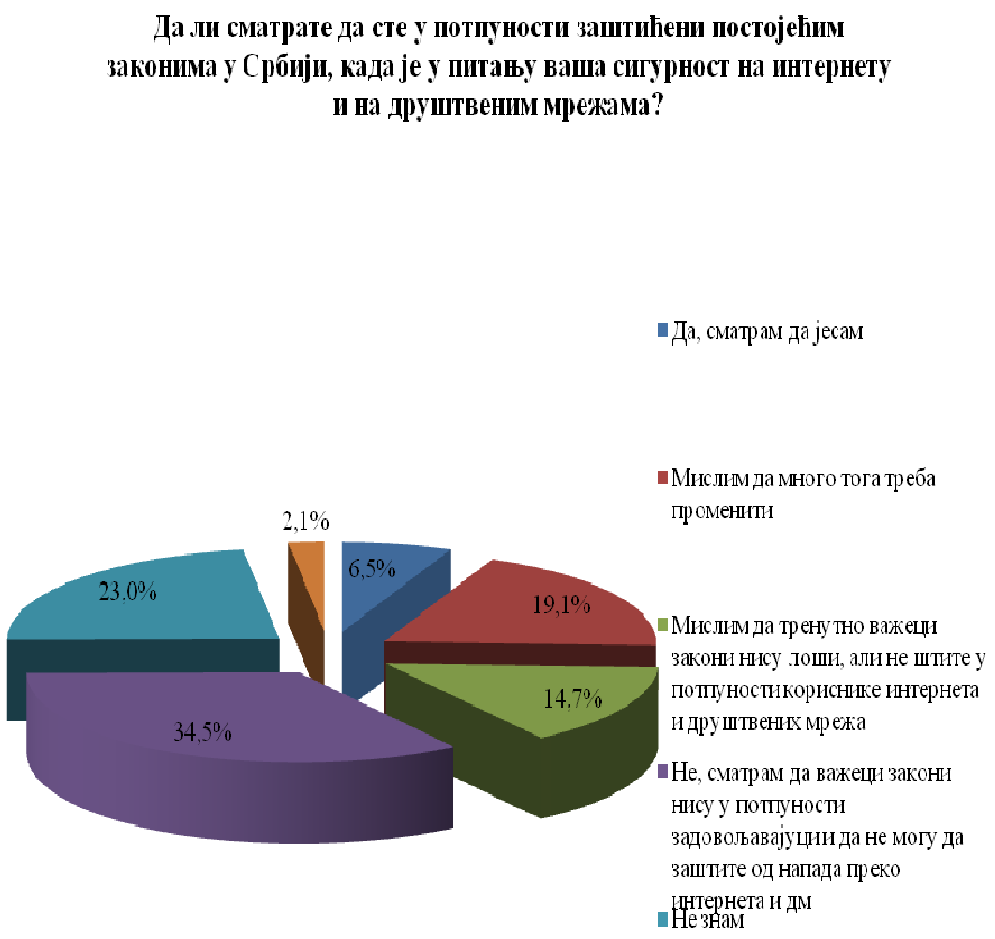
Табела 30.

	Број	*Проценат*
не знам да ово постоји	**91**	**14.9 %**
знам да постоје, али их никада не цитам	**195**	**31.9 %**
мислим да нису ефикасна у довољној мери да заштите кориснике	**143**	**23.4 %**
мислим да су ефикасна, али недовољна	**137**	**22.4 %**
мислим да су у потпуности ефикасна	**33**	**5.4 %**
без одговора	**13**	**2.1 %**
укупно	**612**	**100 %**

У погледу ефикасности законске заштите приватности на интернету и друштвеним мрежама у Србији, мали број испитаника/испитаница сматра да је заштићен постојећим законским одредбама – 40 (6.5%). Највећи број испитаника/испитаница – 211 (34.5%) сматра да закони нису у потпуности задовољавајући и да не могу да заштите кориснике интернета и друштвених мрежа и да много тога у законима треба променити – 117 (19.1%) или да закони нису лоши, али не штите у потпуности кориснике интернета и друштвених мрежа – 90 (14.7%). Чак 141 (23%) испитаника/испитаница не зна да постоје законске могућности за заштиту приватности, што показује да постоји потреба за потпунијим упознавањем корисника друштвенх мрежа и интернета са законским одредбама у овој области, али свакако и за одређеним законским променама када се ради о ефикаснијој заштити приватности (табела 31, графикон 19).

Табела 31.

	Број	*Проценат*
сматрам да јесам	**40**	**6.5 %**
много тога треба променити	**117**	**19.1 %**
закони нису лоши, али не штите у потпуности кориснике интернета и друштвених мрежа	**90**	**14.7 %**
закони нису у потпуности задовољавајући и не могу да заштите од напада преко интернета и друштвених мрежа	**211**	**34.5 %**
не знам	**141**	**23 %**
без одговора	**13**	**2.1 %**
укупно	**612**	**100 %**



Графикон 19.

Испитаници/испитанице су давали различите предлоге за повећање степена сигурности на друштвеним мрежама: одговарајућа законска регулатива

и већа активност државних органа; пријављивање злоупотреба и кажњавање извршилаца; едукација и повећање степена свести корисника; стављање на друштвене мреже што мање личних података; укидање друштвених мрежа; контрола малолетних лица и забрана коришћења друштвених мрежа лицима млађим од 18 година; контрола садржаја који се ставља на друштвену мрежу и бољи надзор администратора; повећање степена заштите приватности на друштвеној мрежи; некомуницирање са нпознатим особама и сл.

Поред наведених предлога, било је и оних који су се односили на мере које држава треба да предузме како би повећала сигурност корисника интернета и друштвених мрежа. Највећи број испитаника/испитаница се изјаснио да држава треба да донесе одговарајуће законе у овој области; затим да организује едукацију деце о опасностима које постоје на друштвеним мрежама; да побољша политику заштите деце од свих врста насиља преко интернета и друштвених мрежа; да научи кориснике друштвених мрежа да се сами заштите од напада којима су изложени; да организује и спроведе едукацију родитеља/старатеља, наставника/професора како би могли да уоче појаву интернет насиља међу децом/ученицима/студентима; да се забрани приступ одређеним интернет сајтовима; да се оснују центри који би поступали по пријавама за узнемиравање, вређање или праћење преко интернета и друштвених мрежа; укидање друштвених мрежа; ограничење коришћења интернета за млађе од 14 година; већа активност државних органа.

Испитаници су такође као препоруке којих треба да се придржавају сами корисници друштвених мрежа препознали забрану комуникације са особама које се лично не познају као и бољу проверу идентитета особа чији је кориснички профил са којим се ступа у комуникацију.

ЗАКЉУЧАК

1. Последица друштвене трансформације, мобилности и основних друштвених потреба да се људи међусобно повезују и резмењују информације, свакако је појава интернета као интреперсоналног медија и пројекције друштва у виртуелни простор. Путем интернета се могу успостављати нове везе међу људима, обнављати старе, могу се ширити вредности и норме, стварати нова култура, зарађивати новац, али, исто тако, може се манипулисати, злоупотребљавати, красти и варати.

Модерни свет интернета значајно је промењен настанком друштвених мрежа. Управо својом популарношћу и великим бројем корисника, друштвене мреже су створиле својеврстан „надзор" над свакодневним активностима људи, њиховим навикама, њиховим кретањем и дружењем. Уз све могућности које пружају интернет и друштвене мреже, небројено је велики број прилика за упознавање нових људи, стицање и развијање личних и професионалних односа, стварање различитих друштвених околности. У ранијем периоду виртуелни простор био је пун занимљивих и корисних информација, али је било веома мало могућности да овај простор буде интерактиван и да се у креирању података активно учествује. У данашње време друштвене мреже представљају начин за повезивање људи широм планете. Поред предности које интернет и друштвене мреже пружају, забележен је пораст злоупотреба везаних за вирутелни простор.

Компјутерски криминалитет припада новијим облицима криминалитета чије је појављивање резултат великог напретка технологије у области телекомуникација. Све већа употреба интернета и друштвених мрежа, као и коришћење компјутерске технике у свакодневном животу, представља огроман напредак са становишта друштвеног развоја. С друге стране, употребом компјутерске технике, посебно интернета и друштвених мрежа, велики број корисника изложен је свакодневној виктимизацији уколико подаци пренети путем друштвених мрежа буду злоупотребљени.

Са повећањем употребе интернета и броја корисника, повећавају се и могућности за злоупотребу интернет мреже. 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.

2. Почетак развоја виртуелних заједница на интернету почиње 1994. године када је покренут један од првих сајтова за друштвено умрежавање Geocities и 1995. године када су настали интернет портали Classmates.com и Theglobe.com. Према предмету интересовања њихових корисника, друштвене мреже је могуће класификовати у неколико основних група: друштвене мреже за кориснике општих интересовања (нпр. Facebook, Twitter, MySpace, Tagged, Meetup, Bebo, Multiply, Orkut, Skyrock, Badoo, StumbleUpon, Delicious, Foursquare, MyOpera, Kiwibox, Hi5); друштвене мреже за размену фотографија (нпр. Flickr, Fotki, Fotolog); друштвене мреже о различитим стиловима живота (нпр. Last.FM, Buzznet, ReverbNation, Cross.TV, WeRead, Flixter, GaiaOnline, BlackPlanet, Care2, CaringBridge, DeviantART, VampireFreaks, CafeMom, Ravelry, ASmallWorld); друштвене мреже посвећене путовањима (нпр. Wayn, CouchSurfing, TravBuddy); друштвене мреже прилагођене мобилним телефонима (нпр. Cellufun, MocoSpace, ItsMy); друштвене мреже на којима се размењују видео садржаји (нпр. Stickam, FunnyOrDie, YouTube); друштвене мреже које за циљ имају проналажење генерацијских школских пријатеља или рођака (нпр. Classmates, MyLife, MyHeritage, Geni); друштвене мреже које служе пословном повезивању и пословној комуникацији (нпр. LinkedIn, Focus, Viadeo, Ryze, XING); друштвене мреже за децу, тинејџере и младе (нпр. WeeWorld, Habbo,Tuenti); друштвене мреже за писање блогова (нпр. WordPress, Tumblr, Xanga, OpenDiary); међународне друштвене мреже каракретистичне за одређена географска подручја (нпр. у Азији - Mixi, QZone, Douban, Renren, у Русији - VKontakte, Odnoklassniki, у Пољској - NK, у Холандији - Hyves, у Латинској Америци - Sonico, у Сједињеним америчким државама - Friendster).

У Србији, прве друштвене мреже јављају се 2006. године, док током 2007. године почиње експанзија друштвених мрежа. Друштвена мрежа Myspace унела је новину у интернет могућност да свако креира своју сопствену страну

коју има на интернету. По први пут људи су добили могућност да направе свој налог, нешто што касније подсећа на мини блог, на коме могу да постављају и коментаришту шта год пожеле. Једна од најновијих домаћих друштвених мрежа Say Serbia (http://sayserbia.com/) појавила се 2013. године и интересантна је по томе што промовише Србију, њене историјске знаменитости, културу, религију, језик, националну кухињу и уметност, али такође садржи и утисак о Србији гледано очима странаца. Најчешће коришћене друштвене мреже у Србији су YouTube и Facebook.

Све друштвене мреже функционишу преко сервиса за друштвену мрежу, који представљају интернет сервис, који се најчешће јавља у облику платформе, прозора или веб-сајта, који омогућава да се људи из различитих крајева света повезују међусобно, склапају нова познанства или одржавају контакт са људима које већ познају. Функционисање друштвених мрежа је на више нивоа, почев од породице до нације; оне имају важну улогу приликом избора начина на који ће се неки проблем решавати и остваривања појединачних циљева.

Компјутери и компјутерска технологија се злоупотребљавају на различите начине, а што је виши степен развијености одређеног друштва, веће су могућности за појаву овог вида криминалитета и за постојање најразноврснијих његових облика, разноврснији су и софистицираније начини извршења, а учиниоци компетентнији и бројнији.

Криминалитет који се реализује помоћу компјутера може да има облик било ког од традиционалних видова криминалитета, ако што су крађе, утаје, проневере, док се подаци који се неовлашћено прибављају злоупотребом информационих система могу на различите начине користити за стицање противправне користи. У односу на штету или противправну користи који овај вид криминалитета може да нанесе друштву или до које може да доведе, материјални и људски ресурски који се улажу су минимални, време извршења је веома кратко што додатно отежава откривање и доказивање дела, а веома често извршилац се уопште физички не налази на месту извршења дела. Ефикасна превенција, откривање и покретање поступака против извршилаца кривичних дела додатно је отежана транснационалним карактером ове врсте криминалитета. Појавом Интернета као глобалне компјутерске комуникационе мреже и снажног утицаја који интернет има на развој модерног друштва, појавила се и нова врста извршилаца кривичног дела – „хакери" - који за свој

субјекат и објекат деловања имају интернет окружење, примењујући своје стечено знање које је по правилу знатно изнад знања којег имају органи откривања и гоњења.

3. 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.

Глобалне друштвене мреже допринеле су даљем развијању компјутерског криминалитета (интернет или cyber криминалитета), где се компјутерске мреже користе као циљ напада (нападају се сервиси, функције, садржаји који се налазе на мрежи), средство или алат (on line продаја сексуалних услуга, људских органа, жена и деце за проституцију, 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). Често се у оквиру компјутерског криминалитета у вези са друштвеним мрежама помиње интернет насиље. Жртве интернет насиља су најчешће младе особе активне на друштвеним мрежама. Интернет насиље (engl. „cyber bullying") се дефинише као свака комуникацијска активност рачунарском технологијом која се састоји у претњи, узнемиравању, омаловажавању, застрашивању или другом начину угрожавања и наношења штете појединцу.

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, као и идентификационе информације које се односе на посетиоца одређене интернет странице.

4. Са развојем информационих технологија, питање правне регулативе која би спречила и санкционисала компјутерски криминалитет добило је глобални значај. Поред земаља које су својим националним законодавством препознавале дела компјутерског криминалитета, бројне међународне организације и заједнице држава, попут Интерпола, Уједињених нација посредством Канцеларије Уједињених нација за борбу против дроге и криминала (UNODC), групе држава званих Г-8, Савета Европе, Организације америчких држава (OAS), Организације за економску сарадњу Азије и Пацифика (APEC), Организације за економску сарадњу и развој (OECD), земаља Комонвелта и Европске уније су се преко својих радних тела укључиле у борбу против компјутерског криминалитета како би предузеле напоре да се обезбеди хармонизација правне регулативе у овој области.

Савет Европе је био једна од првих међународних организација које су покренуле иницијативу за стварање правних претпоставки за сузбијање компјутерског криминалитета удруженим напорима више земаља: у области кривичног права, одржано је преко двадесет конвенција и усвојено је више од осамдесет препорука. Министарски савет састављен од министара иностраних послова држава чланица Савета Европе је 1989. године усвојио Препоруку о криминалитету везаном за рачунаре, којом су државе чланице позване да размотре увођење нових прописа који се односе на сузбијање и санкционисање компјутерског криминала. Препорука је садржала „листу минимума“ дела која морају у националним законодавствима бити препозната и инкриминисана као кривична дела, а коју чине: рачунарска злоупотреба; рачунарски фалсификат; оштећење рачунарских података или рачунарских програма; рачунарска саботажа; неовлашћени приступ рачунарском систему или мрежи кршењем мера безбедности; неовлашћено ометање техничким средствима улазне, излазне или комуникације унутар рачунарског система или мреже; неовлашћено копирање заштићеног рачунарског програма заштићеног законом; неовлашћено копирање законом заштићене топографије, полупроводничког производа или

бесправно комерцијално коришћење или увоз у те сврхе топографије или полупроводничког производа направљеног коришћењем топографије.

Препорука бр. 95 Савета Европе из 1995. године садржи 18 основних принципа борбе против компјутерског криминалитета и представља први покушај међународног дефинисања процедура проналажења и заплене, надгледања, прикупљања и оцене електронских доказа, енкрипције података као и сарадње држава на међународном плану и установљавања принципа међународне правне помоћи у области кривичних дела компјутерског криминалитета.

Европски регулаторни оквир за електронске комуникације, мреже и услуге представља основ за све националне законе земаља чланица ЕУ. Многе међународне организације су се, ослањајући на одредбе Конвенције Савета Европе о високотехнилошком криминалу из 2001. године донеле бројне препоруке у вези са пожељним изменама националних кривичноправних аконодавстава у области спречавања компјутерског криминалитета.

Конвенција Савета Европе о високотехнолошком криминалу бр. 185 из 2001. године са додатним протоколима свакако представља најзначајнији и најсвеобухватнији документ донет на међународном нивоу, чије су одредбе инкорпорисане касније у сва национална кривична права земаља потписница и земаља које су ратификовале овај документ, док су такође од великог значаја и Препорука савета Министара државама чланицама која се односи на заштиту људских права на друштвеним мрежама, директиве Европског парламента, Акциони план Европске комисије из 2009. Године за заштиту критичне информационе инфраструктуре, Стратегија сигурног информационог друштва Европе Савета Европе из 2007. године,[759] Конвенција Савета Европе о заштити појединаца од аутоматске обраде личних података CETS бр. 108. Конвенцију Савета Европе о високотехнолошком криминалу из 2001. године и додатни Протокол уз Конвенцију Република Србија је потписала 16. априла 2005. године у Хелсинкију и ратификовала марта 2009. године. Ови документи су послужили

[759] Резолуција Савета Европе 2007/C 68/01 - Стратегија сигурног информационог друштва Европе (Council Resolution 2007/C 68/01 - Strategy for a Secure Information Society in Europe – "Dialogue, partnership, and empowerment"), 2007, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007G0324%2801%29, претражено 09. 07. 2014. године

као основа за доношење одговарајућих националних правних прописа и стандарда и за формирање посебних државних органа специјализованих за борбу против компјутерског криминалитета уопште.

5. У оквиру законодавства Републике Србије од априла 2005. године донето је 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, Кривични законик Републике Србије, Закон о одговорности правних лица за кривична дела, Законик о кривичном поступку Републике Србије, Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима**,** Закон о одузимању имовине проистекле из кривичног дела**,** Закон о електронском потпису, Закон о заштити података о личности и Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине.

Према важећим законским прописима, насиље на интернету и на друштвеним мрежама се у Републици Србији може пријавити полицији, али и Окружном јавном тужилаштву у Београду – одељење за борбу против високотехнолошког криминала. Његовим радом руководи посебни тужилац за високотехнолошки криминал, кога поставља Републички јавни тужилац. При Окружном суду у Београду образовано је Веће за борбу против високотехнолошког криминала, кога чине судије овог суда које поседују посебна знања из области информационих технологија. У Министарству унутрашњх послова формиран је Одсек за сузбијање компјутерског криминала у оквиру Службе за борбу против организованог криминала Управе криминалистичке полиције (СБПОК).

Регулисање кривичноправне заштите од компјутерског криминалитета у националном законодавству извршено је прописивањем и санкционисањем *кривичних дела против безбедности рачунарских података* у оквиру Главе XXVII. Поред ових кривичних дела, КЗ РС у оквиру Главе XVIII која се односи на *кривична дела против полне слободе* прописује и следећа кривична дела која су директно у складу са чл. 9 Конвенције о високотехнолошком криминалу: приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл.185), и искоришћавање

рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (чл.185б). Кривични законик Републике Србије у оквиру Главе XX која се односи на *кривична дела против интелектуалне својине* прописује следећа кривична дела која су директно у складу са чл. 10 Конвенције о високотехнолошком кримиалу: повреда моралних права аутора и интерпретатора (чл.198), неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199), неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (чл. 200), повреда проналазачког права (чл.201) и неовлашћено коришћење туђег дизајна (чл.202).

Конвенција о високотехнолошком криминалу у чл. 7 ст. 1 као кривична дела у вези са компјутерима посебно прописује кажњивост кривичног дела фалсификовања које је у вези са компјутерима. Радње извршења овог кривичног дела састоје се сваком умишљајно учињеном делу уношења, мењања, брисања или прикривања компјутерских података који могу да доведу до стварања података који су неистинити, а у намери да се они сматрају за аутентичне и истините и да се са њима поступа као да су аутентични. Кривични законик Републике Србије не познаје овако дефинисано кривично дело фалсификовања које је у вези са компјутерима. Конвенција о високотехнолошком криминалу (чл. 7 ст. 2) такође прописује кажњивост кривичног дела преваре које је у вези са компјутерима. Радње извршења овог кривичног дела састоје се сваком умишљајно учињеном делу уношења, мењања, брисања или прикривања компјутерских података или ометању функционисања компјутерских система којим се другим лицима наноси већа имовинска штета, а у намери прибављања веће имовинске користи себи или другом лицу. У КЗ РС не постоји инкриминација кривичног дела преваре у вези са компјутерима.

Кривични законик Републике Србије у *Глави XIV – Кривична дела против слобода и права човека и грађанина* прописује кривично дело *повреда тајности писама и других пошиљки (чл.142)* под којим се санкционише и повреда тајности електронске поште. На овај начин је позитивним законодавством регулисано и прислушкивање и снимање причаоница, које је веома често на друштвеним мрежама. Међутим, код кривичног дела *неовлашћеног прислушкивања и снимања (чл.143),* не конкретизује се да ли се

ово дело односи и на комуникацију у виртуелном свету. С обзиром на учесталост надгледања комуникација на друштвеним мрежама и у причаоницама, неопходно је радњу овог дела проширити и на електронске комуникације а не само ограничити на разговор, изјаву или саопштење. Осим тога, код кривичних дела *неовлашћено фотографисање (чл.144) и неовлашћено објављивање и приказивање туђег списа, портрета или снимка (чл. 145)* при одређивању радње извршења кривичног дела не помињу се злоупотреба фотографија или неовлашћено објављивање података који су објављени на интернету или на друштвеним мрежама. Како повреда приватности може на више начина бити учињена у виртуелном простору, у оквиру кривичног дела *неовлашћено прикупљање личних података (чл.146)* треба санкционисати повреду приватности која је учињена у односу на податке, које су корисници објављивали на друштвеним мрежама у циљу неформалне комуникације са другим корисницима. Овакав проблем може да се јави и у случајевима када послодавци прикупљају податке о запосленима на основу њихових објава на друштвеним мрежама, (сајбер мобинг).

У Кривичном законику Републике Србије постоји велики број кривичних дела чије инкриминације треба прилагодити одредбама Конвенције о високотехнолошком криминалу. То се пре свега односи на кривична дела против слобода и права човека и грађанина, части и угледа, човечности и других добара заштићених међународним правом (расна и друга дискриминација, трговина људима), кривична дела против живота и тела (навођење на самоубиство и помагање у самоубиству), која могу бити извршена у виртуелном простору, код којих компјутер може представљати средство извршења, а коришћење одређених друштвених мрежа може представљати радњу извршења. Позитивно кривично законодавство не садржи одредбе којима би се корисници и друштвених мрежа заштитили од узнемиравања, сексуалног узнемиравања, сајбер мобинга вршњачког злостављања – булинга, лажног представљања, стварања лажног идентитета, интернет превара и сл. С обзиром на постојећу праксу, такође је неопходно код кривичног дела трговине људима предвидети као посебан облик овог кривичног дела коришћење друштвених мрежа за извршење свих наведених радњи.

Остали законски прописи који се односе на компјутерски криминалитет су: Закон о електронском потпису, Закон о посебним овлашћењима ради

ефикасне заштите права интелектуалне својине, Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, Закон о одузимању имовине проистекле из кривичног дела, Закон о заштити података о личности.

6. Како би савремени комуникациони системи могли у потпуности да испуне своју улогу, они морају да буду поуздани и да буду у служби и на располагању корисницима. Поверљивост информација које корисници деле у виртуелном простору са другима не сме да буде угрожена, а корисници морају да буду сигурни у идентитет пошиљаоца и у то да примљена информација мора да буде идентична послатој. Свако одступање од овог правила умањује поверење корисника и може да злоупотреби њихово право на приватност.

Приватност може да се дефинише као право појединца на заштиту од упада у његов лични живот или послове, живот његових чланова породице, било директно одређеним радњама или објављивањем личних информација. Право на приватност, као индивидуално право, може да се схвати као контрола, измена, управљање и брисање информација о себи самом онда када сама особа одлучи када, како и у комуникацији са ким то жели. У контексту друштвених мрежа, приватност и личне информације обухватају све податке које једна индивидуа објављује на свом профилу, а које подразумевају слике, коментаре, податке о кретању и дружењу и слично. Могућност злоупотребе права на приватност на друштвеним мрежама може да се сагледа кроз две конвептуалне категорије: друштвену злоупотребу или организациону злоупотребу права. Злоупотреба права на приватност у виртуелном свету може да се посматра у односу на пол корисника друштвених мрежа, односно на степен виктимизације мушкараца и жена који користе друштвене мреже. Према расположивим подацима, међу најчешћим корисницима друштвених мрежа у пет земаља Европе (Француска, Немачка, Италија, Шпаније и Велика Британија) издвајају се жене, свих старосних структура: на друштвеним мрежама су најчешће активне жене старости између 15 - 24 година које у просеку на друштвеним мрежама проводе око 8,4 сати месечно, а затим следе жене старости између 45 – 54 године са око 5,5 сати месечне активности на друштвеним мрежама. Сматра се да су жене више виктимизиране на друштвеним мрежама у односу на

мушкарце, што свакако зависи од степена патријархалне идеологије у једном друштву, друштвених улога полова, утицаја медија, заштите права жена и сл. Основни облици насиља и повреде приватности које жене могу да доживе на друштвеним мрежама су: изражавање мржње, ширење лажи, прогањање, монтажа фотографија, стварање лажних корисничких профила, хаковање корисничког профила, злостављање, виртуелно силовање, забрана да јавно искаже своје мишљење, називање погрдним именима, наставак породичног насиља, претње и уцене.

Упркос свакодневном развоју информационих технологија и нових појавних облика могућих злоупотреба, корисници интернета очекују да сваки информациони систем мора да одбије нападе који имају капацитете за његово угрожавање. Најчешћи начини непоштовања права на приватност на интернету су неовлашћен приступ, прикупљање и обрада личних података корисника, злоупотреба прикупљених података, пресретање послатих информација. Најчешће злоупотребе и повреде приватности коришћењем података који се налазе на друштвеној мрежи су крађа идентитета, прогањање, узнемиравање и сексуално узнемиравање, мобинг и манипулација личним подацима који се односе на запошљавање, злоупотреба фотографија на интернету и др. Поред наведених дела која су већ дуги низ година проучавана, једно од новијих дела које је све више актуелно је употреба говора мржње на друштвеним мрежама и на интернету уопште.

Постоје четири основна разлога због чега долази до могућности кршења права на приватност на друштвеним мрежама: *несавршеност корисника друштвене мреже, мане у програмима (софтверима) који се користена друштвеним мрежама, ненамерно одавање личних података и сукоб интереса.*

Најбољи начин за заштиту приватности свих интернет корисника је управо принцип контролисаног откривања личних информација. 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. Објављивање „постова" и личних информација на интернету може бити штетно за приватност појединца јер су информације (блогови, слике и интернет стране) које су једном објављене на интернету трајне. Чињеница је да се већина дела компјутерског криминалитета

реализује због незнања или недовољног знања руковања компјутерским системима. Неки од најчешћих узрока злоупотребе могу да буду и слабо програмирани компјутери и компјутерски системи, постављене шифре које су лаке за откривање и немају потребан степен сигурносне заштите, али и непостојање колективне свести о томе колико су заправо сви рачунарски и комуникациони системи рањиви и склони урушавању. Како би се овај сегмент проблема превазишао, на различитим нивоима (школе, интернет провајдери, медији, произвођачи и дистрибутери компјутерске опреме и програма и сл.) мора да се врши едукација корисника интернета како они сами не би правили грешке које би довеле до извршења неког од дела компјутерског криминалитета.

7. Истраживањем ставова корисника различитих друштвених мрежа о могућности злоупотребе права на приватност путем друштвених мрежа, коришћења/некоришћења одређене заштите, утврђивања могућности препознавања злоупотребе приватности путем друштвених мрежа, изложености виктимизацији на узорку 612 испитаника/испитаница долази се до следећих налаза:

- постоји велика учесталост активног коришћења друштвених мрежа јер се 93.6% испитаника/испитаница изјаснило да активно користи друштвене мреже, а само 6.4% корисника/корисница није активно на друштвеним мрежама;

- испитаници/испитанице не користе само једну већ више друштвених мрежа јер је већи проценат испитаника/испитаница активан је на две до пет друштвених мрежа 54.9% или на једној 37.9%, док је на више од пет друштвених мрежа активно 5.4%;

- највећи проценат испитаника/испитаница користи друштвену мрежу Facebook (23.3%), затим Youtube (19.8%), Skype (16%), Gmail Google Talk (9.8%);

- највише испитаника/испитаница користи друштвене мреже неколико пута у току дана 63.4% и једном дневно 19.9%, што показује да су испитаници/ испитанице у току дана веома активни на друштвеним мрежама

- највећи проценат испитаника/испитаника има приватни Facebook профил – 55.4%, али није занемарљив проценат оних који су се изјаснили да је

њихов Facebook профил могу да виде сви корисници друштвене мреже – 10.0% или да је њихов Facebook профил делимично приватан – 23.0%;

- правила о приватности само понекад чита 50.8% или уопште не чита ова правила 26.3%, што показује да овај облик примарне превентивне заштите испитаници/испитанице недовољно примењују. Само 21.2% испитаника/ испитаница увек чита правила о приватности на друштвеним мрежама;

- на Facebook профилу већине испитаника/испитаница пише колико имају година – 60.9% , знатно мање не наводи овај податак – 27.0%;

- исти компјутер на радном месту/школи/факултету приликом приступа интернету и друштвеним мрежама не користи 50.7% испитаника/испитаница, али је такође висок проценат оних који заједнички користе исти компјутер приликом приступа интернету и друштвеним мрежама – 48.2%;

- испитаници/испитанице у највећем проценту на друштвене мреже постављају слике/видео снимке на којима су са својим пријатељима – 59.6% или где су сами – 25.0%. Само 13.6% испитаника/испитаница не поставља своје слике или видео снимке на друштвене мреже, што показује да међу испитаницима/ испитаницама није довољо развијен систем самозаштите приватних података,

- 65.5% испитаника/испитаница никада не поставља слике или видео снимке других људи без сагласности оних чије се слике или видео снимци постављају на друштвене мреже, а само 3.9% испитаника/испитаница поставља на друштвене мреже слике и видео снимке других људи без њихове претходне сагласности;

- разлог за врло ретко постављање слика и видео снимака на друштвене мреже код већине испитаника/испитаника – 89.7% је њихово уверење да слике/ снимци могу да буду предмет злоупотребе. Много мање испитаника/ испитаница (9.0%) сматра да до злоупотребе слика/снимака неће доћи, што показује да су испитаници/испитанице у великој мери упознати са повећаним ризиком од злоупотребе приватности уколико слике/видео снимке поставе на друштвену мрежу коју користе;

- као могући видови злоупотребе слика/снимака стављених на друштвене мреже наведени су: крађа идентитета и преваре; манипулација сликом или подацима са друштвене мреже; коришћење слике у циљу сексуалне

експлоатације, порнографије и педофилије; сексуално узнемиравање; ради уцене, праћења, подсмеха итд.;

- приближан проценат испитаника/испитаница јесте (49.5%) и није (48.9%) у контакту преко друштвених мрежа са људима које лично не познају;

- „захтев за пријатељство" са непознатим људима на друштвеним мрежама не прихвата 49.9% испитаника/испитаница, увек или понекад прихвата 48.9%, што показује постојање велике неопрезности приликом прихватања „захтева за пријатељство" са непознатим људима на друштвеним мрежама;

- веома мали проценат испитаника/испитаница приликом коришћења друштвених мрежа суочио се са насиљем - 14.4%, знатно већи проценат испитаника/испитаница – 80.6% се није суочио са насиљем преко друштвених мрежа, најчешће се радило о о вербалном насиљу, затим о лажном профилу и/или злоупотреби електронске поште, хакованом Facebook профилу и сексуалном насиљу,

- испитаници/испитанице који су одговорили да су били сведоци насиља путем друштвених мрежа у највећем проценту су се изјаснили да нису реаговали – 52.1%. Они који су реаговали на сазнање о насиљу, учинили су то најчешће пријавом администратору мреже – 3.6%, блокирањем корисника – 2.3% и подношењем кривичне пријаве – 0.8%;

- 88.7% испитаника/испитаница нису никада били жртве прогањања или сексуалног узнемиравања преко друштвене мреже; 9.3% су једном или више пута били жртве прогањања или сексуалног узнемиравања,

- 87.1% испитаника/испитаница нису били жртве преваре или крађе преко друштвене мреже, само 5.4% је једном имало такво искуство, док је 5 или 0.8% више пута било жртва преваре или крађе преко друштвене мреже,

- разлози за насиље преко друштвене мреже, према мишљењу испитаника/испитаница може да буде: психички проблем или фрустрација (135 или 22.1%), већа слобода и храброст у виртуелном свету него у реалном јер постоји анонимност (50 или 8.2%), досада или забава (37 или 6%), превелика отвореност у комуникацији и непотребно стављање на друштвену мрежу много приватних података (11 или 1.8%), одсуство санкција (5 или 0.8%), доступност података о личности (5 или 0.8%);

- сигурним приликом коришћења друштвених мрежа осећа се 116 или 17.3% испитаника/испитаница, осећају се сигурним јер нису никада имали било какве непријатности на друштвеним мрежама 192 или 28.6%, осећају се сигурним јер увек када се деси проблем успевају да га сами реше 61 или 9.1%; углавном се осећају сигурним јер знају да постоје они који су имали лоша искуства 187 или 27.8%; углавном се осећају сигурним јер су имали лоша искуства из којих су научии да буду опрезни 22 или 3.3%;

- 92 или 13.7% испитаника/испитанице се никада не осећају сигурним приликом коришћења друштвених мрежа јер „опасност увек вреба“;

- најчешће злоупотребе приватности којима корисници могу да буду изложени приликом коришћења друштвених мрежа према мишљењу испитаника/ испитаница су: злоупотреба фотографије (362 или 17.0%); ширење говора мржње (342 или 16.1%); слање претњи (305 или 14.3%)); узнемиравање или малтретирање од стране пријатеља или познаника (280 или 13.2%); неовлашћено сликање или коришћење фотографије (278 или 13.1%); сексуално узнемиравање у причаоницама, преко друштвене мреже или електронске поште (196 или 9.2%); затрпавање нежељеним сексуалним садржајима (195 или 9.2%); прогањање и присиљавање на нежељену комуникацију преко интернета (169 или 7.9%),

- према искуству испитаника/испитаница најчешће претње којима су били изложени биле су: ширење говора мржње, које обухвата сваку комуникацију која омаловажава особу или групу на основу карактеристика, као што су раса, боја коже, етничка или национална припадност, пол, сексуална оријентација, религија (142 или 18.7%); затрпавање нежељеним сексуалним садржајима (110 или 14.5%); узнемиравање или малтретирање од стране пријатеља или познаника (67 или 8.8%); злоупотреба фотографије (65 или 8.6%); слање претњи (51 или 6.7%); неовлашћено сликање и коришћење фотографије (43 или 5.7%); прогањање или присиљавање на нежељену комуникацију преко интернета (39 или 5.1%) и сексуално узнемиравање у причаоницама, преко друштвене мрежа или електронске поште (33 или 4.3%);

- уколико се догоди нека од наведених претњи испитаници/испитанице се најчешће обраћају једном или неколицини пријатеља (355 или 29.3%), затим полицији (316 или 26.1%); родитељима/старатељима (284 или 23.5%), суду (103

или 8.5%); невладиној опрганизацији (80 или 6.6%); наставнику/професору (58 или 4.8%), док се 14 или 1.2% испитаника никоме не обраћа за помоћ;

- мере заштите које су предузели испитаници/испитанице у циљу превенирања злоупотребе приватности на друштвеним мрежама биле су различите: велики број испитаника/испитаница је обрисао некога са списка контаката – 524 или 85.6%, само 57 или 9.3% испитаника нису обрисали никога са списка контаката; своје име са слике коју је неко други поставио обрисало је 362 или 59.2% испитаника/испитаница, али приличан број испитаника/ испитаница – 208 или 34% то није учинио; коментар који је неко написао обрисало је 376 или 61.4% испитаника/испитаница, није обрисало 189 или 30.9% испитаника/испитаница, 447 или 73% је обрисало или изменио нешто што је објавио, 121 или 19.8% то није учинило;

- испитаници/испитанице пазе шта објављују: 66.2% испитаника/ испитаница није објавило нешто од чега би их касније било срамота; а 143 или 23.4% је то учинило;

- 437 или 71.4% испитаника/испитаница није учинило јавним свој профил на друштвеним мрежама, а 114 или 18.6% јесте;

- адресу становања на свом профилу није написало 505 или 82.5% испитаника/испитаница; 41 или 6.7% је то учинило;

- 398 или 65% испитаника/испитаница је блокирало неку особу да не може више да их контактира, 168 или 27.5% то није учинило;

- 326 или 53.3% испитаника/испитаница није обрисало или деактивирало свој профил на друштвеној мрежи, 232 или 37.9% је обрисало или деактивирало свој профил на друштвеној мрежи;

- нетачан податак у погледу узраста није дало 438 или 71.6% корисника/корисница, док је 116 или 19% је то учинило;

- непознато лице на листу контаката никада није додало 206 или 33.7%, 197 или 32.2% је то учинило 1-5 пута, више од 5 пута 152 или 24.8%; увек то чини 30 или 4.9%, значи, већи је проценат испитаника/испитаница 61,9% који су додавали непознато лице на листу контаката од оних који то нису чинили – 33.7%;

- са особом коју су упознали преко друштвене мреже никада телефоном није разговарало 65.7% испитаника/испитаница; 21.6% је то учинило 1-5 пута, 6.2% више од 5 пута; увек то чини 2% испитаника/испитаница,

- особу коју су упознали преко друштвене мреже никада није лично упознало 50.5%, 32.2% је то учинило 1-5 пута; више од 5 пута 10.3%, увек то чини 2.9% ;

- информације о имену и презимену преко друштвене мреже непознатим људима дало је чак 372 испитаника/испитаница (60.8%), што показује да су испитаници/испитанице прилично искрени у саопштавању својих података;

- информацију о томе где раде или студирају никада није дало је преко друштвених мрежа непознатим људима 46.9%; а увек то чини 46.4%;

- информацију о томе где обично иду са пријатељима никада није дало 75.5%, 17.6% увек даје ову информацију;

- 62.1% испитаника/испитаница никада није послало личне фотографије и фотографије блиских људи непознатим људима преко друштвених мрежа, 30.7% увек то чини;

- e-mail адресу није никада послало непознатим људима преко друштвених мрежа 68.1% испитаника/испитаница, али 25.2% увек то чини;

- информацију о адреси становања непознатим људима преко друштвених мрежа никада није дало 89.2% испитаника/испитаница, само 3.9% увек даје адресу становања;

- информацију о свом броју телефона никада није дало непознатим људима преко друштвених мрежа 79.4% испитаника/испитаница, али 12.9% увек даје информацију о свом броју телефона;

- 80.7% испитаника/испитаница никада није ћаскао на друштвеној мрежи или разговарао телефоном о сексуалним темама са особом коју су упознали преко друштвене мреже, 9.5% је разговарало 1-5 пута, више од пет пута је разговарало 3.4% испитаника/испитаница, увек то чини само 2.1% испитаника/испитаница.

- о ефикасности чувања приватности на друштвеној мрежи (privacy settings) испитаници/испитанице су се различито изјаснили: већина испитаника/испитаница се изјаснила да су правила о чувању приватности ефикасна, али недовољна – 36.1% или да нису ефикасна у довољној мери да заштите кориснике –28.6%; 18.1% зна да ова правила постоје, али их никада не

читају, 6.2% не знају да ова правила постоје, а само 9.2% сматра да су правила о заштити приватности на друштвеним мрежама у потпуности ефикасна;

- познавање правила о заштити приватности и могућностима заштите и пријављивања у случају постојања насиља или узнемиравања на друштвеној мрежи (report abuse buttons) није у подједнакој мери заступљено међу испитаницима/испитаницама: већина испитаника/испитаница 31.9% зна да постоје правила за пријављивање насиља или узнемиравања на друштвеној мрежи, али их никада не читају, нешто мањи проценат 23.4% сматра да ова правила нису ефикасна у довољној мери да заштите кориснике или да су ефикасна, али недовољна - 22.4%. Да су правила о пријављивању насиља или узнемиравања на друштвеној мрежи потпуно ефикасна проценило је само 5.4% испитаника/ испитаница, а 14.9% уопште не зна да постоји могућност за пријављивање насиља или узнемиравања на друштвеној мрежи,

- У погледу ефикасности законске заштите приватности на интернету и друштвеним мрежама у Србији, мали проценат - 6.5% испитаника/испитаница сматра да је заштићен постојећим законским одредбама; највећи проценат - 34.5%) сматра да закони нису у потпуности задовољавајући и да не могу да заштите кориснике интернета и друштвених мрежа; да много тога у законима треба променити – сматра 19.1%; да закони нису лоши, али не штите у потпуности кориснике интернета и друштвених мрежа сматра – 14.7%. Чак 23% испитаника/ испитаница не зна да постоје законске могућности за заштиту приватности, што показује да постоји потреба за потпунијим упознавањем корисника друштвенх мрежа и интернета са законским одредбама у овој области, али свакако и за одређеним законским променама када се ради о ефикаснијој заштити приватности;

- испитаници/испитанице су давали различите предлоге за повећање степена сигурности на друштвеним мрежама: одговарајућа законска регулатива и већа активност државних органа; пријављивање злоупотреба и кажњавање извршилаца; едукација и повећање степена свести корисника; стављање на друштвене мреже што мање личних података; укидање друштвених мрежа; контрола малолетних лица и забрана коришћења друштвених мрежа лицима млађим од 18 година; контрола садржаја који се ставља на друштвену мрежу и

бољи надзор администратора; повећање степена заштите приватности на друштвеној мрежи; некомуницирање са нпознатим особама и сл.

- предлози испитаника/испитаница који су се односили на мере које држава треба да предузме како би повећала сигурност корисника интернета и друштвених мрежа били су различити: држава треба да донесе одговарајуће законе у овој области; организује едукацију деце о опасностима које постоје на друштвеним мрежама; побољша политику заштите деце од свих врста насиља преко интернета и друштвених мрежа; научи кориснике друштвених мрежа да се сами заштите од напада којима су изложени; организује и спроведе едукацију родитеља/старатеља, наставника/професора како би могли да уоче појаву интернет насиља међу децом/ученицима/студентима; да се забрани приступ одређеним интернет сајтовима; да се оснују центри који би поступали по пријавама за узнемиравање, вређање или праћење преко интернета и друштвених мрежа; укидање друштвених мрежа; ограничење коришћења интернета за млађе од 14 година; већа активност државних органа. Испитаници су такође као препоруке којих треба да се придржавају сами корисници друштвених мрежа препознали забрану комуникације са особама које се лично не познају као и бољу проверу идентитета особа чији је кориснички профил са којим се ступа у комуникацију.

8. 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. Међутим, како је компјутерски криминалитет постао транснационални проблем чије последице сежу много даље од територије само једне земље, јасно је да механизми борбе против ове врсте криминалитета не смеју да се фокусирају само на измене националних кривичноправних законодавстава држава, већ на: предузимање одговарајућих техничких, структуралних и образовних мера, доношење одговарајућих међународних

техничких и правних инструмената и стварање свести о значају информација које могу да буду потенцијални ризик за настанак дела компјутерског криминалитета.

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.

ДОДАТАК - VARIA

1. Појмови везани за интернет комуникацију и компјутерски криминалитет

Овај речник објашњава значења појединих израза који су коришћени у докторској дисертацији, а може да се користи и као независан извор информација у смислу појашњења појмова који се везују за компјутерски криминалитет, виртуелни простор и друштвене мреже. Дефиниције су извучене из криминолошке литературе, домаћих и страних правних докумената из наведене области и криминолошких речника и текстова који су цитирани у литератури. Појмови и скраћенице су распоређени по азбучном реду. Када два или више појма имају исто значење, оно је дато поред термина који се чешће користи.

A

Аватар – дводимензиони или тродимензиони графички приказ корисника друштвене мреже; „изглед“ крисника друштвене мреже.

Администратор – лице које је одговорно за инсталацију софтвера, управљање и одржавање рачунара или рачунарске мреже; особа која је овлашћена да дизајнира и управља једном или више база података, при чему је одговорна за додавање нових података у ту базу, за модификвање и брисање података из базе, а често и за саму сигурност базе.

Адреса – низ знакова, слова, цифара и сигнала који је намењен за одређивање одредишта везе.

Ажурирање активности (енгл. News Feed) – активност којом корисник добија вести о променама у профилима корисника које има означене и прихваћене као пријатеље, о предстојећим важним догађајима и активностима, важним датумима и сл.

Анонимизер (енгл. Anonymizer) – сајт-посредник који сакрива или прикрива праву ИП адресу интернета корисника; преко ових сајтова је омогућено интернет корисницима да се укључе у различите интернет активности анонимно и без остављања трагова.

Апликација – део рачунарског програма преко кога је могуће било какво интерактивно деловање на друштвеним мрежама или у виртуелном простору.

Аутинг (енгл. Outing) - јавно показивање, постављање или прослеђивање туђих приватних слика, садржаја или личне комуникације оним особама којима те информације нису биле намењене којим се туђе личне информације чине јавним и доступним свима.

Б

Баг (енгл. Bugg) – програм уграђен у веб страницу или електронску пошту и углавном је невидљив посетиоцу странице или читаоцу и-мејла; омогућава проверавање да ли је особа посетила неку конкретну страницу или прочитала конкретну и-мејл поруку.

База података - колекција података организованих за брзо претраживање и приступ, која заједно са системом за администрацију, организовање и меморисање тих података чини систем базе података; подаци који су на неки логички начин повезани; организована колекција података који су складиштени и који се обрађују употребом рачунарских система.

Белешке (енгл. Notes) – писања корисника слична блоговима који сами корисници креирају и који могу да садрже текст и фотографије, док други корисници могу да их коментаришу или деле даље; начин стварања сопствених бележака о жељеним темама.

Беш борд (енгл. Bash Board) - виртуелна огласна табла на којој појединци могу да објављују, деле и шаљу све шта желе, при чему су ове објаве најчешће злонамерне и пуне изјава мржње која је усмерена против неке особе.

Бикон програм (енгл. Beacon program) – програм који је 2007. године Фејсбук почео да користи који је имао за задатак да пријављује интернет активности корисника разним другим корисницима и рекламним агенцијама, што је разбеснело милионе корисника ове друштвене мреже.

Блокирање - ускраћивање приступа појединих делова интернета или контаката са појединим интернет корисницима, при чему се на екрану прикаже порука о томе да је приступ страници одбијен.

Блог (енгл. Blog) - је скраћеница за веблог и представља часопис или билтен који се често ажурира и намењен за опште јавно читање у виртуелном простору; писано дело на интернету које представља мишљење, став или личност аутора или веб локације; интерактивно писан интернет дневник.

Блогер (енгл. Blogger) – особа која пише блогове.

Блогинг (енгл. Blogging) – писање и ажурирање блогова у виртуелном простору.

Боцкање (енгл. Poke) – симболичан гест на друштвеној мрежи Фејсбук, чачкање, изражавање позитивних емоција према некоме.

Булинг (енгл. Bullying) – поновљено и намерно узнемиравање некога од стране једне особе која је у некој врсти надмоћи; може да подразумева физичке претње или понашања, нападе, индиректне и суптилне облике агресије, оговарања, ширење гласина; најчешће се односи на младе и понашања која су везана за школу; често синоним за вршњачко насиље.

Булицид (енгл. Bullicide) - самоубиство које је директно или индиректно условљено малтретирањем које је жртва трпела преко интернета тј. услед интернет булинга.

В

Вандализам - малициозно понашање и агресија према околини; злонамерно и бесправно уништавање, загађивање или оштећивање туђег материјалног или интелектуалног власништва, без намере да се тиме стекне директна материјална корист за себе или друге.

Веб буба = Баг

Весело шамарање (енгл. Happy Slapping) - екстреман облик булинга где се физичко насиље према некоме снима на неки електронски уређај (нпр. мобилни телефон) како би се касније објавило на интернету или било послато некоме другом на гледање; снимање жртве без њеног пристанка и приморавање да уради нешто понижавајуће или против своје воље или док је злостављана, а затим и објављивање таквог снимка на друштвеној мрежи.

Виртуелни простор = Сајбер простор

Вређање на интернету = Флејминг

Вршњачко насиље - облик континуираног интрагенерацијског насиља које проистиче из одређеног односа међу вршњацима у основној и средњој школи, са циљем да се жртви нанесе штета (најчешће психичка), али примарно да се насилник прикаже доминантним у групи.

Вршњачко насиље на интернету (енгл. Cyber bullying) - сваки облик вршњачког насиља које се догађа у виртуелном свету а може се дефинисати као модерни облик вршњачког насиља који се реализује помоћу средстава масовне комуникације коју користе ученици, у првом реду преко интернета и мобилних телефона, у циљу понижавања, дискредитације, омаловажавања и на друге начине наношења штете другима; агресивно понашање изражено кроз негативне акције у намери да се друга особа повреди а кога одликују несразмера моћи између учесника и репетитивност; булинг који се врши преко интернета.

Г

Гејмер – особа зависна од играња видео игара.

Говор мржње – изјаве које застрашују, вређају или узнемиравају појединце или групе и/или изјаве које позивају на насиље, мржњу или дискриминацију појединаца или група; облици изражавања који шире, подстичу, промовишу или оправдавају мржњу засновану на нетрпељивости, укључујући и верску нетрпељивост; сви облици изражавања који шире, подстичу, промовишу или оправдавају међурасну мржњу, ксенофобију, антисемитизам или мржњу базирану на интолеранцији, укључујући и интолеранцију изражену кроз агресивни национализам или етноцентризам, дискриминацију или анимозитет према мањинама, мигрантима или људима имигрантског порекла; јавно изражавање дискриминаторских ставова путем графита, истицања порука или симбола дискриминаторне садржине, на јавним скуповима, спортским и другим јавним манифестацијама и догађајима и сл; употреба речи, израза и реченица који су увредљивог садржаја, а упућене су појединцу или групи због припадности одређеној раси, нацији, вери, идеологији, сексуалном опредељењу или другом личном својству, које стигматизују, етикетирају, клевећу, повређују или исмевају одређену друштвену групу и понижавају особу која припада тој групи; свака дискриминација, непосредна или посредна, по било ком основу, а

нарочито по основу расе, пола, националне припадности, друштвеног порекла, рођења, вероисповести, политичког или другог уверења, имовног стања, културе, језика, старости и психичког или физичког инвалидитета; изражавање идеја, информација и мишљења којима се подстиче дискриминација, мржња или насиље против лица или групе лица због њиховог личног својства, у јавним гласилима и другим публикацијама, на скуповима и местима доступним јавности, исписивањем и приказивањем порука или симбола и на други начин;

Груминг (engl.Grooming) - предузимање намерних радњи како би се придобила дечија пажња са сврхом развијања емоционалне везе са дететом, а све у циљу припреме за покушај сексуалног злостављања; предузимање низа предаторски мотивисаних поступака који насилнику омогућавају сексуалну злоупотребу малолетне особе.

Д

Давалац услуга - свако јавно или приватно лице које корисницима пружа своје услуге на пољу комуницирања путем компјутерских система; свако друго лице које обрађује или складишти компјутерске податке за рачун таквих комуникацијских услуга или за рачун корисника таквог сервиса.

Дечија порнографија - порнографски материјал који визуелно приказује малолетна лица која учествује у експлицитно сексуалном чину, лица по чијем се изгледу може закључити да је малолетно а које учествује у експлицитно сексуалном чину, реалистичке слике које представљају малолетна лица која учествују у експлицитно сексуалном чину; визуелна, чак и компјутерски генерисана представа детета у било каквим реалним или симулираним експлицитним сексуалним активностима или било какву сексуалну конотацију било ког дела тела детета за коју је јасно да је у сексуалне сврхе.

Дигитална репутација – мишљење или став који јавност поседује о некоме на основу његових/њених активности на друштвеној мрежи.

Дигитални доказ – знак, доказ, информација, податак који показује да се неко понашање догодило – може да буде дигитални снимак екрана или датотеке, траг о активностима на интернету, сачувани део садржаја неког документа и сл.; траг о томе да је нека особа противправно користила интернет, којим данима и у ком трајању, као и које је сајтове посећивала; податак на интернету који може да се

повеже са постојањем неког корисника, присуством на мрежи или његовим идентитетом.

Дигитално насиље - употреба електронске комуникације (интернета или друге дигиталне технологије) како би се нека друга особа заплашила или застрашила, како би јој се претило а све у циљу да се та особа осећа несигурно и емоционално рањива; агресиван, тенденциозан акт који група или појединац спроводи користећи електронска средства комуникације, у више наврата и током дужег периода против жртве која не може лако да се одбрани од оваквих напада.

Дисинг (енгл. Denigration, Dissing) - оговарање и клеветање, слање или постављање увредљивих и неистинитих информација о некоме са намером угрожавања репутације или пријатељских односа коју та особа има; прављење тзв. "електронске књиге утисака" (енгл.slam book) која има за циљ понижавање и исмевање других особа, најчешће школских вршњака.

Дистрибуција дечје порнографије - производња порнографског материјала са децом у циљу дистрибуције преко компјутерских система, нуђење или стављање на располагање дечије порнографије преко компјутерских система, дистрибуција или преношење дечије порнографије преко компјутерских система, добављање дечије порнографије преко компјутерских система за себе или за друга лица као и поседовање дечије порнографије у компјутерском систему или на медијима за смештање компјутерских података.

Догађаји (енгл. Events) – податак који омогућује пријатељима или познаницима организовање неког друштвеног догађаја.

Друштвена мрежа (енгл.Social network) - друштвена структура састављена од појединаца (или организација) који се називају „чворови", а који су повезани са једним или више специфичних типова међузависности, као што су вредности, визије, идеје, финансијски интереси, пријатељство, сродство, заједнички интерес, финансијска размена, недопадање, сексуални односи или односи поверења, знања или престижа; скуп интернет програма који служе да би се људи у комуникацији повезали са својим пријатељима, рођацима, колегама и клијентима, при чему њихови интереси могу да буду друштвени, пословни или мешовити; термин који се користи за облик људске интеракције при којој се путем постојећих познаника упознају нове особе ради остваривања друштвених

или пословних контаката; виртуелна заједница; скуп личних профила различитих људи; презентација на интернету која на једном месту спаја људе како би разменили мишљења, причали, поделили идеје и интересовања и стварали нове контакте; скуп индивидуа који деле своја заједничка интересовања; везе између „чворова“ - међусобно испреплетаних односа појединаца и организација; услуге које се базирају на коришћењу интернета помоћу којих појединци могу да стварају своје јавне или полујавне профиле унутар једног ограниченог система, стварају уређен списак корисника са којима контактирају и размењују информације и да претражују листе контаката оних са којима су повезани у систем; специфична интеракција друштвених и личних односа; интернет страница или апликација која омогућава њеним корисницима да међусобно комуницирају на тај начин што размењују информације, коментаре, поруке, слике и сл.; интернет заједница људи који су окупљени око заједничких интересовања користе компјутерске технологије да би међусобно комуницирали и размењивали информације, а све то преко интернет портала који омогућава њихову комуникацију.

Друштвено умрежавање (енг. Social networking) – радња која наглашава иницирање и покретање односа, најчешће између особа које се не познају.

Е

Е-маил = Електронска пошта

Е-приватност = Информацијска приватност

Експедитивно чување и заштита и делимично откривање података о преносу - адекватна заштите података у циљу да се обезбеди експедитивна конзервација података о преносу без обзира да ли је у преносу тог комуницирања учествовао један давалац услуга или више њих и да се надлежним органима може експедитивно открити она количина података о преносу која ће бити довољна за идентификацију даваоца услуга и путање којом је пренос извршен.

Експедитивно чување ускладиштених компјутерских података - експедитивно конзервисање и заштита одређених компјутерских података, укључујући ту и податке везане за пренос података, који су ускладиштени коришћењем компјутерских система, а посебно у случајевима када постоји

основана сумња да су компјутерски подаци нарочито изложени губљењу или изменама.

Експлоатација људских бића - обухвата експлоатацију проституције других лица или друге облике сексуалне експлоатације, принудни рад или службу, ропство или однос сличан ропству, сервитут или уклањање органа.

Електронска комуникациона мрежа – системи преноса и/или уређаји за комутацију и усмеравање и друге ресурсе, укључујући пасивне мрежне елементе, који омогућавају пренос сигнала помоћу жичних, радио, оптичких или других електромагнетских средстава, укључујући сателитске мреже, фиксне (са комутацијом кола и пакета, укључујући Интернет) и мобилне мреже, енергетске кабловске системе, у делу који се користи за пренос сигнала, мреже које се користе за дистрибуцију и емитовање медијских садржаја, без обзира на врсту података и информација који се преносе.

Електронска комуникациона мрежа за посебне намене – електронска комуникациона мрежа органа одбране и безбедности, органа државне управе надлежних за заштиту и спасавање, као и служби за хитне интервенције која се користи за намене за које су наведени органи основани, не користи се у комерцијалне сврхе и не даје се на коришћење трећим лицима

Електронска комуникациона услуга – услуга која се пружа уз накнаду, а састоји се у целини или претежно од преноса сигнала у електронским комуникационим мрежама, укључујући телекомуникационе услуге и услуге дистрибуције и емитовања медијских садржаја, али не обухвата услуге пружања медијских садржаја или обављања уредничке контроле над медијским садржајима који се преносе путем електронских комуникационих мрежа и услуга, нити обухвата услуге информационог друштва које се у целини или претежно не састоје од преноса сигнала електронским комуникационим мрежама.

Електронска порука – сваки текстуални, гласовни, звучни или сликовни запис послат преко јавне комуникационе мреже који се може похранити у мрежи или у терминалној опреми примаоца све док је прималац не преузме или јој приступи.

Електронска пошта – омогућава кориснику интернета да шаље и прима електронске поруке осталим корисницима интернета и од осталих корисника

интернета; употреба рачунарских и телекомуникационих система за пренос порука; порука послата са рачунара другом кориснику рачунара.

Електронски документ - документ у електронском облику који се користи у правним пословима и другим правним радњама, као и у управном, судском и другом поступку пред државним органом.

Електронски потпис - скуп података у електронском облику који су придружени или су логички повезани са електронским документом и који служе за идентификацију потписника.

З

Заштита података - скуп међусобно повезаних активности, метода, техника и норми којима се обвезбеђује приватност, сигурност, поверљивост и интегритет података од свих опасности које им прете.

Заштитни зид = Зид одбране

Збирка података - скуп података који се аутоматизовано или неаутоматизовано воде и доступни су по личном, предметном или другом основу, независно од начина на који су похрањени и места где се чувају.

Зид (енгл. Wall) - виртуална површина на профилу сваког корисника на којој особе с листе пријатеља могу написати поруку кориснику, с приказом датума и времена када је порука послата.

Зид одбране (заштитни зид, енгл. Firewall) – опрема или програм који брани или регулише долазеће и одлазеће податке и дозвољава приступ одређеним сајтовима или платформама друштвених мрежа; систем или група система којима се спроводи контрола приступа између две мреже на тај начин што може да блокира интернет саобраћај или да дозволи одвијање интернет комуникације; “прва линија одбране” између интерне интернет мреже и спољног света јер може бити тако конфигурисана да дозволи или не дозволи одређеним рачунарским операцијама да се изврше, да отежају или онемогуће нападачу на рачунарски систем да упадне и учини нешто рачунару или подацима који се налазе на рачунару или на интерној мрежи.

Злостављање преко интернета - употреба интернета или неког другог електронског начина комуникације како би се испољавало насилно,

малтретирајуће и нежељено понашање било од стране једне особе или од стране групе.

Злоупотреба друштвених мрежа - девијантно понашање које се састоји у нелегалном коришћењу друштвених мрежа противно правилима о заштити приватности, протоколима о електронској комуникацији, препорукама и утврђеним правилима која постоје на друштвеним мрежама, чиме се друштву и појединцима корисницима друштвених мрежа, али и онима који то нису, наноси материјална и нематеријална штета.

Злоупотреба права на приватност - сакупљање осетљивих личних података о некоме без његове сагласности и знања које има за циљ манипулацију тим подацима; упад у зону приватности (неовлашћеним приступом, прикупљањем и обрадом личних података), одавање или деловање на основу доступне информације, пресретање и уклапање информација (профилисање).

Злоупотреба уређаја пројектованих у сврху извршења неког од претходно наведених кривичних дела - производња, продаја, набављање ради употребе, увоз, дистрибуција и други видови стављања на располагање средстава, компјутерских програма, компјутерских лозинки, шифри за приступ и сличних података путем којих се може извршити неко од претходно наведених кривичних дела или се може приступити компјутерском систему као целини или неком његовом делу са намером да буде употребљен у сврху извршења неког од наведених кривичних дела; поседовање компјутерских програма, компјутерских лозинки, шифри за приступ и сличних података са намером да се употребе за извршење неког од наведених кривичних дела.

Злоупотреба фотографија на интернету - облик повреде приватности када се неовлашћено користе и приказују фотографије са налога корисника друштвених мрежа без њихове сагласности.

И

Идентификација – има за циљ да идентификује корисника и да потврди његов идентитет; најједноставнији начин за идентификацију јесте употреба лозинке приликом логовања корисника док су компликованији начини коришћење картица (SmartCard) или биометријских метода у комбинацији са лозинкама.

Издавање наредбе за предавање компјутерских података – радња када надлежни органи држава потписница могу да наређе сваком лицу на територији ове државе да мора да преда одређене компјутерске податке које поседује или који су под његовом контролом, а који су смештени на компјутерском систему или на медијуму за смештај компјутерских података као и да сваком даваоцу услуга који своје услуге врши на територији те државе нареди да мора да преда податке о претплатнику на те услуге које тај даваоц услуга поседује или над којима има контролу.

Имперсонација = Лажно представљање

Интернет - глобални комуникациони систем сачињен од великог броја међусобно повезаних аутономних система (мрежа), који размењују податке користећи заједнички скуп комуникационих протокола (ТЦП/ИП); мрежа компјутера који комуницирају међусобно са различитих локација широм света користећи за повезивање телефонске линије, сателитске везе, бежичне мреже и кабловске системе.

Интернет домен - текстуална ознака које повезује скуп рачунара, уређаја и сервиса на Интернету у јединствену административно-техничку целину; сваки домен на Интернету једнозначно је одређен глобално јединственим називом, а назив домена састоји се из низа алфанумеричких сегмената међусобно раздвојених тачкама.

Интернет насиље (engl. „Cyber bullying") - свака комуникацијска активност рачунарском технологијом која се састоји у претњи, узнемиравању, омаловажавању, застрашивању или другом начину угрожавања и наношења штете појединцу, употреба технологије како би се неко намерно и систематски малтретирао.

Интернет провајдер (енгл. ISP, Internet Service Provider) – компанија која појединцима и удружењима омогућава приступ интернету.

Интернет прогонитељ (енгл. Cyber stalker) - особа која користи интернет као оружје или средство за праћење, узнемиравање, слање претњи и стварање страха и стрепње код жртве, користећи софистициране тактике.

Интернет тероризам = сајбер тероризам

Информација - податак са одређеним значењем, знање које се може пренети на било који начин (писмом, аудио, визуелно, електронски).

Информација од јавног значаја - инфомација којом располаже орган јавне

власти, настала у раду или у вези са радом органа јавне власти, садржана у одређеном документу, а односи се на све оно о чему јавност има оправдан интерес да зна.

Информацијска приватност - захтев појединаца, група или институција да самостално одлуче када ће, како и које информације о себи уступити другима; правне вредности права појединаца у друштву развијених информацијских технологија.

Информацијска сигурност – могућност појединца да у условима постојања информацијског друштва одлучује када, коме, колико и како ће да саопшти личне податке, водећи рачуна о својим правима и потребама, као и о правима и потребама заједнице у којој живи.

Информациони криминалитет = Компјутерски криминалитет

ИП (IP) адреса – адреса интернет протокола, јединствена адреса додељена компјутерском уређају преко које се шаљу и примају подаци у циљу комуникације са другим рачунаром, који такође има своју посебну јединствену адресу.

ИП (IP) број - нумерички идентификатор, дефинисан у склопу ИП протокола, који на једнозначан начин омогућава адресирање уређаја повезаних на Интернет.

Искључивање (енгл. Exlusion, Ostracism) - индиректни метод сајбер насиља који се састоји у намерном искључивању неке особе из одређене виртуелне групе или заједнице (нпр. листа пријатеља, е-маил листа, соба за ћаскање и сл.).

Историја претраживача (енгл.History) – база прегледаваних интернет сајтова са одређеног рачунара у одређеном временском периоду.

ИТ криминалитет =Компјутерски криминалитет

К

Кетфишинг (енгл. Catfishing) – постављање фиктивног, лажног профила на некој од друштвених мрежа како би се намамила особа супротног пола ради покушаја стварања лажног емотивног односа.

Кеш меморија (енгл. Cache) - меморија малог капацитета која служи за запис података који се често користе; мала меморија велике брзине која побољшава преформансе рачунара.

Клерамболтов синдром (Clerambault's syndrome) - врста поремећаја понашања слична еротоманији која подразумева опсесивно и компулзивно понашање особе која искрено верује да је у интимној вези са жртвом.

Колачићи (енгл. Cookies) – злонамерни рачунарски програм; подаци сачувани на рачунару корисника који помажу аутоматском приступу веб страницама или другим облицима информација које су тражене на комплексним веб страницама.

Компјутер = Рачунар

Компјутерски криминал(итет) - облик криминалног понашања, једног или више лица у сајбер простору, у којем се рачунарске мреже појављују као средство, циљ, доказ или окружење извршеног кривичног дела; облик криминалног понашања, код кога се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривично-правном смислу релевантна последица; противправна повреда имовине код које се рачунарски подаци с предумишљајем мењају (манипулација рачунара), разарају (рачунарска саботажа), или се користе заједно са хардвером (крађа времена); сваки злочин који се деси у оквиру неког компјутерског система; врста криминалитета белог оковратника који је почињен у оквиру неког компјутерског система, при чему се компјутер користи као средство извршења овог пословног кривичног дела; облик криминалног понашања за који је неопходно знање из области компјутерских и информационих технологија.

Компјутерски подаци - свако излагање чињеница, података или концепата у облику који је погодан за њихову обраду у компјутерском систему, укључујући ту и одговарајући програм на основу којег компјутерски систем врши своју функцију.

Компјутерски систем - сваки уређај или групу међусобно повезаних или условљених уређаја, од којих један или више њих, у зависности од програма, врши аутоматску обраду података.

Комуникација – размена или преношење информација између одређеног броја особа путем јавно доступних електронских комуникационих услуга, изузев

информација које се преносе у склопу услуга јавног емитовања програма преко електронских комуникационих мрежа и које се не могу повезати са одређеним претплатником или корисником, односно примаоцем.

Корисник података - физичко или правно лице, односно орган власти, који је законом или по пристанку лица овлашћен да користи податке; физичко или правно лице које користи или захтева јавно доступну електронску комуникациону услугу.

Крађа идентитета - неовлашћено коришћење личних података (датум рођења, тренутно пребивалиште, број телефона, занимање, пријатељи, личне слике) који су постали јавно доступни; злоупотреба личних података који се налазе у виртуелном простору, најчешће ради стицања финанасијске добити; облик преваре којом се од корисника рачунара путем лажне поруке електронске поште или веб-сајта сазнају лични и финансијски подаци; радња која се догађа приликом преварног приступа информацијама о нечијем идентитету у циљу извршења крађе тих личних података без обзира да ли је особа чији се идентитет преузима жива или покојна.

Крекер (енгл. Cracker) – особа која се бави упадима и проваљивањем у компјутерске (рачунарске) мреже.

Л

Лажно представљање (енгл. Impersonation) - понашање када једна особа користи туђи идентитет, најчешће користећи шифру те особе како би приступила њеним налозима, а затим комуницирала на негативан или неприкладан начин са другима, стварајући утисак да изражава мишљење особе чији налог користи.

Листа пријатеља (енгл. List of Friends) –списак свих корисника друштвене мреже коју је неки конкретан корисник прихватио и означио као "пријатеље"; у зависности од безбедоносних подешавања сваког корисничког налога, овај податак могу видети или само пријатељи корисника или може да буде јаван и доступан свима који су на интернету; збирка имена или надимака корисника друштвене мреже који представљају пријатеље у оквиру тренутних порука или програма за ћаскање.

Личне информације о кориснику (енгл. Personal Information) – део који обухвата све информације које је корисник желео да наведе о себи, попут имена и презимена, занимања, старости, политичке и верске припадности, ствари које корисник воли, лична интересовања, чланства у различитим групама на друштвеној мрежи и сл.; све информације, подаци или комбинација података помоћу које се може идентификовати нека особа.

Локална интернет заједница – заједница коју чине сва правна и физичка лица која послују у области Интернета или користе Интернет услуге на подручју Републике Србије.

М

Малвер (злонамерни програм, енгл. Malware) - софтвер који се користи да би нанео штету рачунару, серверу, или мрежи рачунара, најчешће преко вируса, тројанца, спајвера и сл.; обухвата рачунарске вирусе, рачунарске црве, тројанце, спајвер и сличне нежељене злонамерне програме.

Малолетник - лице које је навршило четрнаест година, а није навршило осамнаест година.

Малолетно лице - лице које није навршило осамнаест година.

Мобинг (енгл. Workplace bullying)- одбојно и неетично опхођење које је, по једном утврђеном систему, усмерено од стране једне или више особа најчешће ка једној особи, подесној да буде изложена мобингу, која је стављена у позицију беспомоћности и без могућности да се одбрани и она се држи у тој позицији предузимањем поступака (активности) од стране мобера; неетички вид комуникације која се понавља и потиче од једне или више особа, систематски је усмерен против појединца у беспомоћној или незаштићеној позицији и која може да резултује пост-трауматским стресним поремећајима; специфично понашање на радном месту којим особа или група психички (морално) злоставља и понижава другу особу ради угрожавања њеног угледа, части, људског достојанства и интегритета све до елиминације са радног места; емотивни напад који почиње када појединац постане мета неучтивих и штетних понашања кроз алузије, гласине и јавно дискредитовање, непријатељско окружење у коме један појединац окупља друге да вољно или невољно, учествују у сталним злонамерним акцијама које за циљ имају трајно напуштање

радног места злостављане особе; специфичан систем који се састоји од пет доминантних фактора који су у међусобној интеракцији и који зависи од: психолошког профила и особина мобера; корпоративне климе и културе организације; психолошког профила и особина жртве; врсте конфликта који је окидач; и утицаја фактора изван организације попут вредности и норми ширег друштвеног окружења.

Мрежа (енгл. Network) – два или више рачунара повезаних тако да омогућавају међусобну комуникацију.

Надгледање и „затрпавање" електронске поште (енгл. Spam) - злоупотреба електронских система у сврху слања нежељених масовних порука без икаквог критеријума; нежељена порука добијена од стране неког кога корисник не познаје.

Н

Надимак (енгл. Nickname) – псеудоним којим се одређени корисник представља на друштвеној мрежи у комуникацији са другима.

Недозвољен приступ - намерно учињено бесправно приступање компјутерском систему или неком делу система, најчешће са намером прибављања компјутерских података или са неком другом противправном намером; бесправан приступ рачунарском систему или мрежи кршењем мера безбедности.

Недозвољено пресретање података - недозвољено пресретање преноса компјутерских података који нису јавне природе а који су усмерени ка одређеном компјутерском систему; електромагнетска емисија из компјутерских система којима се преносе такви подаци, уколико је дело учињено са намером и уз коришћење адекватних техничких уређаја.

Недозвољено саопштавање = Аутинг

Нежељена сексуална пажња - понашање које је нежељено и за које не постоји повод, а којим се експлицитно исказују сексуалне жеље или намере усмерене ка некој особи (нпр. сексуално експлицитни коменмтари и понашања, зурење у делове тела друге особе итд.).

Нежељена сексуална пажња у сајбер простору - непосредна, лична, вербална комуникација између злостављача и жртве која се одвија на интернету и манифестује се кроз поруке у којима се директно помиње секс или сексуалност (нпр. поруке које се односе на полне органе жртве, њен сексуални живот, њене интимне садржаје и сл.); инсинуације или провокације сексуалне природе; понашање које има за циљ да доведе до извесног сексуалног контакта између злостављача и жртве било у виртуелном или у личном контакту при чему жртва сматра овакав контакт као насилан, тј. не жели га.

Неовлашћени приступ - **Недозвољен приступ**

Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података - свако понашање којим се неко кршећи мере заштите неовлашћено укључи у рачунар или рачунарску мрежу или неовлашћено приступи електронској обради података, као и снимање или употреба података добијених на овај начин; понашање услед кога је дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице.

Неовлашћено искоришћавање ауторског дела или предмета сродног права - неовлашћено објављивање, снимање, умножавање, или на други начин јавно саопштавање у целини или делимично ауторског дела, интерпретације, фонограма, видеограма, емисије, рачунарског програма или базе података, као и стављање у промет и неовлашћено држање наведених предмета; производња, увоз, стављање у промет, продаја, давање у закуп, рекламирање у циљу продаје или давања у закуп или држања у комерцијалне сврхе уређаја или средства чија је основна или претежна намена уклањање, заобилажење или осујећивање технолошких мера намењених спречавању повреда ауторских и сродних права, или коришћење ових уређаја или средстава у циљу повреде ауторских или сродних права.

Неовлашћено копирање заштићеног рачунарског програма - бесправно копирање, дистрибуција или јавно објављивање рачунарских програма заштићених законом.

Неовлашћено копирање топографије - бесправно копирање законом заштићене топографије, полупроводничког производа или бесправно комерцијално коришћење или увоз у те сврхе топографије или полупроводничког производа направљеног коришћењем топографије.

Неовлашћено коришћење рачунара или рачунарске мреже - неовлашћено коришћење рачунарских услуга или рачунарске мреже у намери да се себи или другом прибави противправна имовинска корист.

Неовлашћено коришћење туђег дизајна - неовлашћена употреба туђег пријављеног, односно заштићеног дизајна производа; чињење доступним јавности предмета пријаве туђег дизајна пре него што је објављен на законом утврђен начин.

Неовлашћено ометање - бесправно ометање техничким средствима улазне, излазне или комуникације унутар рачунарског система или мреже.

Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима - стављање у промет, увоз, извоз, емитовање или на други начин јавно саопштавање ауторског дела или предмета сродноправне заштите са којег је електронска информација о правима неовлашћено уклоњена или измењена.

Нетикета (енгл. Netiquette, Network etiquette) – незванична правила прихваћеног понашања преко друштвених мрежа.

Нигеријска превара - улагање одређене своте новца у одређени „посао“, уз обећање да ће се као бенефит остварити знатно већа сума новца од уложене, слање електронске поруке која је тако осмишљена да изгледа као да је намерно послата примаоцу поруке, а почиње убеђивањем потенцијалне жртве преваре да учествује у подели новчаних фондова ако унапред уплати одређени износ који је неупоредиво мањи од оног износа који би требало да добије као корист од тог фонда.

Њ

Њуби (енгл. Newbie, скраћено newb, n00b, nob, noob, nub) – особа која је нова и неискусна у активностима на интернету, на друштвеним мрежама или у примени интернет технологија.

О

Обмањивање (енгл. Trickery) - нападач преваром или лукавством открива личне, најчешће тајне и понижавајуће информације о некој особи, а затим их

дели са другима; за разлику од недозвољеног саопштавања где је насилник у поседу одређених информација о некоме, код обмањивања он користи превару како би до поверљивих информација дошао.

Обрада података - свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин.

Обрађивач података о личности - физичко или правно лице, односно орган власти, коме руковалац на основу закона или уговора поверава одређене послове у вези са обрадом података о личности.

Одговорно лице - власник предузећа или другог субјекта привредног пословања или лице у предузећу, установи или другом субјекту којем је, с обзиром на његову функцију, уложена средства или на основу овлашћења, поверен одређени круг послова у управљању имовином, производњи или другој делатности или у вршењу надзора над њима или му је фактички поверено обављање појединих послова; службено лице кад су у питању кривична дела код којих је као извршилац означено одговорно лице; физичко лице којима је правно или фактички поверен одређени круг послова у правном лицу, овлашћено лице и лице које је овлашћено за поступање у име правног лица.

Означити = Таговати

Ометање података – мењање, брисање или оштећење рачунарских података; бесправно оштећење, брисање, кварење, мењање или прикривање компјутерских података које може за последицу да има настанак велике материјалне штете.

Ометање нормалног рада рачунара или рачунарског система - свако умишљајно ометање функционисања компјутерских система које је учињено уношењем, преношењем, оштећењем, брисањем, кварењем, мењањем или прикривањем компјутерских података и које у великој мери резултује ометањем нормалног рада рачунара или рачунарског система.

Online дезинхибиција - попуштање социјалних норми и правила у интернет комуникацији, која иначе поштујемо у интеракцији са људима уживо.

Оштећење рачунарских података или рачунарских програма - бесправно брисање, оштећивање, кварење или потискивање рачунарских података или рачунарских програма); неовлашћено брисање, измена, оштећење, прикривање или на било који други начин чињење неупотрбљивим рачунарских података или програма.

П

Поверљивост података – поверљиви подаци се не смеју открити од стране неауторизованих појединаца и других ентитета, или у неовлашћеним процесима.

Повреда моралних права аутора и интерпретатора - објављивање, стављање у промет примерака туђег ауторског дела или интерпретације, или на други начин јавно саопштавање туђег ауторског дела или интерпретације, а под својим именом или именом другог.

Повреда проналазачког права - неовлашћена производња, увоз, извоз, нуђење ради стављања у промет, стављање у промет, складиштење или коришћење у привредном промету производа или поступка који је заштићен патентом; неовлашћено објављивање или на други начин чињење доступним суштине туђег пријављеног проналаска пре него што је овај проналазак објављен на начин утврђен законом; неовлашћено подношење пријаве патента, ненавођење или лажно навођење имена проналазача.

Податак о личности - свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и сл.), по чијем налогу, у чије име, односно за чији рачун је информација похрањена, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и сл, односно посредно, путем увида у документ у којем је информација садржана и сл.), или без обзира на друго својство информације.

Податак о претплатнику - подразумева сваки податак који постоји у облику компјутерских података или у било ком другом облику а које поседује давалац

услуга и који се односе на претплатника на његове услуге, а на основу којих се може утврдити врста коришћених комуникацијских и техничких услуга као и временски период њиховог коришћења, идентитет претплатника; његова поштанска адреса или географска локација, број телефона и остали бројеви преко којих се може контактирати, листинг плаћања и подаци о плаћању, односно сви други подаци који су доступни кроз уговор о коришћењу комуникацијских и техничких услуга; као и свака информација о локацији на којој је комуникациона опрема постављена, до које се може доћи преко уговора о коришћењу комуникацијских и техничких услуга.

Покретна ствар – поред ствари које је физички могуће померити представља и свака произведена или сакупљена енергија за давање светлости, топлоте или кретања, телефонски импулс, као и рачунарски податак и рачунарски програм.

Порнографија из освете - поступак јавног објављивања сексуално експлицитних фотографија или видео снимака на Интернету, посебно на порнографским интернет страницама, без сагласности особе која је се налази на њима, са циљем да се она осрамоти и понизи.

Порука (енгл. Message) – приватна порука примљена од других корисника друштвене мреже, попут поруке електронске поште.

Пост на „зиду" корисниковог профила = Статус

Права интелектуалне својине – обухватају ауторска и сродна права, жиг, географске ознаке порекла, дизајн, патент, мали патент и топографија интегрисаних кола.

Прављење и уношење рачунарских вируса - свако умишљајно ометање функционисања компјутерских система које је учињено уношењем, преношењем, оштећењем, брисањем, кварењем, мењањем или прикривањем компјутерских података и које у великој мери резултује ометањем нормалног рада рачунара или рачунарског система.

Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података – подразумева поседовање, прављење, набавку, продају или давање другоме на употребу рачунара, рачунарских система, рачунарских података и програма ради извршења кривичног дела против безбедности рачунарских података; злоупотреба уређаја пројектованих у сврху извршења кривичних дела; производња, продаја, набављање ради употребе, увоз, дистрибуција и други видови стављања на

располагање средстава, компјутерских програма, компјутерских лозинки, шифри за приступ и сличних података путем којих се може извршити неко кривично дело или се може приступити компјутерском систему као целини или неком његовом делу са намером да буде употребљен у сврху извршења кривичних дела; поседовање компјутерских програма, компјутерских лозинки, шифри за приступ и сличних података са намером да се употребе за извршење кривичних дела.

Право на обавештеност – право да се истинито, потпуно и благовремено буде обавештаван о питањима од јавног значаја и да се, у складу са законом, има право на приступ подацима који су у поседу државних органа и организација којима су поверене јавна овлашћења.

Право на приватност - право појединаца да сами одређују када, како и у којој мери информација о њиховим комуникацијама треба и може да буде доступна другима; контролисање нечег што припада некој особи, њену аутономију и интегритет; право човека да контролише које ће детаљи његовог живота сазнати; одређивање личних ствари које ће се објавити и начин коришћења ових података; интерес који има изражену моралну вредност; морално или законско право појединца да буде заштићен од стране друштва или закона; право појединца на заштиту од упада у његов лични живот или послове, живот његових чланова породице, било директно одређеним радњама или објављивањем личних информација.

Пратити некога на друштвеној мрежи – прихватити захтев неког корисника друштвене мреже за контакт или повезивање на некој друштвеној мрежи.

Превара 419 = Нигеријска превара

Превара које су у вези са компјутерима - свако умишљајно учињено дело којим се уношењем, мењањем, брисањем или прикривањем компјутерских података или ометањем функционисања компјутерских система другим лицима наноси већа имовинска штета, а у намери прибављања веће имовинске користи себи или другом лицу; унос нетачног податка, пропуштање уношење тачног податка или на други начин прикривање или лажно приказивање податка и утицање на тај начин на резултат електронске обраде и преноса података, са намером да се себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинска штета; преварно понашање при чијем извршењу

лице које у намери прибављања противправне имовинске користи за себе и другога искористи једну или више компоненти Интернета (собе за ћаскање, веб странице или електронска пошта) да би се створили услови за лажно приказивање или прикривање чињеница којим би се неко лице довело у заблуду или у њој одржавало, да би то лице учинило нешто на штету своје или туђе имовине, тако што би на пример спровело неку финансијску трансакцију или пренело неке податке некој финансијској институцији која је мета напада.

Претраживање и заплена ускладиштених компјутерских података - давање овлашћење надлежним органима државе да на њеној територији могу да претражују или на сличан начин приступају компјутерском систему и компјутерским подацима, као и медијумима за смештај компјутерских података на којима би одређени компјутерски подаци могли да буду смештени.

Приватност - жеља неке особе да не буде узнемиравана; сигурност грађана да држава неће да се уплиће у њихове личе ствари; слобода од систематског посматрања и бележења активности и личних података; сложен појам који обухвата личну аутономију, демократску партиципацију, управљање сопственим идентитетом и друштвену координацију; контрола, измена, управљање и брисање информација о себи самом онда када сама особа одлучи када, како и у комуникацији са ким то жели; подаци које једна индивидуа објављује на свом профилу, а које подразумевају слике, коментаре, податке о кретању и дружењу и слично; стање брижљиво ограниченог приступа личним подацима.

Привремени интернет фајлови (енгл.Temporary internet files) – фајлови који се налазе на рачунару корисника где се чувају сви подаци о интернет странама и адресама које су посећиване; када сервер пошаље одређену страницу кориснику и следећи пут чим корисник захтева исту страну она се појављује заправо са простора на хард диску на који се адреса прекопирала (отвара се страница са рачунара корисника, а не директно са интернета); место где се чувају кеширани фајлови.

Пријатељ (енгл. Friend) – било ко прихвати или пошаље позив неком кориснику друштвене мреже да га дода на листу својих контаката; када корисник друштвене мреже неког дода за пријатеља то значи да у односу на релацију коју има са осталим контактима може ограничити видљивост података које је објавио и тако заштитити своју приватност.

Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију - продаја, приказивање или јавно излагање малолетном лицу или на други начин чињење доступним текстова, слика, аудио-визуелних или других предмета порнографске садржине, као и приказивање малолетном лицу порнографских садржаја и представа; искоришћавање малолетног лица за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу; поседовање, продаја, приказивање, јавно излагање или електронски или на други начин чињење доступним слика, аудио-визуелних или других предмета порнографске садржине који су настали искоришћавањем малолетног лица.

Прикупљање информација о промету података у моменту њиховог настајања – радња приликом које се надлежним органима државе потписнице дају овлашћења да на територији те државе примењујући техничка средства прикупљају или снимају податке које сматрају потребнима, као и да у сарадњи или под претњом примене санкције обавежу даваоца услуга да у оквиру његових техничких могућности на територији те државе ове податке прикупља или снима у реалном времену податке који се односе на пренос одређеног комуницирања које се преноси преко компјутерских система.

Приступ – давање на коришћење средстава или услуга другим операторима, под одређеним условима, било на ексклузивној или неексклузивној основи, ради пружања електронских комуникационих услуга, укључујући услуге путем којих се пружају услуге информационог друштва или медијски садржаји, што, између осталог, обухвата: приступ елементима мреже и припадајућим средствима, што може обухватати прикључење опреме путем фиксних или бежичних веза (нарочито приступ локалној петљи, те средствима и услугама неопходним за пружање услуга преко локалне петље), приступ физичкој инфраструктури (укључујући зградама, кабловској канализацији и антенским стубовима), приступ одговарајућим софтверским системима (укључујући системима за оперативну подршку), приступ информационим системима и базама података за наручивање, пружање, одржавање, обрачун и наплату услуга, приступ системима за превођење бројева или системима са истоветном функционалношћу, приступ фиксним и мобилним мрежама (посебно за потребе

роминга), приступ системима условног приступа, као и приступ виртуелним мрежним услугама.

Прогањање - трајнији облик злостављања према истој особи наметањем комуникације или контакта које та особа не жели; понављање извесних радњи које трају дуже време, попут: честих телефонских позива упућених жртви, слање жртви писама или поклона различите садржине, праћење и посматрање жртве, прелазак и боравак у простору који је у власништву жртве, ступање у контакт са породицом жртве, са њеним пријатељима или сарадницима; више пута поновљен начин понашања којим једна особа другој намеће нежељену комуникацију или сусрете, што има за последицу испољавање жртвиног страха да није безбедна; нежељена и злонамерна комуникацију, оштећење туђе имовине и физички или сексуални напад на неку особу, који је интензиван и нежељен и изазива страх.

Прогањање путем интернета (енгл. Cyber stalking) – више пута поновљено коришћење интернета, електронске поште или неког другог електронског начина комуникације у циљу нервирања, застрашивања, претњи или злостављања одређене особе; скуп понашања којима индивидуа, група људи или организација користи информационе и комуникационе технологије како би злостављала другу индивидуу, групу људи или организацију; примена претњи, лажних оптужби, крађе идентитета, крађе података, оштећење података и опреме, неовлашћено коришћење видео надзора и контроле, било какав вид агресије, коришћење одређене информације и сл. којом се некој особи наноси емоционални бол и несигурност; употреба интернета, електронске поште или било ког облика електронске комуникације којом се ствара криминални ниво застрашивања, злостављања и осећања страха код једне или код више жртава; прогањање путем свих средстава информационе и комуникационе технологије; упорно и циљано злостављање појединца путем електронских начина комуникације; употреба нових технологија у циљу прогањања неке особе.

Промет података - сви компјутерски подаци који су у вези са комуницирањем путем компјутерских система, а које генерише компјутерски систем и који чине део ланца комуницирања, у којима се садрже подаци о пореклу, одредишту, путањи, времену, датуму, велицини, трајању и врсти предметне услуге.

Профил(и) корисника - јединствене странице на којима сваки појединац може себе да представи другима у оној мери и на начин на који то жели; коришћење

одређене интернет странице како би се створиле јавне личне карте и стварали одређени односи са другим људима који имају приступ корисничком профилу; профил може такође да означава приказ биографије неке особе, њена интересовања, пријатеље, слике, контакт податке и све остале чињенице о одређеном кориснику друштвене мреже.

Р

Рачунар - сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке.

Рачунарска безбедност –доступност и исправно функционисање рачунара и рачунарског система.

Рачунарска злоупотреба - унос, измена, брисање или потискивање рачунарских података или програма, као и остале врсте мешања у обраду података које утичу на њен резултат, чиме се изазива економски или имовински губитак другог лица са намером да се стекне незаконита економска добит за себе или треће лице - алтернатива - са намером да се то лице лиши имовине на незаконит начин; било какав противправни инцидент који нека особа свесно почини а који је повезан са компјутерским технологијама услед кога жртва трпи или може да претрпи неки губитак.

Рачунарска мрежа - скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући и преносећи податке.

Рачунарска превара = Превара које су у вези са компјутерима

Рачунарска саботажа - унос, измена, брисање или потискивање рачунарских података или рачунарских програма или мешање у рачунарски систем са намером да се онемогући функционисање рачунара или телекомуникационог система; уношење, уништавање, брисање, измена, оштећење, прикривање или на други начин чињење неупотребљивим рачунарског податка или програма или уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте.

Рачунарски вирус - рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података; компјутерски програм који се сам умножава и шири од једног рачунара на други; појам који обухвата различите врсте злонамерних програма; вирусе треба разликовати од црва, спајвера и тројанаца јер су технички другачији – црви злоупотребљајану слабост одбрамбеног сигурносног система рачунара да би се аутоматски ширили на друге рачунаре кроз мрежу, спајвер нема могућност да се самостално шири унутар једог рачунара и на друге рачунаре преко мреже док тројанци су програми који се наизглед чине безазленим али у себи крију злонамерне функције.

Рачунарски податак - свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију; податак који се уноси или користи ради несметаног рада рачунара, електронске обраде или који се преносе рачунарским мрежама.

Рачунарски програм - уређени скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара.

Рачунарски систем - сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података.

Рачунарски фалсификат - унос, измена, брисање или потискивање рачунарских података или програма, као и остале врсте мешања у обраду података на рачунару или под условима, предвиђеним домаћим законом, који би представљао дело фалсификата да је почињен у односу на класичан предмет таквог кривичног дела.

Рекламирање прилагођено понашању корисника (енгл. „Behavioural Advertising“) - посебна врста рекламирања на интернету којом се посматра кретање корисника на интернету и који се садржају претражују како би им се приказао одређени рекламни материјал уз помоћ реклама (тзв.банера).

Родно засновано злостављање – понашање које се састоји од давања непожељних вербалних и визуелних коментара и примедби које вређају појединаца због њиховог пола/рода или који има за циљ да изазове негативне

емоције (нпр. постављање порнографских слика у јавности или на местима где се то сматра увредљивим, причање шовинистичких вицева, примедбе које су родно деградирајуће и сл.).

Родно засновано злостављање у сајбер простору - слање увредљивих порука сексуалног карактера које су понижавајуће за жртву (активно вербално злостављање); намерно слање еротских или порнографских садржаја путем електронских комуникација или њихово објављивање на друштвеној мрежи или у виртуелном простору (активно графичко злостављање); објављивање слика или видео снимака увредљивог садржаја на различите интернет портале, на којима жртва и не претпоставља да овакви садржаји могу да се налазе (пасивно графичко злостављање).

Руковалац података - физичко или правно лице, односно орган власти који обрађује податке о личности.

С

Сајбер - све што се односи на или укључује рачунаре или рачунарске мреже; подразумева не само хардвер, софтвер и информационе системе, већ и људе и друштвену интеракцију у оквиру ових мрежа; представља системе и сервисе повезане било директно или индиректно на Интернет, телекомуникационе системе или компјутерске мреже; то је комплексно окружење које резултира из интеракције људи, софтвера и сервиса на интернету и то посредством технолошких уређаја и мрежа са њима повезаним који не постоји у било ком физичком облику.

Сајбер вандализам - уништавање и оштећивање интелектуалног власништва у виртуалном простору, без намере да се стекне материјална корист.

Сајбер криминал = Компјутерски криминал

Сајбер криминалитет = Компјутерски криминалитет

Сајбер криминологија (енгл. Cyber cryminology) –студија о узрочности криминалитета који се појављује у сајбер (cyber) простору и његовог утицаја на дешавања у физичком простору.

Сајбер мобинг – манипулација личним подацима запослених који се налазе на интернету од стране послодаваца.

Сајбер претња – електронски исказана тврдња (претња) којом се некоме намеће брига и стрепња да њен аутор има намеру да некога повреди или над њим изврши насиље.

Сајбер прогањање - Прогањање путем интернета

Сајбер простор (енгл. Cyber space) – простор у коме се одвијају активности на интернету; виртуелни, невидљиви простор који је неограничен, базиран на технологији тј.рачунарским мрежама; нематеријални простор који је заснован на информационо-комуникационој технологији*;* глобална заједница где живе рачунарски повезане индивидуе и групе.

Сајбер секс – симулација сексуалних односа на даљину путим информационо-комуникационих технологија.

Сајбер тероризам – смишљени, политички мотивисани напади на компјутерске системе и програме, као и на податке којима треба да се изазову насиље и страх код цивилних мета; употреба рачунара у функцији оружја или мете, од стране политички мотивисаних међународних или пара-националних група или појединаца који прете или спроводе насиље како би утицали на јавност и на званичне владе да промене свој начин вођења политике; коришћење модерне технологије како би се стратешки створиле слабе тачке неког система које ће затим искористити за постизања терористичких циљева; насилан облик компјутерског криминалитета, који је извршен, планиран или координисан у виртуелном простору и помоћу рачунарских мрежа; криминални акт у виртуелоном простору који има за циљ да се заплаши влада или њени грађани у циљу остварења политичких циљева; криминални акт у виртуелоном простору који има за циљ да се заплаши влада или њени грађани у циљу остварења политичких циљева; криминална радња извршена употребом рачунара и телекомуникационе опреме, која за последицу има насиље, уништење и стварање страха, збуњености и несигурности код народа, а за циљ има утицање на владу те државе како би се спровела одговарајућа политичка, друштвена или идеолошка промена или циљ; посебна врста терористичких напада усмерених ка рачунарским системима и мрежама у намери остваривања политичких циљева.

Секстинг (енгл. Sexting) - слање сексуално провокативних, сексуално обојених фотографија и експлицитних слика, порука и електронске поште коришћењем телефона или рачунара.

Сексуална експлоатација деце преко интернета - било какав сексуално оријентисани контакт преко интернета, производња, прикупљање и дистрибуција дечје порнографије; нежељено излагање деце порнографији; сексуални туризам који се односи циљано на децу и дечију проституцију; свака врста интернет експлоатације деце која на директан или индиректан начин доводи до сексуалног контакта између одраслих и деце.

Сексуална принуда преко интернета - употреба различитих средстава доступних на друштвеној мрежи или интернету уопште у циљу успостављања сексуалног контакта са жртвом која овај акт сматра нежељеним и насилним.

Сексуално задовољење - вршење физичког и/или психичког притиска на неку особу како би се она натерала на „сексуалну сарадњу“ (нпр. нежељено физичко додиривање, нуђење новца за нежељени сексуални однос, претња у циљу иостваривања сексуалног односа и сл.).

Сексуално узнемиравање (енгл. Sexual harrasment) - насилнички чин усмерен против особе који подразумева различита понашања од сексистичке дискриминације до сексуалне агресије.

Сервис за друштвену мрежу - интернет услуга која омогућава појединцима да направе јавни или полу-јавни профил у оквиру једног ограниченог система, контролишу листу других корисника са којима су повезани, и контролишу односе које имају са корисницима унутар мреже; интернет сервис који се најчешће јавља у облику платформе, прозора или веб-сајта, који омогућава да се људи из различитих крајева света повезују међусобно, склапају нова познанства или одржавају контакт са људима које већ познају.

Сигурност података – обезбеђење података од случајног или намерног откривања неовлашћеним корисницима или заштиту од неовлашћеног мењања, брисања и коришћења од стране овлашћених корисника.

Скиминг (енгл. Skimming) - превара платним или кредитним картицама, која за основни циљ има крађу идентитета власника картице снимањем магнетног записа са картице.

Скам (енгл. Scam) – врсте превара и трикова који се шаљу путем електронске поште, најчешће у виду лажних лутрија, фишинг порука, нигеријских превара и сл.

Службено лице - лице које у државном органу врши службене дужности; изабрано, именовано или постављено лице у државном органу, органу локалне самоуправе или лице које стално или повремено врши службене дужности или службене функције у тим органима; лице у установи, предузећу или другом субјекту, којем је поверено вршење јавних овлашћења, које одлучује о правима, обавезама или интересима физичких или правних лица или о јавном интересу; лице којем је фактички поверено вршење појединих службених дужности или послова; војно лице.

Соба за ћаскање (енлг. Chat Room) – виртурелни простор на мрежи, „соба“, где групе људио шаљу, пишу и примају поруке које се свима исписују у једном „прозору“ на екрану; виртуелни простор који омогућаја комуникацију и до више стотина људи у исто време где се поруке приказују одмах како се куцају, у реалном времену; конверзација у којој су надимци или имена свих учесника исписана на једној страни екрана како би олакшало комуникацију.

Социјална мрежа = Друштвена мрежа

Социјални инжињеринг (енгл. Social Engineering) - акт манипулације којим се људи наводе да одају поверљиве информације о себи, заснива се на ометању пажње одређеног лица у циљу прикупљања информација које оно иначе не би одало, а како би се ти подаци касније злоупотребили (ради одавања корисничких имена, лозинки или, нпр. података о платним картицама); може да има више форми у којима се појављује нпр. електронске поруке које се јављају као веома важне вести, различите честитке, обавештења о добитку на лутрији и сл.

Спајвер (енгл. Spyware) - део софтвера који добија информације са корисниковог рачунара без његове сагласности.

Спам (енгл. Spam) = Надгледање и „затрпавање” електронске поште

Спречавање и ограничавање приступа јавној рачунарској мрежи - неовлашћено спречавање или ометање приступа јавној рачунарској мрежи.

Спуфинг (енгл. Spoofing) – фалсификовање података релевантних за осигурање поверљивости на Интернету, неауторизован приступ некој интернет локацији како би се дошло до других важних података.

Статус (енгл. Wall post) – јавне поруке које је неки корисник примио од других корисника или апликација које корисни на друштвеној мрежи, могу да представљају и различите врсте обавештења; они најчешће изражавају како се корисник осећа, шта ради, шта мисли и са ким је у одређеном тренутку.

Стеганографија - научна дисциплина која се бави прикривеном разменом информација и методима скривања тајних порука унутар медија безазленог садржаја.

Страно службено лице - лице које је члан законодавног, извршног или судског органа стране државе, јавни функционер или службеник међународне организације и њених органа, судија и други функционер међународног суда.

Т

Таговати (енгл. Tag) – ставити нечије име на слику или белешку која је објављена.

Твит (енгл. Tweet) – порука не дужа од 140 карактера (знакова) која се објављује на друштвеној мрежи Твитер.

Трговина људима - врбовање, превожење, пребацивање, скривање и примање лица, путем претње силом или употребом силе или других облика присиле, отмице, преваре, обмане, злоупотребе овлашћења или тешког положаја или давања или примања новца или користи да би се добио пристанак лица које има контролу над другим лицем, у циљу експлоатације; свако силом или претњом, довођењем у заблуду или одржавањем у заблуди, злоупотребом овлашћења, поверења, односа зависности, тешких прилика другог, задржавањем личних исправа или давањем или примањем новца или друге користи, врбовање, превожење, пребацивање, предавање, продају, куповање, посредовање у продаји, сакривање или држање другог лица, а у циљу експлоатације његовог рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употреба у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима.

Тројанац (енгл. Malware, Trojan horse, Trojans) - програм који изгледа као да је користан али заправо истовремено врши и оштећивање рачунара; у рачунар тајно убачена инструкција за понашање рачунарских програма која резултује извршењем одређених радњи које корисник не би свесно и намерно учинио; програм који изгледа као легалан али извршава неку бесправну активност, може да има за циљ да открива корисничке лозинке, да систем учини рањивим или

једноставно да уништи податке или програме који се налазе на рачунару; програм сличан рачунарском вирусу уз разлику да он не умножава самог себе и не шири се као вирус, већ се обично "настане" у рачунару правећи му штету и дозвољавајући да неко други а не корисник управља рачунаром са даљине.

Ћ

Ћаскање (енгл. Chat) – интернет конверзација у реалном времену између два или више корисника који користе своје интернет надимке уместо личних имена, служи за слање и писање порука као и вођење различитих дискусија.

У

Узнемиравање посредством интернет мреже (енгл. Cyber harrasment) - слање претњи и порука које имају за циљ да узнемире или повреде особу којој су послате; коришћење интернета или неког другог електронског средства како би се уходила нека особа, група или организација; намерно понашање које је претеће и узнемиравајуће и које има тенденцију да се понавља; понављано слање увредљивих, провокативних, грубих и непријатељских порука једној особи или групи.

Учинилац кривичног дела – подразумева извршиоца, саизвршиоца, подстрекача и помагача у извршењу кривичног дела.

Ф

Фајл (енгл. File) - скуп података или програма који су негде сачувани и складиштени; све што је трајно сачувано у рачунарском систему под посебним именом; низ бајтова које оперативни систем препознаје; дигитални подаци који имају своје име и формат; скуп података који чине целину.

Фалсификовање које је у вези са компјутерима - свако умишљајно учињено дело уношења, мењања, брисања или прикривања компјутерских података који могу да доведу до стварања података који су неистинити, а у намери да се они сматрају за аутентичне и истините и да се са њима поступа као да су аутентични.

Фарминг (енгл. Pharming) – облик крађе идентитета путем злонамерног софтвера; покушај хакера да преусмери електронску комуникацију и размену података са легитимне веб странице на потпуно другачију интернет адресу променом фајлова на компјутеру корисника - жртве или искоришћавањем недостатака на серверу који се користи, у рачунар се учитава вирус или тројанац који краде информације корисника па је могуће креирати лажне идентификације, фалсификовати документа, чекове или кредитне картице.

Фид (енгл. Feed) – формат података који омогућава корисницима често ажурирање садржаја, користи се и код интернет преноса који се преносе уживо.

Физичко лице - човек на кога се односи податак, чији је идентитет одређен или одредив на основу личног имена, јединственог матичног броја грађана, адресног кода или другог обележја његовог физичког, психолошког, духовног, економског, културног или друштвеног идентитета.

Филтеринг = Филтрирање

Филтрирање (енгл. Filtering) – компјутерска радња којом се забрањује приступ одређеним интернет сајтовима или друштвеним мрежама.

Фишинг (енг. Phishing) – облик крађе идентитета путем електронске поште; чин слања е-маил поруке кориснику у којој се наводи да поруку шаље легитимно правно лице или овлашћена особа тражећи личне податке и приватне информације при чему су наводи у поруци лажни, а уколико прималац напише податке који се траже, они ће касније бити искоришћени за крађу идентитета; кривично дело прибављања заштићених информација корисника (корисничко име, лозинка, број кредитне картице) које настаје „преузимањем“ идентитета корисника у неком облику електронске комуникације при чему електронска пошта усмерава корисника да посети веб сајт где се тражи да се лични подаци (лозинке и кредитне картице, социјално осигурање, бројеви банковних рачуна) које легитимна организација већ има, ажурирају а веб сајт који се наводи је лажан и подешен само за крађу информација корисника.

Флејминг (енгл. Flaming) - кратка и жустра расправу између две или више особа путем било које комуникационе технологије, која се састоји у намерном постављању или слању електронских порука са увредљивим, злобним, понижавајућим или вулгарним садржајима.

Фотографије (енгл. Photos) – слике које корисници друштвених мрежа објављују по својој вољи на свом или туђем профилу и на њима могу да означе све особе које се налазе на њима; слике о којима, у зависности од безбедоносних подешавања, корисници друштвене мреже могу да постављају коментаре.

Френдинг (енгл. Friending) – захтевање од једног корисника друштвене мреже да се повеже са другим корисником друштвене мреже и да постану "пријатељи" на друштвеној мрежи, израз се повезује са друштвеном мрежом Фејсбук.

X

Хакер - особа, компјутерска „мудрица", која поседује знања о компјутерима, способности и жељу за истраживањем и унапређивањем компјутерских система; особа која детаљно испитује програмске системе и који тежи да максимално прошири своје знање у овом домену, као и особа која на илегални начин упада у компјутерске системе; особа која поседује знања, способности и жељу за потпуним истраживањем система; особа која провађује у компјутерске системе и бесплатно их користи; вандал који неовлашћено добија приступ компјутерским системима и уништава податке и програме који се налазе на њима.

Хакинг представља упадање у компјутерске системе тајно и без овлашћења; активност хакера; представља последицу две активности хакера - истраживање и неовлашћено коришћење компјутерског система и покушај неовлашћеног приступа компјутерском систему; процес у коме нека особа спроводи нелегалан упад у компјутерски или комуникациони систем и тамо чита податке, оставља поруке, стартује програме, брише или исправља програме и информације; приступ компјутерском или комуникационом систему за који не постоји дозвола његовог власника; неовлашћени упад у компјутерске или телекомуникационе системе и неовлашћено коришћење компјутерских или телекомуникационих ресурса (читање, копирање, измена, брисање, убацивање података и програма или електронско пресретање података у њиховој трансмисији) у циљу незаконите манипулације резултатима наведених активности (лична употреба, пренос употребе на друга лица, продаја, уцена, тероризам и слично).

Хаштаг (енгл. Hashtag) – кратак опис некога или нечега изречен у једној речи или фрази и праћен знаком (#) који корисницима омогућава да лакше пронађу друге садржаје на мрежи који се односе на задату фразу или реч; друштвене мреже које омогућују комуникацију на овај начин су Фејсбук, Твитер и Инстаграм, јер њихови корисници могу претрагом објављених хаштагова да пронађу садржаје које су други корисници објављивали са истом или сличном тематиком.

Ц

Централни регистар збирки података - евиденција коју чини регистар збирки података о личности и каталог збирки података о личности коју води Повереник за територију Републике Србије.

Црв (енгл. Worm) - програми који се шире преко електронске поште, имају могућност да се сами копирају и да се шире без знања корисника, што на крају може да доведе до потпуног загушења меморије рачунара.

Цурење података – неовлашћено брисање података или неовлашћено умножавање података или копија података из нечијег или неког рачунарског система.

Ч

Чет = Ћаскање

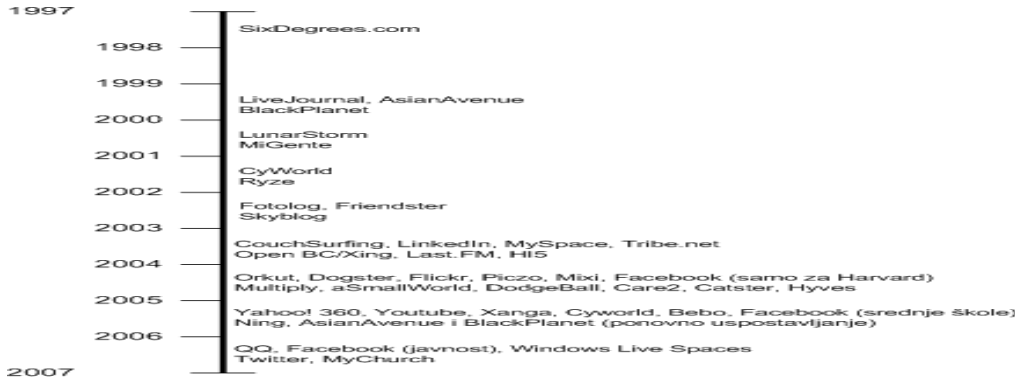
Чет рум = Соба за ћаскање

Ш

Ширење расистичког и ксенофобичног материјала преко рачунарских система - свака радња којом се материјал расистичке и ксенофобичне садржине чини доступним јавности коришћењем рачунара, односно рачунарског система.

2. Хронологија настанка популарних друштвених мрежа и најчешће коришћене друштвене мреже

Почетак развоја виртуелних заједница на интернету почиње 1994. године, када је покренут један од првих сајтова за друштвено умрежавање - Geocities и 1995. године, када су настали интернет портали Classmates.com и Theglobe.com. Године 1997. настао је AOL Instant Messenger, који је популаризовао размену инстант порука, а исте године је настао и Sixdegrees.com, који је први омогућавао креирање профила и додавање пријатеља. Након пионирског покушаја стварања друштвене мреже преко виртуелне заједнице Friends Reunited 1999. године, 2002. године настаје прва права друштвена мрежа у данашњем смислу ове речи - Friendster, који је служио за интернет повезивање пријатеља уопште, а не само генерацијских школских пријатеља и који је у прва три месеца постојања окупио око 3 милиона корисника.[760] Затим се 2003. године појавио портал Myspace, који је дуго времена био најпопуларнији сајт тог типа у свету као и LinkedIn, као специфична друштвена мрежа пословних контаката и сарадника. Појавом ових сајтова друштвене мреже су добиле свој основни облик, а постављањем нових стандарда 2004. године почиње развој друштвене мреже Facebook, најпре само за кориснике студентске мреже у оквиру Харвардског Универзитета а 2006. године и за све кориснике широм света.



Графикон 2: Хронологија настанка најбитнијих друштвених мрежа [761]

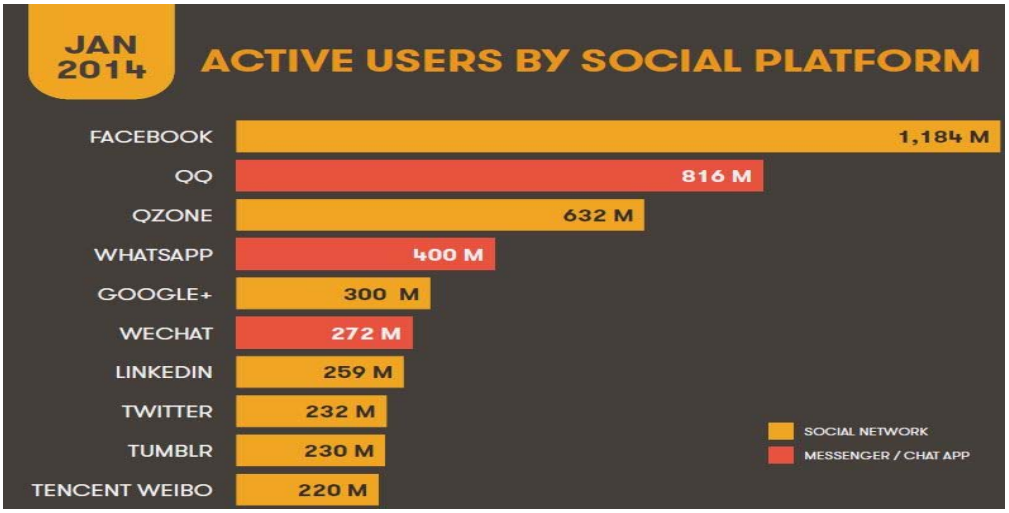
[760] Edosomwan, Simeon, Prakasan, Kalangot, Kouame, Doriane, Watson, Jonelle, Seymour, Tom: „The History of Social Media and its Impact on Business“, The Journal of Applied Management and Entrepreneurship, 2011, Vol. 16, No.3, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.6848&rep=rep1&type=pdf, претражено 05. 11. 2013. године

[761] Boyd, M. Danah, Ellison, B.Nicole, *op.cit.,*2007, стр.216

Број корисника сваке од друштвених мрежа се драстично мења из дана у дан, чинећи неке од мрежа популарним, а друге „заборављеним“. Популарност друштвених мрежа је различита и у зависности о ком делу света је реч. Поједине друштвене мреже (Facebook, Instagram, YouTube) су, према подацима из 2013. године биле популарне и коришћене широм планете, док су поједине друштвене мреже и даље остале карактеристичне да се користе више у одређеним деловима света у којима имају већу популарност и број корисника од неких других (нпр. током 2013. године Pinterest је друштвена мрежа која највише корисника има у Северној Америци, Orkut у Јужној Америци и Азији и сл.):

Графикон 3: Најчешће коришћене друштвене мреже у различитим деловима света током 2013. године, за регистроване кориснике старости 16-64 године [762]

[762] Извор: Lunden, Ingrid: “Instagram Is The Fastest-Growing Social Site”, 21. 01. 2014. године, http://goo.gl/TSJM3C, претражено 09. 07. 2014. године



Графикон 4: Најчешће коришћене друштвене мреже током 2014.године [763]

Подаци из 2013. године[764] указују да је Facebook током ове године достигао број од 1,1 милијарду корисника, Twitter је достигао број од 500 милиона корисника од којих се процењује да је 200 милиона активних корисника, LinkedIn је достигао број од 225 милиона, MySpace од 25 милиона, Tumblr од 170 милиона, Flickr од 87 милиона, Pinterest од 48,7 милиона, Google+ 343 милиона корисника, док је YouTube као видео друштвена мрежа забележио број од 4 милијарди прегледа дневно.

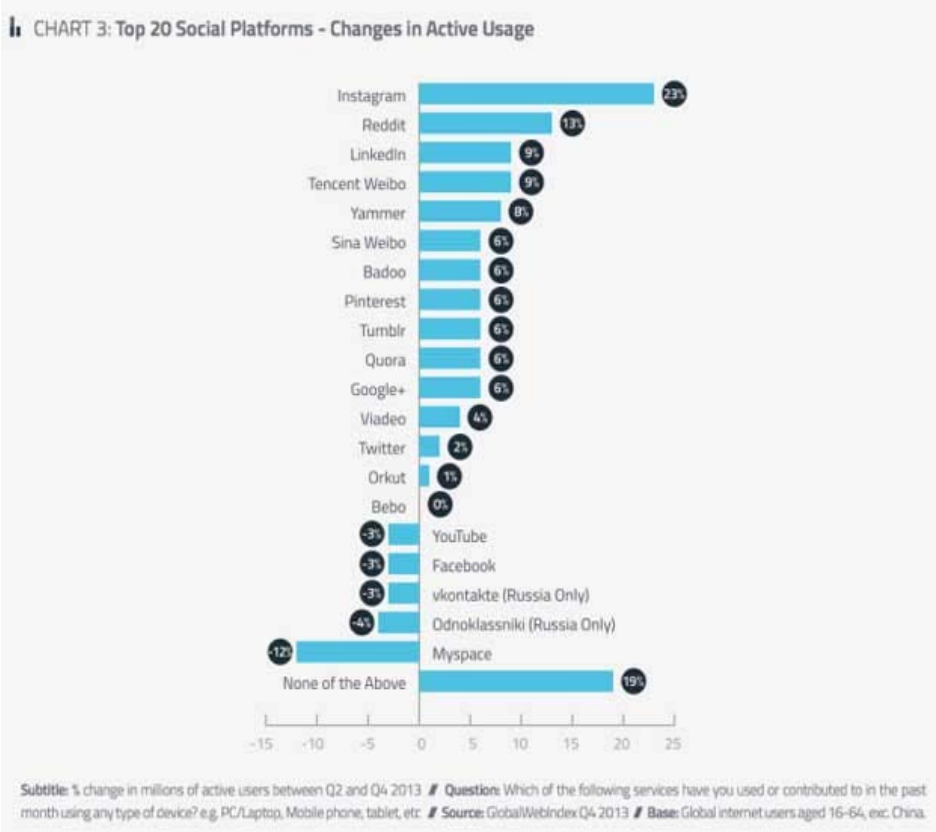
У Србији прве друштвене мреже јављају се 2006. године[765], док током 2007. године почиње експанзија друштвених мрежа. Друштвена мрежа Myspace унела је новину у интернет могућност да свако креира своју сопствену страну коју има на интернету. По први пут људи су добили могућност да направе свој налог, нешто што касније подсећа на мини блог, на коме могу да постављају и коментаришту шта год пожеле. Једна од најновијих домаћих друштвених мрежа Say Serbia[766] појавила се 2013. године и интересантна је по томе што промовише Србију, њене историјске знаменитости, културу, религију, језик, националну

[763] *Ibid.*
[764] The Brief History of Social Media: Where people interact freely, sharing and discussing information about their lives, http://www2.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html, претражено 07. 02. 2015. године
[765] Први сајт овог типа био је www.bleja.com.
[766] Say Serbia, http://sayserbia.com/ , претражено 07. 06. 2014. године

кухињу и уметност, али такође садржи и утисак о Србији гледано очима странаца.[767]

Најчешће коришћене друштвене мреже у Србији су YouTube, са 546.135 локалних корисника и Facebook, са 544.381 регистрованих корисника.[768]

Све друштвене мреже функционишу преко сервиса за друштвену мрежу, који представљају интернет сервис, најчешће у облику платформе, прозора или веб-сајта, који омогућава да се људи из различитих крајева света повезују међусобно, склапају нова познанства или одржавају контакт са људима које већ познају. Функционисање друштвених мрежа је на више нивоа, почев од породице до нације; оне имају важну улогу приликом избора начина на који ће се неки проблем решавати и остваривања појединачних циљева.



Графикон 5: 20 сервиса за друштвене мреже рангираних према броју нових активних корисника[769]

[767] Say Serbia, http://sayserbia.com/forum/categories/foreigner-reviews/listForCategory , претражено 07. 06. 2014. године

[768] Social Bakers, http://www.socialbakers.com/facebook-statistics/serbia, претражено 11. 07. 2014. године

[769] Извор: Lunden, Ingrid: "Instagram Is The Fastest-Growing Social Site", 21.01.2014., http://goo.gl/TSJM3C, претражено 09. 07. 2014. године

Како је знатно повећан број друштвених мрежа и њихових корисника, појавиле су се различите компаније које проучавају посећеност различитих друштвених мрежа и анализирају финансијску исплативост рекламирања путем друштвених мрежа. Једна од водећих компанија која се бави интернет технологијама је ComScore Inc.[770] чији је задатак да мери и обрађује податке о интернет страницама на које људи најчешће одлазе и на којима највише бораве док су на интернету. Ова компанија има преко 2 милиона корисника услуга који су дали своје дозволе да ComScore Inc. поверљиво може да анализира сва интернет претраживања, трансакције које се обављају преко интернет сајтова клијената, понашање индивидуалних корисника интернета док се налазе на друштвеним мрежама, као и да врше анкетна истраживања у којима корисници снимају и интегришу своје ставове и намере. Кроз своје технологије, ComScore Inc. мери оно што је битно у широком спектру понашања и ставова, како би аналитичари ове компаније добијене податке могли да примене да би помогли својим клијентима да дизајнирају моћне маркетиншке стратегије и тактике које би им обезбедиле надмоћ и доминацију у бескрајном интернет простору. Само неки од клијената ове компаније су Microsoft, Yahoo и BBC.

Према анализама које је ова компаније вршила током 2007. године, популарност друштвених мрежа и број корисника драстично су се мењали. За истраживање које је спровео ComScore изабране су друштвене мреже које су у свету током 2006. године имале више од 10 милиона корисника и 50% више корисника у односу на претходну годину. У наведеном периоду, забележен је највећи пораст популарности друштвених мрежа Facebook, Bebo и Tagged, које су у том периоду имале и највећи пораст броја корисника:[771]

[770] ComScore, http://www.comscore.com/ , претражено 12. 06. 2014. године

[771] Lipsman, Andrew: „Social networking goes global“, ComScore press release, јули 2007, http://www.comscore.com/Insights/Press-Releases/2007/07/Social-Networking-Goes-Global, претражено 12. 06. 2014. године

Број регистрованих корисника друштвених мрежа старијих од 15 година из целог света, у периоду јуни 2006 - јуни 2007.године			
Друштвена мрежа	Укупан број регистрованих корисника (у хиљадама)		
	Број корисника јуна 2006. године	Број корисника јуна 2007. године	% разлике
MySpace	66,401	114,147	72
Facebook	14,083	52,167	270
Hi5	18,098	28,174	56
Friendster	14,917	24,675	65
Orkut	13,588	24,120	78
Bebo	6,694	18,200	172
Tagged	1,506	13,167	774

Извор: ComScore World Metrix, јули 2007.

Број дневних посета одређеној друштвеној мрежи од стране регистрованих корисника старијих од 15 година из целог света, у периоду јуни 2006 - јуни 2007. године			
Друштвена мрежа	Укупан број регистрованих корисника (у хиљадама)		
	Број корисника јуна 2006. године	Број корисника јуна 2007. године	% разлике
MySpace	16,764	28,786	72
Facebook	3,742	14,917	299
Hi5	2,873	4,727	65
Friendster	3,037	5,966	96
Orkut	5,488	9,628	75
Bebo	1,188	4,833	307
Tagged	202	983	386

Извор: ComScore World Metrix, јули 2007.

Анализом података истог извора, током 2007.године друштвена мрежа Bebo била је најпопуларнија друштвена мрежа у Европи (62.5%), у Северној

Америци су то биле My Space (62.1%) и Facebook (68.4%), у Јужној Америци Orkut (48.9%), у Азији Friendster (88.7%), а на Блиском Истоку и у Африци Hi5 (8.7%) и Bebo (10.0%). Упоређујући податке из 2007.године са подацима о популарности и заступљености друштвених мрежа у различитим крајевима света, може се закључити да је једино друштвена мрежа Orkut успела да одржи једнако исту популарност у Јужној Америци све ове године. [772]

Број дневних посета одређеној друштвеној мрежи од стране регистрованих корисника старијих од 15 година из целог света, у периоду јуни 2006 - јуни 2007. године

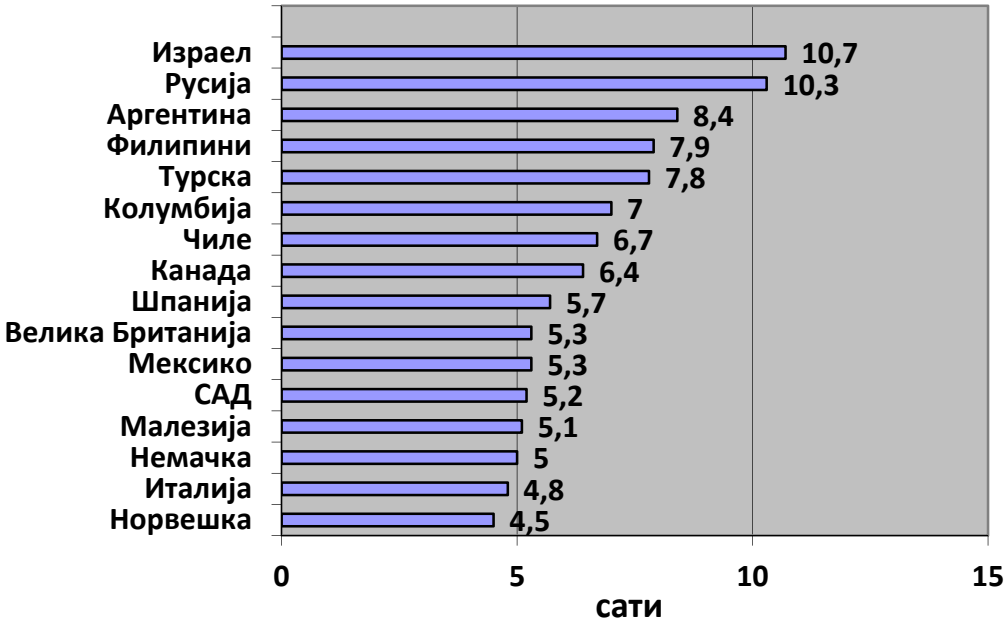
Друштвена мрежа	Проценат (%) регистрованих корисника					
	Свет (укупно)	Европа	Јужна Америка	Северна Америка	Блиски исток и Африка	Азија
MySpace	100.0%	24.7%	3.8%	62.1%	1.3%	8.1%
Facebook	100.0%	16.8%	2.0%	68.4%	5.7%	7.1%
Hi5	100.0%	31.0%	24.1%	15.3%	8.7%	20.8%
Friendster	100.0%	2.5%	0.4%	7.7%	0.8%	88.7%
Orkut	100.0%	4.6%	48.9%	2.9%	0.6%	43.0%
Bebo	100.0%	62.5%	0.5%	21.8%	1.3%	13.9%
Tagged	100.0%	23.4%	14.6%	22.7%	10.0%	29.2%

Извор: ComScore World Metrix, јули 2007.

ComScore Inc. је такође априла 2011. године спровео испитивање о просечној дужини времена коју корисници широм света проведу у активној интеракцији користећи сајтове за друштвено умрежавање и закључили да учесталост приступа друштвеним мрежама зависи од земље до земље. Израел је била највише рангирана земља према времену проведеном по кориснику - у просеку 10,7 сати је сваки од корисника на месечном нивоу проводио користећи неку од друштвених мрежа; на другом месту се налазила Русија са 10,3 сати

[772] Видети Графикон 2: Најчешће коришћене друштвене мреже у различитим деловима света током 2013. године, за регистроване кориснике старости 16 - 64 године

друштвеног умрежавања по кориснику, а затим следе Аргентина са 8,4 сати, Филипини са 7,9 сати и Турска са 7,8 сати. [773]



Графикон 6: просечна дужина времена коју корисници широм света проведу на друштвеним мрежама [774]

Међу најчешћим корисницима друштвених мрежа у пет земаља Европе (Француска, Немачка, Италија, Шпанија и Велика Британија) издвајају се жене, свих старосних структура: на друштвеним мрежама су најчешће активне жене старости између 15 - 24 година које у просеку на друштвеним мрежама проводе око 8,4 сати месечно, а затим следе жене старости између 45 – 54 године са око 5,5 сати месечне активности на друштвеним мрежама.[775] Мушкарци према овом спроведеном истраживању на друштвеним мрежама проводе дупло мање времена.[776]

---

[773] Lella, Adam: „Average Time Spent on Social Networking Sites Across Geographies“, ComScore Insights - ComScore Media Metrix, јуни 2011., http://www.comscore.com/Insights/Data-Mine/Average-Time-Spent-on-Social-Networking-Sites-Across-Geographies, претражено 12. 06. 2014. године

[774] *Ibid.*

[775] Radwanick, Sarah: „Young European Women Spent Most Time on Social Networks“, ComScore Insights, јуни 2011, http://www.comscore.com/Insights/Data-Mine/Young-European-Women-Spent-Most-Time-on-Social-Networks, претражено 12. 06. 2014. године

[776] *Ibid.*

Интересантно истраживање је током октобра и новембра 2006. године спроведено у Сједињеним Америчким Државама у оквиру пројекта Pew Internet & American Life Project. Телефонским путем је интервјуисано 935 младих особа, старости од 12 до 17 година, који су одговарали на питања да ли користе друштвене мреже и ако их користе који су најчешћи разлози за то.[777] Више од половине анкетираних тинејџера (55%) је одговорило да су регистровани као корисници друштвене мреже MySpace или Facebook и да њихови профили нису видљиви према свим корисницима друштвене мреже већ само према особама које додају као пријатеље (66%).[778] Проценат 22% анкетираних корисника друштвених мрежа који више пута у току дана практикује овај вид виртуелне комуникације је 22%, 91% разговара преко друштвене мреже са пријатељима које свакодневно виђа, а 17% тинејџера за искључиви циљ овакве врсте комуникације има "флертовање".[779]

Према предмету интересовања њихових корисника, друштвене мреже је могуће класификовати у неколико основних група:[780]

1. друштвене мреже за кориснике општих интересовања (нпр. Facebook, Twitter, MySpace, Tagged, Meetup, Bebo, Multiply, Orkut, Skyrock, Badoo, StumbleUpon, Delicious, Foursquare, MyOpera, Kiwibox, Hi5);
2. друштвене мреже за размену фотографија (нпр.Flickr, Fotki, Fotolog);
3. друштвене мреже о различитим стиловима живота (нпр.Last.FM, Buzznet, ReverbNation, Cross.TV, WeRead, Flixter, GaiaOnline, BlackPlanet, Care2, CaringBridge, DeviantART, VampireFreaks, CafeMom, Ravelry, ASmallWorld);
4. друштвене мреже посвећене путовањима (нпр. Wayn, CouchSurfing, TravBuddy);
5. друштвене мреже прилагођене мобилним телефонима (нпр. Cellufun, MocoSpace, ItsMy);

---

[777] Lenhart, Amanda, Madden, Mary: „Social Networking Websites and Teens: An Overview", Pew Internet & and American Life Project (2007), http://www.pewinternet.org/2007/01/07/social-networking-websites-and-teens/, претражено 15. 07. 2014. године
[778] *Ibid.*
[779] *Ibid.*
[780] Beyond Facebook: 74 Popular Social Networks Worldwide, http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide, претражено 12. 11. 2014. године

6. друштвене мреже на којима се размењују видео садржаји (нпр. Stickam, FunnyOrDie, YouTube);
7. друштвене мреже које за циљ имају проналажење генерацијских школских пријатеља или рођака (нпр. Classmates, MyLife, MyHeritage, Geni);
8. друштвене мреже које служе пословном повезивању и пословној комуникацији (нпр.LinkedIn, Focus, Viadeo, Ryze, XING);
9. друштвене мреже за децу, тинејџере и младе (нпр. WeeWorld, Habbo,Tuenti);
10. друштвене мреже за писање блогова (нпр.WordPress, Tumblr, Xanga, OpenDiary);
11. међународне друштвене мреже каракретистичне за одређена географска подручја (нпр.у Азији - Mixi, QZone, Douban, Renren, у Русији - VKontakte, Odnoklassniki, у Пољској - NK, у Холандији - Hyves, у Латинској Америци - Sonico, у Сједињеним Америчким Државама - Friendster).

У огромном простору комуникација, неколико друштвених мрежа је обележило овакав вид друштвених контаката.

2.1. Friendster (http://www.friendster.com/)

Представља један од првих интернет сајтова који је промовисао друштвено умрежавање на интернету. Оснивач мреже је Џонатан Абрамс (Jonathan Abrams), а мрежа је први пут активирана 2002. године. Циљ формирања ове мреже био је стварање сајта који би сви широм света могли да користе. Пошто се мрежа кретала ка вртоглавом успеху, 2003. године Google је понудио да је купи, али договор није постигнут. Неколико година касније, две компаније потписале су уговор вредан 20 милиона долара којим је Friendster инкорпорисан у Google search services. Процењује се да је по броју корисника

ова друштвена мрежа 25. на свету[781], али и даље важи за посећеније друштвене мреже у САД и Азији (нпр. у Малезији овој друштвеној мрежи има приступ 23.6% интернет корисника, на Филипинима 22.1%, у Сингапуру 17.9%, а у САД 5.8%).[782]

Ова друштвена мрежа не дозвољава регистрацију особама млађим од 16 година.

2.2. MySpace (http://www.myspace.com/)

Иако није најстарија друштвена мрежа (основана је 2003. године а омасовљавање и највећу популарност је доживела 2006. године), помогла је у дефинисању многих популарнијих на тај начин што је прва инкорпорисала много различитих интернет услуга у један јединствени облик. Сви профили на MySpace имају могућност објављивања блогова, новости и ажурирања статуса, чиме је створен веома детаљан и богат профил појединца. Регистровани корисници могу да објављују и шаљу фотографије, видео снимке и музику, као и да створе различите интересне групе којима и други корисници могу да се прикључе. Интересантан је детаљ да у почетку свог постојања ова друштвена мрежа није за кориснике прихватала малолетна лица, али је са порастом популарности овог сајта промењен и овај принцип, па су и малолетницима била доступна умрежавања, стварање нових пријатељстава и контаката са пријатељима, члановима породице и познатим личностима.[783] Августа 2006. године је направљена статистика корисника MySpace: више од половине посетилаца ове мреже било је старије од 35 година, 34,8% је било узраста од 18 до 34 године, а само 12% посетилаца било је узраста од 12 до 17 година.[784]

---

[781] Goldberg, Scott: "Analysis: Friendster is doing just fine", Digital Media Wire, http://www.dmwmedia.com/news/2007/05/14/analysis-friendster-is-doing-just-fine, претражено 15. 05. 2014. године

[782] *Ibid.*

[783] Boyd, M.Danah, Ellison, B.Nicole, *op.cit.,* 2007, страна 217

[784] Према подацима ComScore из 2006.године, наведено код Jones, Steve, Millermaier, Sarah, Goya-Martinez, Mariana, Schuler, Jessica: "Whose Space is MySpace? A content analysis of MySpace profiles", Journal First Monday, vol.13 no.9, 2008, http://firstmonday.org/article/view/2202/2024, претражено 10. 07. 2014. године

Оваква промена правила приступања овој друштвеној мрежи веома брзо је показала и своју негативну страну: већ током јула 2005. године чуле су се прве оптужбе да се преко ове мреже одвија велики број недозвољених сексуалних контаката између одраслих и малолетника - један од седам анкетираних тинејџера је био жртва нежељеног сексуалног контакта.[785] Ипак, то и даље није резултовало померањем старосне границе за учлањење на ову друштвену мрежу: минимална старосна граница за постајање чланом ове друштвене мреже је и даље 13 година.

Иако је MySpace једна од првих и најстаријих друштвених мрежа, њена популарност није драстично смањена, већ ова мрежа и данас спада у веома популарне и једну од најчешће коришћених друштвених мрежа. Процењује се да ова друштвена мрежа има око 34 милиона корисника широм света.[786]

2.3. Orkut (http://www.orkut.com/)

Представља друштвену мрежу чији је власник Google, иако се мрежом управља из Бразила. Ову друштвену мрежу је развио инжењер Orkut Buyukkokten,[787] у чију је част његовим именом названа мрежа. Пре него што је развио ову друштвену мрежу, Buyukkokten је био један од оснивача Клуба Нексус (енгл. Club Nexus), друштвеног интернет сервиса који је почео са радом на јесен 2001. године и који је имао за циљ да повеже међусобно студенте Стенфорд универзитета како би комуницирали електронском поштом, слали циркуларне позивнице за разне догађаје, куповали и продавали половне ствари, делили са колегама своје радове, упознавали се и дружили. [788]

---

[785] Wolak, Mitchell, & Finkelhor, 2006, наведено код Boyd, M.Danah, Ellison, B.Nicole, *op.cit.,* 2007, страна 217

[786] Beyond Facebook: 74 Popular Social Networks Worldwide, http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide , претражено 12. 11. 2014. године

[787] Orkut, https://support.google.com/orkut, претражено 11. 07. 2014. године

[788] Adamic, Lada, Buyukkokten, Orkut, Adar, Eytan: "A social network caught in the Web", Journal First Monday, vol. 8 no.6, 2003, http://www.firstmonday.org/issues/issue8_6/adamic/index.html, претражено 12. 07. 2014. године

Orkut представља праву друштвену мрежу, јер је друштвено умрежавање и остваривање контаката једина сврха постојања ове мреже, нема дељења садржаја или постављања садржаја без сагласности онога на кога се садржај односи.[789]

Према анализама које је спровела аналитичка кућа ComScore, више од 20 милиона Бразилаца је током 2008. године посетило ову друштвену мрежу, док је у истом периоду MySpace посетило само 893,000 Бразилаца.[790] Ова друштвена мрежа је популарна и у Индији, јер је 17% укупног броја корисника из ове земље.[791] Иако има око 100 милиона корисника широм света,[792] Orkut није популаран ни у Европи ни у САД.

Ова друштвена мрежа не дозвољава регистрацију особама млађим од 18 година, а нови корисници могу да се придруже мрежи само уколико им неко од постојећих корисника пошаље позив за прикључење.

2.4. 51.com (http://51.com/)

Друштвена мрежа која, за разлику од осталих, нема за циљ да створи једно глобално друштво: усмерена је само на једну географску циљну групу – на Кину, а 2008. године ова мрежа имала је 120 милиона чланова у Кини[793]. Регистровани чланови ове друштвене мреже могу да персонализују странице свог профила, постављају фотографије и пишу блогове.

---

[789] Mislove, Alan, Marcon, Massimiliano, Gummadi, P. Krishna, Druschel, Peter, Bhattacharjee, Bobby:
"Measurement and Analysis of Online Social Networks",
http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf , претражено 11. 03. 2015. године
[790] ComScore, http://www.comscore.com/, претражено 05. 08. 2012. године
[791] *Ibid.*
[792] Beyond Facebook: 74 Popular Social Networks Worldwide,
http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide, претражено 12. 11. 2014. године
[793] *Ibid.*

2.5. Skyrock (http://www.skyrock.com/)

Представља најпознатију друштвену мрежу у Француској, која се најпре појавила као место за објављивање блогова у склопу француске независне радио станице из Париза - SKYROCK Radio, 96.0 FM. Како је популарност расла, развио се у праву друштвену мрежу где регистровани корисници могу да праве своје профиле, пишу блогове, разговарају у виртуелним собама за ћаскање и да шаљу поруке једни другима. Иако је Skyrock настао у Француској, регистрованих чланова има широм света – у јулу 2009. године имао је преко 39 милиона регистрованих корисника[794].

Не постоји ограничење у погледу минимума година старости да би неко постао корисник ове друштвене мреже.

2.6. Hi5 (http://www.hi5.com/)

Hi5 је настао у Сан Франциску у САД 2003. године. До 2005.године имао је око 10 милиона регистрованих чланова, а 2008. године представљала је мрежу која се најбрже ширила – само у периоду јануар-јуни 2008. године Hi5 је користило 78% укупног броја регистрованих корисника свих друштвених мрежа[795]. Када су Facebook и MySpace почели да доминирају по броју регистрованих корисника у САД, Hi5 је постала друштвена мрежа усмерена на чланове са других континената, а данас је фокусирана на кориснике из Латиноамеричких земаља, Тајланд, Афрички континент и поједине земље Источне Европе.

Ова друштвена мрежа не дозвољава регистрацију особама млађим од 18 година.

---

[794] *Ibid.*
[795] *Ibid.*

2.7. YouTube (http://www.youtube.com/)

Youtube не представља класичну друштвену мрежу, већ виртуелно место где је могуће постављати музику и видео снимке. То је јавни интернет портал преко кога корисници комуницирају кроз музику, при чему та комуникација може да се креће од постављања и објављивања видеа, њиховог оцењивања па до дељења музичких видео спотова у циљу одржавања одређених друштвених односа. [796]

Начин комуникације који је сличан са комуникацијом на другим друштвеним мрежама огледа се у томе да корисници могу да комуницирају преко писања коментара и гледања/слушања музике. Као регистровани члан, сваки појединац може да има свој профил, да поставља или коментарише музику, да уписује које год информације жели. Јединственост ове мреже се огледа у могућности влогинга (енгл. Video logging – vlogging) који представља паралелу блогингу (енгл. Blogging) – регистровани чланови комуницирају и размењују поруке преко музике коју објављују.

2.8. LinkedIn (http://www.linkedin.com/)

Мисија ове друштвене мреже је да повеже пословне људе широм света како би они били продуктивнији и успешнији. У том смислу, LinkedIn престаља друштвену мрежу која је дизајнирана само за професионалне кориснике и повезивање некадашњих, садашњих и будућих пословних

[796] Lange, G. Patricia: " Publicly Private and Privately Public: Social Networking on YouTube", Journal of Computer-Mediated Communication volume 13 - International Communication Association, 2008, стр. 361–380, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00400.x/pdf, претражено 02. 05. 2014. године

сарадника, којих се процењује да има око 35 милиона.[797] На овој мрежи је могуће успоставити контакт са послодавцима који нуде запослење, пронаћи потенцијалне клијенте за пословну сарадњу, сарађивати на различитим пројектима кроз „виђење" у виртуелним собама и сл. На LinkedIn мрежи налази се више од 354.961 пословних понуда широм света: сваки од ових огласа у просеку се погледа 1.047 пута а на сваки оглас се у просеку пријави 68 кандидата.[798] Процена је да ова друштвена мрежа данас броји око 100 милиона корисника.[799]

Ова друштвена мрежа не дозвољава регистрацију особама млађим од 18 година.

2.9. Twitter (http://www.twitter.com/)

Осмишљен једним делом као веб сајт а делом као јавна мрежа, Twitter је виртуелно место створено за креирање профила, пласирање информација и прављење група „обожаватеља" који вас у том вирутуелном простору "прате" (енгл. Follow), исто као што неко прати њих. Створио га је марта 2006. године Џек Дорси (Jack Dorsey),[800] а мрежа је почела са радом од 13. јула 2006. године. Twitter представља бесплатну друштвену мрежу и микро-блог алат који омогућава својим корисницима да читају туђе и шаљу своје микро-текстуалне уносе, такозване „твитове" (енгл. Tweets) – кратке поруке од највише 140 знакова свима који вас „прате". Овај нови феномен се назива микроблогинг (енгл. Microblogging) и све више добија на популарности.

Twitter је изузетно популаран међу познатим личностима јер омогућава јефтино и популарно рекламирање. На овој друштвеној мрежи не постоје пријатељи, већ само следбеници, јер се сама мрежа користи углавном за

[797] *Ibid.*
[798] LinkedIn, https://www.linkedin.com/job/, претражено 10. 07. 2014. године
[799] Beyond Facebook: 74 Popular Social Networks Worldwide, http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide, претражено 12. 11. 2014. године
[800] Самчовић, Андреја, *op.cit.,* 2013., страна 860

изражавање мишљења о различитим догађајима. Уноси се објављују на корисниковом профилу и испоручују другим корисницима који су се пријавили да их добијају. Они који шаљу твитове могу да ограниче испоруку само на оне из свог круга пријатеља, док је услуга у старту подешена тако да шаље уносе свима који се на њих пријаве. Преко интернета услуга је бесплатна, али слање и примање уноса преко СМС-а може бити наплаћено од стране телефонског провајдера.

Од марта 2009. године Twitter је забележио раст популарности у свету. До 2011. године регистровано је око 300 милиона корисника,[801] а већ током 2013. године овај број је порастао на 500 милиона корисника.[802] Број тренутно активних регистрованих корисника из Србије је тешко проценити. Подаци из 2009. године указивали су да је те године било најмање око три стотине корисника[803] али је извесно да је данас овај број знатно већи и да је 2013.године било око 21.500 налога регистрованих из Србије.[804]

У политици приватности ове мреже је наведено да се особама млађим од 13 година не препоручује коришћење ове мреже.

2.10. Facebook –FB (http://www.facebook.com/)

Марк Цукерберг (Mark Zuckerberg) је, са својим колегама на Харварду, 2004. године успео да осмисли и направи виртуелну интернет заједницу у којој ће корисници моћи да се представе, да потраже друге и да позову остале људе које знају у овакав вид комуникације. Првобитно, чланство на овој интернет страници је било дозвољено само студентима са Харварда, да би се касније проширило на студенте са свих колеџа који су чланови „Ајви лиге“ (Ivy League).

---

[801] Taylor, Chris: “Social networking 'utopia' isn't coming”, CNN интернет емисија од 27. 06. 2011. године, http://articles.cnn.com/2011-06-27/tech/limits.social.networking.taylor_1_twitter-users-facebook-friends-connections?_s=PM:TECH, претражено 10. 08. 2012. године

[802] Самчовић, Андреја, op.cit., страна 861

[803] Broj Twitter korisnika u Srbiji, http://zsteva.info/blog/2009/01/29/broj-twitter-korisnika-u-srbiji/, претражено 10. 08. 2012. године

[804] Самчовић, Андреја, op.cit., страна 861

После извесног времена, чланови су могли да постану сви студенти и средњошколци, а затим и све особе старије од 13 година.

Facebook представља интернет страницу која служи као сервис за друштвену мрежу. Почео је са радом 4. фебруара 2004. године, а корисници ове интернет странице, на коју се свако може учланити, могу се придруживати у мреже које су организоване по градовима, радним местима, школама и регионима, како би се повезали и комуницирали са другим људима. Такође, људи могу додавати пријатеље, слати им поруке, а могу и убацивати нове податке у своје профиле како би обавестили пријатеље о себи.

Када је 2006. године постао отворена мрежа, корисници широм света су позивани да уписивањем само адресе електронске поште постану део ове заједнице. Поред размењивања личних информација и стварања профила, креиран је револуционарни програмски интерфејс (Application programming interface-API) преко којих су регистрованим корисницима постале доступне бројне апликације и видео игре. Само неколико година касније, ФБ мрежа је постала најпосећенија друштвена мрежа на свету, која је у току само једног месеца (јануар 2009. године)[805] имала више од 10 милиона регистрованих посетилаца. Приход основачима од коришћења ове друштвене мреже (реклама и видео-игрица) у току 2011. године износио је 4.27 милијарди долара[806], а број корисника је до краја 2011. године порастао на 600 милиона.

Према подацима са сајта, Facebook данас има око 750 милиона активних корисника широм света[807]. У неким земљама, као што су Сирија,[808] Кина,[809] Вијетнам[810] и Иран,[811] приступ овој интернет страници је повремено блокиран, а

---

[805] *Ibid.*

[806] Facebook '09 revenue neared $800 mn: Sources - The Economic Times, http:// economictimes.indiatimes.com/topic/infotech-internet-Facebook-09-revenue-neared-800-mn-Sources-articleshow-6063819 , претражено 10. 09. 2012. године

[807] Facebook – newsroom, http://newsroom.fb.com/, претражено 10. 09. 2012. године

[808] Khaled Yacoub Oweis: „Syria blocks Facebook in Internet crackdown“, извор Reuters – вест од 23. новембра 2007. године, http://www.reuters.com/article/2007/11/23/us-syria-facebook-idUSOWE37285020071123, претражено 10. 08. 2012. године

[809] China's Facebook Status: Blocked, ABC News – вест од 08. 07. 2009. године, http://abcnews.go.com/blogs/headlines/2009/07/chinas-facebook-status-blocked/, претражено 10. 08. 2012. године

[810] Stocking, Ben: „Vietnam Internet users fear Facebook blackout“, Associated Press – вест од 17. 11. 2009. године, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/11/17/international/i033256S37.DTL, претражено 10. 08. 2012. године

исто је учињено и на бројним радним местима, како запослени не би трошили време на посету сајту.[812] Један од проблема је представљало поштовање приватности корисника, које је неколико пута доведено у питање.

Процењује се да у Србији данас има око 4.000.000 регистрованих корисничких налога, да 50% становништва има профил на некој од друштвених мрежа од чега 45,9% чине жене а 54,1% мушкарци.[813] Највише је корисника ове друштвене мреже старости од 18-29 година (89%).[814]

2.11. Facebook Srbija (http://www.fejsbuksrbija.com, www.facebooksrbija.com, www.fbsrbija.com)

Fejcbuk Srbija (FacebookSrbija) представља веома интересантну друштвену мрежу која се најпре јавила као друштвена мрежа посвећена другој друштвеној мрежи – Facebook, а која пружа савете за боље руковање и сналажење на овој мрежи. Како сами оснивачи и администратори Милош Петровић и Небојша Радовић кажу, Фејсбук Србија представља забавно-информативни сајт о друштвеној мрежи Facebook,[815] који је најпре децембра 2008.године покренут у форми блога а почетком 2010. године био трансформисан у модерни интернет магазин. Овај сајт није замена за коришћење друштвене мреже Facebook, већ служи као допуна у коришћењу ове мреже, где корисници могу да пронађу информације, савете, занимљивости, упутства, мултимедијалне прилоге, савете за превенцију злоупотребе налога на мрежи Facebook, новитете и све што има везе са коришћењем друштвене мреже Facebook.

---

[811] Shahi, Afshin: „Iran's digital war", Daily News Egypt – вест од 27. 07. 2008. године, http://dailystaregypt.com/article.aspx?ArticleID=15313, претражено 10. 08. 2012. године
[812] Benzie, Robert: „Facebook banned for Ontario staffers", TheStar.com – вест од 03. 05. 2007. године, http://www.thestar.com/News/article/210014, претражено 10. 08. 2012. године
[813] Блиц – дневна новина од 01. 02. 2015. године, www.blic.rs, претражено 01. 02. 2015. године
[814] *Ibid.*
[815] Фејсбук Србија, http://www.fejsbuksrbija.com/, претражено 15. 02. 2015. године

Интересантан је податак да су се оснивачи Фејсбук Србија већ септембра 2011. године сусрели са проблемом: компанија Facebook је тражила промену адресе домена www.facebooksrbija.com[816], па је сајт премештен да две нове адресе - www.FejsbukSrbija.com и www.fbsrbija.com.

На овом сајту корисници друштвене мреже могу да прочитају интересантне савете о томе како да се не објављују слике без ауторизације корисника,[817] подешавања сигурносних података,[818] како трајно обрисати кориснички налог,[819] како препознати лажни налог на Фејсбуку,[820] како заштитити лозинку од злоупотребе[821] и сл.

2.12. Google Plus (http://plus.google.com/)

Google Plus (Google+) представља најновију и веома популарну мрежу компаније Google која је своје постојање отпочела средином 2011. године и сматра се да већ представља другу друштвену мрежу према броју регистрованих корисника којих има око 500 милиона, одмах после друштвене мреже Facebook.[822] Старосна граница за приступање овој друштвеној мрежи је 13 година старости.

Google+, иако представља својеврсну мешавину неколико популарних мрежа, има више предности које је чине популарном. Дељење и размена садржаја је могућа преко ове друштвене мреже само са особама са којима

---

[816] Фејсбук Србија, http://www.fejsbuksrbija.com/facebook-kompanija-trazi-promenu-adrese-sajta-facebooksrbija-com/informacije/1785.html, претражено 15. 02. 2015. године

[817] Фејсбук Србија, http://www.fejsbuksrbija.com/neces-me-vise-tagovati/uputstva/1975.html, претражено 15. 02. 2015. године

[818] Фејсбук Србија, http://www.fejsbuksrbija.com/jos-jednom-podesite-svoje-sigurnosne-podatke/uputstva/1491.html, претражено 15. 02. 2015. године

[819] Фејсбук Србија, http://www.fejsbuksrbija.com/brisanje-facebook-naloga/uputstva/1412.html, претражено 15. 02. 2015. године

[820] Фејсбук Србија, http://www.fejsbuksrbija.com/facebook-lazni-profil-prijava/uputstva/1336.html, претражено 15. 02. 2015. године

[821] Фејсбук Србија, http://www.fejsbuksrbija.com/kako-nam-kradu-lozinke/uputstva/850.html, претражено 15. 02. 2015. године

[822] Фејсбук Србија, http://social-networking-websites-review.toptenreviews.com/google--review.html, претражено 11.07.2014. године

корисник то жели, јер приликом сваког публиковања информација може да одреди да ли ће те информације видети особе које су му класификоване у један од четири кругова: чланови породице, пријатељи, познаници или особе чији се рад прати преко интернета. Корисник може да прошири број својих кругова тако што ће зависно од афинитета и потреба лакше комуникације направити нове, чији број није ограничен правилима мреже.

Сваки корисник може да подеси своју видљивост на друштвеној мрежи и да забрани да се његови контакти и постављени садржај прослеђују даље другим корисницима, па је на овај начин смањена вероватноћа злоупотребе објављеног садржаја, што је и највећа предност ове мреже. Постоји могућност да се органичи и слање обавештења које други корисници желе да пошаљу једни другима, могућност забране коментара на објављене садржаје, могуће је ограничини опцију "ћаскања" само на мали и проверен круг људи. Коришћење видео позива (енгл. Video hangout) је преко одређене апликације доступно како са рачунара тако и са мобилног телефона, у њему може да учествује више људи (највише до девет), а овакву видео комуникацију је могуће преносити и директно на YouTube.

Новост је и да на овој мрежи нема обавештења о видео играма, реклама и других нежељених садржаја које успоравају рад.

2.13. Instagram (http://instagram.com/)

Инстаграм представља најбрже растућу друштвену мрежу, чији је број активних корисника порастао од почетка 2014. године за 23%.[823] Оснивачи ове мреже су Kevin Systrom и Mike Krieger, а мрежа је пуштена у виртуелни простор октобра 2010. године, најпре као апликација за мобилне телефоне са интернет платформом. За само месец дана постојања, имала је милион регистрованих

[823] Економски портал, http://www.ekonomskiportal.com/instagram-najbrze-rastuca-drustvena-mreza/, претражено 12. 07. 2014. године

корисника,[824] а овај број се до јануара 2014. године попео на 150 милиона активних корисника, 16 милијарди подељених слика и 7.3 милиона посетилаца ове мреже по једном дану.[825]

Корисници ове друштвене мреже за основни циљ имају размену фотографија и на тај начин осликавају своје виртуелне животе кроз серију својих фотографија и фотографија њима блиских људи. Сам назив друштвене мреже је веома сликовито означава природу комуникације на њој: „инстаграм" потиче од речи „инстант" којом је представљена брзина стварања слике и њено објављивање на интернету.[826] Овако настале фотографије могу да се деле преко других друштвених мрежа, за сада преко Flickr, Facebook и Twitter. Процењује се да 9 од 10 корисника своју слику ипак одабере да са остатком виртуелног света подели преко друштвене мреже Facebook.[827]

Уколико је кориснички профил на овој друштвеној мрежи јаван, сви могу видети фотографије, али постоје и могућности да се приватност подеси тако да сам корисник мора да одобри ко сме да му види слике које објави. Ништа од објављених садржаја (текст, фотографије, видео снимци, музика и звучни записи и сл.) није у власништву ове друштвене мреже, али она може да поједине објављене делове прослеђује даље и користи јер је на то „овлашћују" сами корисници.[828] Управо су овде могуће злоупотребе јер неко од корисника може да „присвоји" туђ садржај, да га објави као свој а да прави аутор остане без заштите.[829]

---

[824] 30 Things You Absolutely Need To Know About Instagram, http://www.searchenginejournal.com/30-things-absolutely-need-know-instagram/85991/, претражено 12. 07. 2014. године

[825] *Ibid.*

[826] Инстаграм, http://instagram.com/about/faq/ , претражено 12. 07. 2014. године

[827] 30 Things You Absolutely Need To Know About Instagram, http://www.searchenginejournal.com/30-things-absolutely-need-know-instagram/85991/, претражено 12. 07. 2014. године

[828] 6 Things Everyone Should Know About Instagram,http://thesocialu101.com/6-things-everyone-should-know-about-instagram/, претражено 12. 07. 2014. године

[829] На овој друштвеној мрежи је забележен случај да су са налога једне од регистрованих корисница (Amanda - I Am Baker) ове друштвене мреже преузете фотографије које је неко касније поставио као његове ауторске, па чак се и са тим фотографијама пријавио на такмичење које организује ова друштвена мрежа. На такмичењу је за ову фотографију гласало 24.000 корисника Инстаграма, који заправо нису ни знали чијем се делу диве. Власница фотографије је контактирала и администраторе Инстаграма као и кориснике који су делили њено дело. Нико јој ни даље није званично у име ове друштвене мреже одговорио како је до оваквог нечега дошло и шта даље може да се предузме како би корисницима могла да се обезбеди извесна сигурност.

Instagram је популаран у свим крајевима света, преко 60% корисника је из Европе, 33% из Северне Америке: 5,6% корисника је из Бразила, 3,8% је из Велике Британије, 3,5% из Русије, 3,2% из Мексика.[830]

Минимална старосна граница за придруживање овој друштвеној мрежи је 13 година.

2.14. Bebo (http://www.bebo.com/)

Bebo представља популарну друштвену мрежу која је заступљена у свим деловима света преко које њени корисници могу (јавно или са ограничењем приватности) да деле фотографије, текстове, своје блогове. Оснивачи ове друштвене мреже су Michael и Xochi Birch. Званично, мрежа је пуштена у виртуелни простор 2005. године и за само девет дана постојања успела је да региструје милион корисника.[831] Прва пробна верзија мреже направљена је 2000. године у земљама енглеског говорног подручја – Ирској, Енглеској и Новом Зеланду.[832] Сам назив друштвене мреже представља акроним за крилатицу „Блогуј рано, блогуј често" (енгл. Blog Early, Blog Often).

Мрежа је прилично лака и сигурна за коришћење, а подешавање приватности профила корисника је аутоматски: сви профили су приватни, осим ако сам корисник не одлучи да профил подеси да могу сви који приступају интернету да га виде. Са овим правилом, Bebo је јединствена друштвена мрежа.

Посебну сигурносну меру ова друштвена мрежа има за своје кориснике који имају мање од 21 године: на сваком профилу може да се ограничи старосна граница људи са којима корисник жели да контактира. Ипак, члан ове друштвене мреже може бити свака особа старија од 13 година.

(*извор:* 6 Things Everyone Should Know About Instagram, http://thesocialu101.com/6-things-everyone-should-know-about-instagram/, претражено 12. 07. 2014. године)

[830] *Ibid.*

[831] Bebo, http://www.bebo.com/faq , претражено 06. 06. 2014. године

[832] Bebo, http://social-networking-websites-review.toptenreviews.com/bebo-review.html, претражено 06. 06. 2014. године

Bebo је продата 2008. године да би 2013. године ипак била враћена њеним оснивачима, који покушавају да врате све информације које је ова друштвена мрежа делила међу својим корисницима и да се по броју старих и нових корисника поново дођу у сам врх најпопуларнијих виртуелних места за комуникацију.

2.15. Classmates (http://www.classmates.com/)

Карактеристична само за територију Сједињених Америчких Држава, ова друштвена мрежа представља најчешће коришћен сервис за проналажење генерацијских пријатеља из средње школе, одржавање њихових контаката и организовање прослава и годишњица. Регистровање корисника је могуће и преко налога једне друге друштвене мреже – коришћењем већ постојећег Facebook налога. У почетку је ова друштвена мрежа представљала мрежу која је била посебно направљена за кориснике из САД - првенствено за школарце, студенте и пословне људе, да би временом почела да се користи не само у САД већ и у Канади, Аустрији, Шведској, Швајцарској, Немачкој и Француској.

Старосна граница за приступање овој друштвеној мрежи је 18 година старости.

2.16. StumbleUpon (http://www.stumbleupon.com/)

Ова друштвена мрежа је специфична по свом циљу постојања: она не жели да се преко ње њени корисници упознају и друже, већ само да једни другима у складу са интересовањима које имају препоруче које интернет локације обавезно треба посетити или треба избегавати. StumbleUpon омогућава регистрованим корисницима да гласају за интернет сајтове који им се свиђају или који им се не свиђају, како би створили своју личну страницу са местима

које воле или не воле да посећују док су у виртуелном простору. Регистровање корисника је такође могуће и коришћењем већ постојећег Facebook налога.

Не постоји ограничење у погледу минимума година старости да би неко постао корисник ове друштвене мреже.

2.17 SaySerbia (http://sayserbia.com)

Настала децембра 2013. године, ова друштвена мрежа представља део пројекта који реализује група младих и талентованих студената уз помоћ Чарлса Катера (Charles Cather), како би се разбили стереотипи о Србији и открило право лице Србије.[833] На друштвеној мрежи се промовише Србија, њене историјске знаменитости, култура, религија, језик, национална кухиња и уметност, а постоји и посебан део који садржи утиске о Србији гледано очима странаца.[834] Корисници ове мреже могу да буду све особе старије од 13 година.

Овај „српски Facebook", како се међу медијима и корисницима ова мрежа назива,[835] већ има више од 2.000 чланова[836] и повезује Србе и пријатеље Србије, како је написано на Facebook презентацији ове друштвене мреже а преносе медији земаља из региона.[837] Сама друштвена мрежа је једини власник свих објављених садржаја и једина има приступ свим објављеним подацима. Правило је да се подаци сакупљени од корисника неће отуђити, продавати нити делити са неким другим субјектима. [838]

---

[833] SAY SERBIA: Ovo je srpska verzija Fejsbuka, http://www.telegraf.rs/hi-tech/internet/894983-srbija-dobija-svoj-fejsbuk-koji-se-zove-say-serbia, претражено 07. 06. 2014. године

[834] Say Serbia, http://sayserbia.com/forum/categories/foreigner-reviews/listForCategory, претражено 07. 06. 2014. године

[835] Srbija dobila „svoj Facebook" – Say Serbia, http://www.b92.net/tehnopolis/vesti.php?yyyy=2013&mm=12&nav_id=786328, претражено 07. 06. 2014. године

[836] SAY SERBIA: Ovo je srpska verzija Fejsbuka, http://www.telegraf.rs/hi-tech/internet/894983-srbija-dobija-svoj-fejsbuk-koji-se-zove-say-serbia, претражено 07. 06. 2014. године

[837] Друштвена мрежа која спаја Србе и пријатеље Србије: Наши сусједи добили свој Facebook, http://www.index.hr/black/clanak/quotdrustvena-mreza-koja-spaja-srbe-i-prijatelje-srbijequot-nasi-susjedi-dobili-svoj-quotfacebookquot/715359.aspx , претражено 07. 06. 2014. године

[838] Say Serbia, http://sayserbia.com/main/authorization/privacyPolicy, претражено 07. 06. 2014. године

Интересантни су и услови коришћења које сваки корисник приликом регистрације свог профила мора да прочита и да се сложи, да потврди да их је разумео и да је сагласан како би креирао сопствени налог.[839] Сваки корисник је одговоран за своје понашање на мрежи јер се регистровањем налога обавезао да неће објављивати садржаје којима се на било који начин врши повреда нечијег права интелектуалне својине или власничких права других, садржаје који садрже вирусе, промовишу незаконите активности, угрожавају нечију сигурност и интегритет, који су узнемиравајући, злонамерни или нарушавају нечију приватност или су на било који начин негативни по млађе и малолетне кориснике и сл.[840] Корисници су такође у обавези да се уздржавају од прогањања и узнемиравања других корисника, коришћења или откривања личних података о другим корисницима без њиховог пристанка, постављања било каквог садржаја који указује на порнографију, дечију порнографију или екстремно насиље и сл.[841]

[839] Say Serbia, http://sayserbia.com/main/authorization/termsOfService, претражено 07. 06. 2014. године
[840] *Ibid.*
[841] *Ibid.*

3. Индекс појмова

К

Л

М

Н

О

П

Р

С

Т

Ћ

Ф

Х

Ц

Ч

Ш

ЛИТЕРАТУРА

Књиге, монографије и чланци

1. A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, стр. 225-229, https://openlibrary.org/works/OL11001385W/Criminological_aspects_of_economic_crime, претражено 08. 11. 2014. године
2. Abdul Manap Nazura, Moslemzadeh Tehrani Pardis: "Cyber Terrorism: Issues in Its Interpretation and Enforcement", International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012, стр. 409-413, http://www.ijiee.org/papers/126-I149.pdf, претражено 17. 07. 2015. године
3. Adamic, Lada, Buyukkokten, Orkut, Adar, Eytan: "A social network caught in the Web", Journal.First Monday, vol. 8 no.6, 2003, http://www.firstmonday.org/issues/issue8_6/adamic/index.html, претражено 12. 07. 2014. године
4. Aftab, Parry: "What methods work with the different kinds of cyberbullies?, 2006, www.stopcyberbullying.org/pdf/howdoyouhandleacyberbully.pdf, претражено 12. 03. 2014. године
5. Alexy, M. Eileen, Burgess, W. Ann, Baker, Timothy :"Internet Offenders: Traders, Travelers, and Combination Trader-Travelers", Journal of Interpersonal Violence, volume 20 number 7, 2005, стр. 804-812
6. Alonzo-Dunsmoor, Monica:"Phoenix Officials to Crack Down on Child Prostitution", The Arizona Republic, 2006, http://www.azcentral.com/arizonarepublic/local/articles/0311prostitution0311.html, претражено 07. 09. 2014. године
7. Анонимус: „Deep Web - Мрачна страна интернета", Лагуна, Београд, 2015
8. Ален, Рајко: „Информацијско управно право", Хрватска јавна управа, год. 9 (2009) бр. 1
9. Ashley, K. Bradley: "Anatomy of cyber terrorism: Is America vulnerable?", Air University, Maxwell AFB, AL, 2003, www.au.af.mil/au/awc/awcgate/awc/ashley.pdf, претражено 17. 07. 2015. године

10. Бабић, Владица: „Нови облици дјеловања терориста (Cyber тероризам)“, 4th International Scientific and Professional Conference ‘Police College Research Days In Zagreb’ , стр. 11-26, http://www.mup.hr/UserDocsImages/PA/vps/idvps2015/Zbornik_radova_Konferencije.pdf, претражено 15. 08. 2015. године
11. Бабовић, Милош.:„Хакерска субкултура и компјутерски криминал“, Правни живот – часопис за правну теорију и праксу, бр. 9/2004, година LIII, књига 485, стр. 749-750, Удружење правника Србије, Београд
12. Balachander, Krishnamurthy, Wills E.Craig: “On the Leakage of Personally Identifiable Information Via Online Social Networks”, http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf, претражено 12. 08. 2013. године
13. Bangeman, Eric: “ 2010. Report: Facebook caught sharing secret data with advisers“, http://arstechnica.com/tech-policy/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers/, претражено 04. 10. 2013. године
14. Barak, Azy: “Sexual harrasmet on Internet”, Social Science Computer Review, Vol. 23 No. 1, 2005, стр. 77-92, http://construct.haifa.ac.il/~azy/SexualHarassmentBarak.pdf, претражено 09. 02. 2014. године
15. Barnes, Susan: “A privacy paradox: Social networking in the United States“, часопис “First Monday”, volume 11, number 9, 2006, http://firstmonday.org/article/view/1394/1312, претражено 23. 05. 2014. године
16. Beal, Vangie: ”How to Defend Yourself Against Identity Theft”, http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp, претражено 17. 09. 2012. године
17. Бејатовић, Станко: “Високотехнолошки криминал и кривичноправни инструменти супротстављања”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., с. 17-30 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

18. Benschop, Albert: „CyberStalking: menaced on the internet", SocioSite-Social & Behavioral Sciences -
Sociology & Anthropology University of Amsterdam, October, 2003, http://www.sociosite.org/cyberstalking_en.php , претражено 14. 07. 2014. године
19. Benzie, Robert: „Facebook banned for Ontario staffers", TheStar.com – вест од 03. 05. 2007. године, http://www.thestar.com/News/article/210014, претражено 10. 08. 2012. године
20. Beran, Tanya, Li, Qing:"The relationship between cyberbullying and school bullying", Journal of Student Wellbeing. 2007;volume 1(2), стр.15-33, http://www.ojs.unisa.edu.au/index.php/JSW/article/viewFile/172/139, претражено 03. 10. 2014. године
21. Beran, Tanya, Li, Qing:"The relationship between cyberbullying and school bullying", Journal of Student Wellbeing. 2007;volume 1(2), стр.15-33, http://www.ojs.unisa.edu.au/index.php/JSW/article/viewFile/172/139, претражено 03. 10. 2014. године
22. Бобан, Марија: „Право на приватност и право на приступ информацијама у савременом информацијском друштву", Зборник радова Правног факултета у Сплиту, год. 49, 3/2012., стр. 575.- 598, http://hrcak.srce.hr/file/129212, претражено 06. 08. 2015. године
23. Bocij, Paul: "Cyberstalking: harrasment in the Internet age and how to protect your family", Praeger Publications, 2004
24. Bork, Robert :"The Tempting of America: The Political Seduction of the Law", New York: Simon and Schuster, 1990, http://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1896&context=lawreview, претражено 18. 02. 2015. године
25. Bosler, A., Holt, Thomas: „Malware Victimisation, A Routline Activities Framework" и Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, Edited by K. Jaishankar, CRS Press, 2011., стр. 319, http://ruangbacafmipa.staff.ub.ac.id/files/2012/02/Cyber_Criminology__Exploring_Internet_Crimes_and_Criminal_Behavior.pdf, претражено 28. 08. 2015. године
26. Бошковић, Горан, Ивановић, Звонимир: "Стратешке концепције у супротстављању високотехнолошком криминалу", Зборник радова,

међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 79-92 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године

27. Bowers, Toni: "Employers who check out job candidates on MySpace could be legally liable", 2008, http://www.techrepublic.com/blog/career/employers-who-check-out-job-candidates-on-myspace-could-be-legally-liable/338, претражено 29. 04. 2013. године
28. Bowie, Vaughan, Fisher, S. Bonnie, Cooper, Cary : „Workplace Violence", Routledge, 2012, https://books.google.si/books?hl=sr&lr=&id=OmkQBAAAQBAJ&oi=fnd&pg=PA248&dq=cyber+workplaceviolence+&ots=0VUnUUGL2Q&sig=p4519veMQ5z3k5gt9SpzoMqdQk&redir_esc=y#v=onepage&q=cyber%20workplaceviolence&f=false, претражено 12. 08. 2015. године
29. Boyd, M.Danah, Ellison, B.Nicole: "Social Network Sites: Definition, History,and Scholarship", Journal of Computer-Mediated Communication Volume 13, Issue 1, International Communication Association, октобар 2007, стр. 210–230
30. Boyd, Danah, Hargittai, Eszter: "Facebook Privacy Settings: Who Cares?", First Monday, Volume 15, Number 8, 2010, http://firstmonday.org/article/view/3086/2589 , претражено 15. 04. 2014. године
31. Brunker, Mike: "Streetwalkers in Cyberspace", MSNBC, 1999, http://www.nbcnews.com/id/3078778/#.VRcei_nF-T8, претражено 07. 09. 2014. године
32. Calvete, Esther, Orue, Izaskun, Estévez, Ana, Villardón, Lourdes, Padilla, Patricia:"Cyberbullying in adolescents: modalities and aggressors' profile", Computers in Human Behavior, 2010; volume 26, number 5, стр.1128-1135, http://database.cmch.tv/SearchDetailBrowser.aspx?rtrn=advnce&cid=5762, претражено 13. 03. 2015. године
33. Cannataci, Joseph A.: "Privacy and Data Protection Law: International Development and Maltese Perspectives", Complex series, 1987.

34. Cassidy, Wanda, Jackson, Margaret, Brown, N.Karen: "Sticks and stones can break my bones, but how can pixels hurt me? Students' experiences with cyber-bullying", School Psychology Internaional, 2009, volume 30(4), стр.383-402, http://extension.fullerton.edu/professionaldevelopment/assets/pdf/bullying/sticks_and_stones.pdf, претражено 14. 03. 2015. године
35. Catanese, A. Salvatore, De Meo, Pasquale, Ferrara, Emilio, Fiumara, Giacomo, Provetti, Alessandro: "Crawling Facebook for Social Network Analysis Purposes", 2011, http://arxiv.org/pdf/1105.6307.pdf, претражено 15. 02. 2015. године
36. Cho, Hichang, Rivera-Sánchez, Milagros, Lim, Sun Sun: "A Multinational Study on Online Privacy: Global Concern and Local Responses. New Media & Society", vol.11, 2009., стр.395-416, http://nms.sagepub.com/content/11/3/395.short, приступ 12. 11. 2014. године
37. Clough, Jonathan: "Principles of Cybercrime", Cambridge University Press, 2010
38. Comprehensive Study on Cybercrime – Draft, United Nations office on drugs and crime, Vienna, February 2013, United Nations, New York 2013, str. Ix, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, претражено 12. 10. 2014. године
39. Cyber Criminology, Exploring Internet Crimes and Criminal Behavior, Edited by K. Jaishankar, CRS Press, 2011, http://ruangbacafmipa.staff.ub.ac.id/files/2012/02/Cyber_Criminology__Exploring_Internet_Crimes_and_Criminal_Behavior.pdf, претражено 28. 08. 2015. године
40. D'Ovidio, Robert, Doyle, James: "Cyberstalking: Understanding the Investigative Hurdles", FBI Law Enforcement Bulletin, volume 72 no.3, 2003, стр. 10 – 17, https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=199743, претражено 24. 03. 2015. године
41. Danquah P. , Longe, O.B. : "An Empirical Test of The Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana", African Journal of Computing & ICT September 2011, Vol. 2. No. 2

Issue 1, str.37-48, http://www.ajocict.net/uploads/V4N1P6-2011_AJOCICT_-_An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality_-_The_Case_of_Ghana_and_Beyond.pdf, претражено 28. 08. 2015. године

42. Davenport N.Zanolli, Elliott G.Pursell, Schwartz R. Diestler: "Mobbing, Emotional Abuse in the American Workplace", 3rd Edition 2005, Civil Society Publishing. Ames, IA, http://www.mobbing-usa.com/, претражено 20. 04. 2013. године
43. Delmonico David, Griffin Elizabeth: „Cybersex and the e-teen: what marriage and family therapists should know", Journal of Marital Family Therapy, volume 34, number 4, 2008; стр.431-444, http://www.researchgate.net/publication/23481408_Cybersex_and_the_E-teen_what_marriage_and_family_therapists_should_know, претражено 05. 11. 2014. године и 18. 12. 2014. године
44. Denning, Dorothy, Drake, Frank:"A Dialog on Hacking and Security", edicija: Computers under attack: intruders, worms, and viruses, Association for Computing Machinery Publications, New York, 1990., str. 421-439
45. Dey, Ratan, Jelveh, Zubin, Ross, Keith,: "Facebook Users Have Become Much More Private:A Large-Scale Study", 2011, http://cis.poly.edu/~ratan/facebookusertrends.pdf, претражено 04. 08. 2013. године
46. Diamanduros Terry, Downs Elizabeth, Jenkins J. Stephen: "The role of school psychologists in the assessment, prevention, and intervention of cyberbullying", Psychology in School Publications., 2008; volume 45, number 8, стр. 693-704, http://www.researchgate.net/publication/227828178_The_role_of_school_psychologists_in_the_assessment_prevention_and_intervention_of_cyberbullying, претражено 03. 10. 2014. године
47. Дилигенски, Андреј, Прља, Драган: „Фејсбук и право", Институт за упоредно право, Београд, 2014
48. Димовски, Злате, Илијевски, Ице, Бебаноски, Кире: "Безбедоносно-криминалистичке димензије сајбер-терористичких напада", Зборник радова, међународна научностручна конференција, Сузбијање криминала

и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 65-78 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

49. Драговић, Свјетлана, Милијевић, Драгана; Вишњић Дражен: "Мјесто и улога прикривеног истражитеља у спречавању и сузбијању кривичних дјела из области вискотехмолошког криминалитета", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године
50. Дракић, Драгиша: „Сукоб кривичног права и медицинске етике и психијатријске науке на примеру психијатријског вештачења", Зборник радова Правног факултета у Новом Саду, 2/2012, стр. 193-205, http://scindeks-clanci.ceon.rs/data/pdf/0550-2179/2012/0550-21791202193D.pdf, претражено 14.01.2016. године
51. Дракулић, Мирјана: „Основи компјутерског права", Друштво операционих истраживача Југославије - ДОПИС, Београд, 1996.
52. Дракулић, Мирјана, Дракулић, Ратимир: „Cyber криминал", Твининг пројекат ЕУ – зборник „Везе cyber криминала са ирегуларном миграцијом и трговином људима", Министарство унутрашњих послова Републике Србије, 2014. година, стр.165-386, http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/Cyber%20kriminal,%20iregularne%20migracije%20i%20trgovina%20ljudima.pdf, претражено 23. 07. 2015. године
53. Dressing, Harald, Henn, A. Fritz, Gass, Peter: „Stalking behavior - an overview of the problem and a case report of male-to-male stalking during delusional disorder", Psychopathology Vol. 35, No. 5, 2002, стр. 313-318.
54. Duermyer, Randy: „Social Networks - Define Social Networks", http://homebusiness.about.com/od/homebusinessglossar1/g/social-networks.htm, претражено 07. 06. 2014. године

55. Duffy, Michael: „A dad's encounter with the vortex of Facebook," http://www.time.com/time/magazine/article/0,9171,1174704,00.html, претражено 23. 01. 2015. године
56. Edosomwan, Simeon, Prakasan, Kalangot, Kouame, Doriane, Watson, Jonelle, Seymour, Tom: „The History of Social Media and its Impact on Business", The Journal of Applied Management and Entrepreneurship, 2011, Vol. 16, No.3, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.6848&rep=rep1&type=pdf, претражено 05. 11. 2013. године
57. Ellison, Louise: "Cyberstalking: Tackling harrasment on the Internet", Crime and the internet, London: Routledge, 2001, http://books.google.rs/books?id=JRb9BDTlrUsC&pg=PA141&lpg=PA141&dq=Ellison+Cyberstalking:+Tackling+harrasment+on+the+Internet&source=bl&ots=K2rQ0sNGFK&sig=dtrxWvfu2e5atvbxvXtKvYehCmI&hl=sr&sa=X&ei=5AUIu_Gc_IsgaioYG4BA&sqi=2&redir_esc=y#v=onepage&q=Ellison%20Cyberstalking%3A%20Tackling%20harrasment%20on%20the%20Internet&f=false, претражено 02. 03. 2013. године
58. Гаћиновић, Радослав: „Облици савременог тероризма", НБП Журнал за криминалистику и право, Криминалистичко-полицијска академија, 2012. година, стр. 1-18, http://www.kpa.edu.rs/cms/data/akademija/nbp/NBP_2012_1.pdf, претражено 21. 06. 2015. године
59. Galley, Patrick: „Computer terrorism: what are the risks?", Science, Technology and Society Swiss Federal Institute of Technology, 1996, http://www.home.ch/~spaw1165/infosec/sts_en/, претражено 14. 02. 2014. године
60. Garfinkel, Simson: "Database nation: The death of privacy in the 21st century", Sebastopol, Calif.: O'Reilly, 2000, http://monoskop.org/images/3/3f/Garfinkel_Simson_Database_Nation_The_Death_of_Privacy_in_the_21st_Century.pdf, претражено 15. 01. 2015. године
61. Gilbert, Pamela: "On Sex, Cyberspace, and Being Stalked", Women and Performance 9, No.1, 1996, стр. 125-149 .

62. Goldberg, Scott :“Analysis: Friendster is doing just fine“, Digital Media Wire, http://www.dmwmedia.com/news/2007/05/14/analysis-friendster-is-doing-just-fine, претражено 15. 05. 2014. године
63. Gross, Ralph, Acquisti, Alessandro: “Information revelation and privacy in online social networks (The Facebook Case)”, In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, стр. 71-80. ACM, 2005, http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, претражено 14. 10. 2013. године и 15. 02. 2015. године
64. Група аутора: „Високотехнолошки криминал“, Практични водич кроз савремено кривично право и примери из праксе, OSCE, Подгорица, март 2014, www.osce.org/me/montenegro/117630?download=true, претражено 15. 08. 2015. године
65. Halder, Debarati, Jaishankar, Karuppannan: “Cyber Socializing and Victimization of Women”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 5-26
66. Hall, Macalister Malcolm.: “The Darker Side of Travel”, The UK Telegraph, 2003, http://www.telegraph.co.uk/travel/destinations/asia/cambodia/728691/The-darker-side-of-travel.html, претражено 07. 09. 2014. године
67. Hargittai, Eszter: “Whose Space? Differences Among Users and Non-Users of Social Network Sites“, Journal of Computer-Mediated Communication, volume 13, issue 1, str. 276-297, октобар 2007, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00396.x/full, претражено 13. 04. 2013. године
68. Havenstein, Heather: “One in five employers uses social networks in hiring process“, 2008, http://www.computerworld.com/s/article/9114560/One_in_five_employers_uses_social_networks_in_hiring_process, претражено 29. 04. 2013. године
69. Hayden, Erik: „On Facebook, You are who you know“, 2010, http://www.psmag.com/culture-society/on-facebook-you-are-who-you-know-10385/, претражено 12. 08. 2012. године
70. Hensler-McGinnis, Nancy Felicity:” Cyberstalking victimization: impact and coping responses in a national University sample”, 2008,

http://drum.lib.umd.edu/bitstream/1903/8206/1/umi-umd-5402.pdf, претражено 12. 12. 2014. године

71. Hinduja, Sameer, Patchin, W.Justin:"Bullying, cyberbullying, and suicide", Archive of Suicide Research, 2010; volume 14(3), стр.206-221, http://www.tandfonline.com/doi/full/10.1080/13811118.2010.494133#abstract , претражено 03. 10. 2014. године
72. Hinduja, Sumeer, Patchin, W.Justin:"Cyberbullying Fact Sheet: What You Need To Know About Online Aggression", http://www.cyberbullying.us/cyberbullying_fact_sheet.pdf, претражено 13. 03. 2015. године
73. Игњатовић, Ђорђе: „Теорије у криминологији", Правни факултет Универзитета у Београду, Београд, 2009.
74. Ивановић, Звонимир, Уљанов, Сергеј, Урошевић, Владимир: "Анализа феномена крађе идентитета", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28 - 30. 03. 2012, с. 143-156, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године
75. Jaishankar, K.: "Editorial: Establishing a Theory of Cyber Crimes", International Journal of Cyber Criminology, Vol 1 Issue 2 July 2007, http://www.cybercrimejournal.com/Editoriaijccjuly.pdf, претражено 28. 08. 2015. године
76. Jones, Steve, Millermaier, Sarah, Goya-Martinez, Mariana, Schuler, Jessica: "Whose Space is MySpace? A content analysis of MySpace profiles", Journal First Monday, vol.13 no.9, 2008, http://firstmonday.org/article/view/2202/2024, претражено 10. 07. 2014. године
77. Јокић, Мирела: „Дјечија порнографија као облик насиља над дјецом и високотехнолошког криминала", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28 - 30. 03. 2012, стр. 293-302, http://education.muprs.org/wp-

content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

78. Јовановић, Светлана: „Приватност и заштита података на интернету", Твининг пројекат ЕУ – зборник „Везе cyber криминала са иерегуларном миграцијом и трговином људима", Министарство унутрашњих послова Републике Србије, 2014. година, стр. 87-164, http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/Cyber%20kriminal,%20iregularne%20migracije%20i%20trgovina%20ljudima.pdf, претражено 23. 07. 2015. године
79. Јовашевић, Драган, Хашимбеговић, Тарик: „Кривичноправна заштита безбедности рачунарских података", http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-08.pdf, претражено 12. 03. 2014. године
80. Кешетовић, Желимир, Благојевић, Марија: „Интернет и тероризам", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28 -30.03.2012, стр. 43-52. , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године
81. Khaled Yacoub Oweis: „Syria blocks Facebook in Internet crackdown", извор Reuters – вест од 23. новембра 2007. године, http://www.reuters.com/article/2007/11/23/us-syria-facebook-idUSOWE37285020071123, претражено 10. 08. 2012. године
82. King, Jennifer, Lampinen, Airi, Smolen, Alex: " Privacy: Is There An App for That?", Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2011, https://www.truststc.org/pubs/864.html, претражено 23. 11. 2014. године
83. Klain, Eva, Davies, Heather, Hicks, Molly:"Child Pornography: The Criminal Justice System Response", Washington, DC: National Center for Missing and Exploited Children, 2001, https://www.ncjtc.org/NCJTC_Member_Resources/Public/Child%20Pornography%20Criminal%20Justice%20Response.pdf , претражено 15. 11. 2014. године

84. Кнежевић, Саша: „Кривично процесно право: општи део“, Ниш: Правни факултет, Центар за публикације, Ниш, 2015
85. Kosiński, Jerzy: „Cybercrime in Poland“, http://www.academia.edu/3878063/Cybercrime_in_Poland, претражено 16. 01. 2015. године
86. Ковачевић-Лепојевић, Марина: „Појам и карактеристике интернет зависности“, Специјална едукација и рехабилитација, Vol. 10, br. 4., Београд, http://www.casopis.fasper.bg.ac.rs/izdanja/SEIR2011/vol10br4/1Spec_Edu_i_Reh_ISTRAZIVANJA/4-Marina_Kovacevic_Lepojevic.pdf, претражено 09. 12. 2015. године
87. Ковачевић-Лепојевић, Марина, Лепојевић, Борко: “Жртве сајбер прогањања у Србији”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 89-108
88. Колико сам безбедна? – безбедоносне препоруке за жене и девојке, Аутономни женски центар, Организација за европску безбедност и сарадњу – мисија у Србији, 2015, стр.18-22
89. Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна, Костић, Миомира: “Криминологија”, 5. измењено и допуњено издање, Ниш: Правни факултет, Центар за публикације, 2012, стр. 178-182.
90. Костелић Мартић, Андреја: “Мобинг: психичко малтретирање на радном месту”, Школска књига, Загреб, 2005.
91. Kowalski, Melanie:”Cyber-Crime: Issues, data sources, and feasibility of collecting police-reported statistic”, Cat no. 85-558, Canadian Centre fot Justice Statistic, 2002, http://www.statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf, претражено 01. 11. 2012. године
92. Krasnova, Hanna, Gunther, Oliver, Spiekermann, Sarah, Koroleva, Ksenia:”Privacy concerns and identity in online social Networks”, Identity in the Information Society, vol. 2, no.1, 2009, стр.39-63, http://download.springer.com/static/pdf/675/art%253A10.1007%252Fs12394-009-0019-1.pdf?auth66=1424106684_18f9ff6659fd034e563c2b1309efc0ba&ext=.pdf, приступ 23. 11. 2014. године

93. Кушић, Синиша: „Online друштвене мреже и друштвено умрежавање код ученика основне школе: навике facebook генерације", Живот и школа, бр. 24 (2/2010.), год. 56, стр. 103– 125
94. Lange, G. Patricia: "Publicly Private and Privately Public: Social Networking on YouTube", Journal of Computer-Mediated Communication volume 13 - International Communication Association, 2008, стр. 361–380, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00400.x/pdf, претражено 02. 05. 2014. године
95. Lella, Adam: „Average Time Spent on Social Networking Sites Across Geographies", ComScore Insights - ComScore Media Metrix, јуни 2011., http://www.comscore.com/Insights/Data-Mine/Average-Time-Spent-on-Social-Networking-Sites-Across-Geographies, претражено 12. 06. 2014. године
96. Lenhart, Amanda: "Data Memo: Cyberbullying and Online Teens", http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf, претражено 03. 10. 2014. године
97. Lenhart, Amanda, Madden, Mary: „Social Networking Websites and Teens: An Overview", Pew Internet & and American Life Project (2007), http://www.pewinternet.org/2007/01/07/social-networking-websites-and-teens/, претражено 15. 07. 2014. године
98. Lewis, A., James: "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies, Washington DC, 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, претражено 24. 10. 2015. године
99. Lipsman, Andrew: „Social networking goes global", ComScore press release, јули 2007., http://www.comscore.com/Insights/Press-Releases/2007/07/Social-Networking-Goes-Global, претражено 12. 06. 2014. године
100. Littlejohn Shinder, Debra: "Scene of the Cybercrime: Computer Forensics Handbook", 2002, http://www.dvara.net/hk/Syngress%20Scene%20of%20the%20CyberCrime.pdf, претражено 24. 10. 2015. године

101. Lunden, Ingrid: "Instagram Is The Fastest-Growing Social Site", објављено 21. 01. 2014. године, http://goo.gl/TSJM3C, претражено 09. 07. 2014. године
102. Lutgen-Sandvik, Pamela: "Take This Job and ... : Quitting and Other Forms of Resistance to Workplace Bullying", Routledge, Communication Monographs, Vol. 73, No. 4, December 2006
103. Љепава, Николина: "Реално злостављање у виртуелном окружењу: Превенција и интервенција у случајевима злостављања дјеце на интернету", Часопис Актуелности, стр. 22–33, 2011, Бања Лука: Бања Лука колеџ, http://www.roditelj.org/wp-content/uploads/2011/12/aktuelnosti-2011-sajberzlostavljanje-nljepava-1.pdf, претражено 24. 03. 2015. године
104. MacKinnon, Catharine: „Toward a Feminist Theory of the State", Cambridge: Harvard University Press, 1989, http://books.google.co.uk/books/about/Toward_a_Feminist_Theory_of_the_State.html?id=Shn5xHywtHIC, претражено 18. 02. 2015. године
105. Малетић, Варвара, Дакић, Јелена: „Интернет, социјалне мреже и људска права", INFOTEH-JAHORINA Vol. 11, 2012, стр. 771 – 776, http://infoteh.etf.unssa.rs.ba/zbornik/2012/radovi/RSS-5/RSS-5-8.pdf, претражено 06. 08. 2015. године
106. Маричић, Татјана, Ковачевић, Верица: „Вршњачко – дигитално насиље и начини превазилажења", Зборник радова - Међународна научностручна конференција „Вршњачко насиље (етиологија, феноменологија, начини превазилажења и компаративна искуства)", Висока школа унутрашњих послова, Бања Лука, 2013. стр. 233-211, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Vrsnjacko-nasilje.pdf, претражено 14. 10. 2014. године
107. Mattice, M.Catherine: "Proactive Solutions for Workplace Bullying: Looking at the Benefits of Positive Psychology", 2010, http://www.thefreelibrary.com/Helping+targets+%26+their+employers+effectively+resolve+workplace...-a0263658932, претражено 03. 05. 2013. године
108. Матијашевић, Јелена, Спалевић, Жаклина, Игњатијевић, Светлана: „Врсте интернет превара - појам, значај и утицај на економске и моралне аспекте друштвене заједнице", ИНФОТЕХ-ЈАХОРИНА Вол. 11, 2012,

стр. 562 – 565, http://www.academia.edu/3061962/Vrste_internet_prevara-pojam_zna%C4%8Daj_i_uticaj_na_ekonomske_i_moralne_aspekte_dru%C5%A1tvene_zajednice, претражено 01. 04. 2015. године

109. McCown, Frank, Nelson, L. Michael: „What happens when facebook is gone?“, In Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries, стр.251-254. ACM, 2009, http://www.cs.odu.edu/~mln/pubs/jcdl09/archiving-facebook-jcdl2009.pdf, претражено 15. 02. 2015. године
110. McFarlane, Leroy , Bocij, Paul :”An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers”, Journal First Monday, 2005, volume 8, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/1076/996/, претражено 02. 03. 2013. године
111. McGrath, Michael, Casey, Eoghan: “Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace”, 30. journal of the American Academy of Psychiatry and the Law 81, Volume 30, Number 1, 2002, http://www.jaapl.org/content/30/1/81.full.pdf+html, претражено 02. 03. 2013. и 12. 09. 2014. године године
112. McGuire, Brian, Wraith, Anita: “Legal and psychological aspects of stalking: A review”, Journal of Forensic Psychiatry, volume 11 no.2, 2000.
113. McKim, Jennifer: “Pimp Pleads Guilty to Prostituting Minor”, Orange County Register, 2006, http://www.ocregister.com/ocregister/news/atoz/article_1209170.php, претражено 10. 09. 2014. године
114. Миладиновић, Александар, Петричевић, Витомир: „Електронско вршњачко насиље”, Зборник радова - Међународна научностручна конференција “Вршњачко насиље (етиологија, феноменологија, начини превазилажења и компаративна искуства)”, Висока школа унутрашњих послова, Бања Лука, 2013, стр. 245-258, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Vrsnjacko-nasilje.pdf, претражено 14. 10. 2014. године
115. Миладиновић, Александар, Петричевић, Витомир: „Криминогени аспект друштвених мрежа“, Зборник радова, међународна научностручна

конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012, стр. 257-270, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

116. Милић, Ненад: „Место извршења кривичног дела у теоријским промишљањима“, Журнал за криминалистику и право НБП, scindeks-clanci.ceon.is/data/pdf/0354-88721401141M претражено 09. 12. 2015. године
117. Милићевић, Слободанка, Вујовић, Срђан: “Проблем савремене доби: облици крађе и злоупотребе идентитета и мјере превенције”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012, стр. 303-316, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године
118. Мирић,Филип: „Облици вршњачког насиља путем интернета и друштвених мрежа”, Зборник радова - Међународна научностручна конференција “Вршњачко насиље (етиологија, феноменологија, начини превазилажења и компаративна искуства)”, Висока школа унутрашњих послова, Бања Лука, 2013, стр. 397-408, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Vrsnjacko-nasilje.pdf, претражено 14. 10. 2014. године
119. Mishna, Faye, McLuckie, Alan, Saini, Michael:”Real-world dangers in an online reality: a qualitative study examining online relationships and cyber abuse”, Social Work Research, 2009; volume 33, number 2, стр.107-118, http://icbtt.arizona.edu/sites/default/files/Mishna,_McLuckie,_&_Saini_Social_Work_Research_KHP_Cyber_Abuse_0.pdf, претражено 13. 03. 2015. године
120. Mislove, Alan, Marcon, Massimiliano, Gummadi, P. Krishna, Druschel, Peter, Bhattacharjee, Bobby: “Measurement and Analysis of Online Social Networks”, http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf , претражено 11. 03. 2015. године

121. Mohamed, Azza Abdel-Azim: "Online Privacy Concerns Among Social Networks'Users", Cross-cultural communication, Vol. 6, No. 4, 2010, стр. 74-89, www.cscanada.org, претражено 03. 04. 2014. године
122. Molokomme, L. Athaliah: „The Botswana Experience with cybercrime legislation and other measures", Speaking notes at the opening session of the Octopus Conference on Cooperation Against Cybercrime - Strasbourg, France, 6th June, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus2012/presentations/Octopus_2012_Botswana.pdf, претражено 20. 11. 2014. године
123. Mullen E.Paul, Pathe, Michele, Purcell, Rosemary: „Stalkers and their Victims. Cambridge University Press", 2009, https://books.google.rs/books?hl=sr&lr=&id=Kir_ypPb7IQC&oi=fnd&pg=PR11&dq=Mullen,+Pathe+and+Purcell+Stalkers+and+their+Victims&ots=HG0TrlavDC&sig=65ass5vvLW1o5aRWsaL2uW0Qlc8&redir_esc=y#v=onepage&q=Mullen%2C%20Pathe%20and%20Purcell%20Stalkers%20and%20their%20Victims&f=false, претражено 24. 11. 2014. године
124. Никић, Срђан: „Најчешће методе напада cyber криминалаца и како се одбранити", http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf, претражено 25. 10. 2014. године
125. Николић Комлен, Лидија, Гвозденовић, Радоје, Радуловић, Саша, Милосављевић, Александар, Јерковић, Ранко, Живковић, Владан, Живановић, Саша, Рељановић Марио; Алексић Иван: „Кратак приказ развоја правне регулативе о високотехнолошком криминалитету на међународном нивоу", Сузбијање високотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010.
126. Николић, Милан: „Практични аспекти заштите приватности корисника и безбедности електронских комуникационих мрежа и услуга у Србији", http://www.telekomunikacije.rs/arhiva_brojeva/peti_broj/milan_nikolic:_prakticni_aspekti_zastite_privatnosti_korisnika_i_bezbednosti_elektronskih_komunikacionih_mredja_i_usluga_u_srbiji_.305.html, претражено 15. 06. 2014. и 30. 07. 2014. године

127. Николић, Слађан: „Случај економског бироа КОНЕКО-аларм за узбуну", APIS Security Consulting, http://www.apisgroup.org/sec.html?id=26, претражено 08. 06. 2012. године
128. Nourten, Thomas:"Vandalism or Prank?", edicija: Computers under attack: intruders, worms, and viruses, Association for Computing Machinery Publications, New York, 1990, str. 522-523
129. O'Donovan, Eamonn:"Sexting and student discipline", District Administration, 2010; volume 46, numeber 3, стр. 60-64, http://www.districtadministration.com/article/sexting-and-student-discipline, претражено 14. 03. 2015. године
130. O'Leary, J.Robert, D'Ovidio, Robert: "Online sexual exploitation of children", The International Association of Computer Investigative Specialists, 2007, http://www.nga.org/files/live/sites/NGA/files/pdf/0703ONLINECHILD.PDF, претражено 27. 03. 2015. године
131. Paget, Francois: „Identity theft", McAfee Avert Labs technical white paper No 1., 2007, http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf, претражено 01. 12. 2014. године
132. Parker, Don: "Fighting computer crime", New York, 1983
133. Patchin, W. Justin, Hinduja, Sameer:"Cyberbullying and self-esteem", http://www.cyberbullying.us/cyberbullying_and_self_esteem_research_fact_sheet.pdf, претражено 03. 10. 2014. године
134. Patchin, W.Justin, Hinduja, Sameer:"Bullies move beyond the schoolyard: a preliminary look at cyberbullying", Youth Violence Juvenile Justice, 2006; volume 4, number 2, стр.148-169, https://www.ncjrs.gov/App/publications/abstract.aspx?ID=234986, претражено 13. 03. 2015. године
135. Pathé, Michele, Mullen, Paul E., Purcell, Rosemary: „Management of victims of stalking", 2001, http://apt.rcpsych.org/content/7/6/399.full , претражено 07. 06. 2014. године
136. Perry, Jennifer: „Digital Stalking: A guide to technology risks for victims", 2012, Women's Aid, National Stalking Service and Nominet Trust,

http://www.womensaid.org.uk/core/core_picker/download.asp?id=3492, претражено 17. 09. 2014. године

137. Petherick, Wayne : ”Cyberstalking: Obsessional pursuit and the digital criminal,” 2001, http://www.crimelibrary.com/criminology/cyberstalking/index.html, претражено 14. 11. 2014. године
138. Петровић, М. Никола: „Ставови младих према сајбер вандализму”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр.3, година 12, септембар 2009, стр. 75-87
139. Петровић, Слободан: „Компјутерски криминал”, МУП Републике Србије , 2001,стр.115-200, претражено 24. 10. 2015. године
140. Pettinari, Dave: “Cyberstalking investigation and prevention“, http://www.crime-research.org/library/Cyberstalking.htm, претражено 03. 08. 2014. године
141. Писарић, Милана: „Претресање рачунара ради проналажења електронских доказа“, Зборник радова Правног факултета у Новом Саду, 1/2015
142. Pittaro, L. Michael: “Cyber stalking: An Analysis of Online Harassment and Intimidation”, International Journal of Cyber Criminology, Vol 1 Issue 2, 2007, стр. 180–197, http://www.cybercrimejournal.com/pittaroijccvol1is2.htm, претражено 10. 05. 2014. године
143. Поповић, Драган, Вучановић, Драган, Лазаревић, Ристо: „Имплементација стандарда серије ISO/IEC 27000 као мјера сузбијања високотехнолошког криминала”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 157-168 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године
144. Поповић-Ћирић, Бранислава: „Вршњачко насиље у сајбер простору”, ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр.3, година 12, септембар 2009, стр. 43-62

145. Поробић, Миралем, Барјактаревић, Мирсад: „Cyber crime, pranje novca i finansijske istrage“, http://pravosudje.ba/vstv/faces/pdfservlet;jsessionid=d740751503b9f050afe655ea08e6d17ddc0412e00b660550df17d03959a09f65.e34TbxyRbNiRb40Qb34MahuLaNv0?p_id_doc=20568, претражено 24. 07. 2015. године
146. Posner, Richard :“The Economics of Justice“, Cambridge: Harvard University Press, 1981, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2449&context=faculty_scholarship, претражено 18. 02. 2015. године
147. Практикум о компјутерском криминалитету (The Computer Crime: Criminal Justice Resource Manual), US Department of Justice/ National Institute of Justice/Office of Justice Programs, уредник Donn B. Parker, објављен 1979 - друго издање из 1989. године, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf, претражено 29. 11. 2014. године
148. Prensky, Marc: “Digital Natives, Digital Immigrants”, On the Horizon vol. 9 no. 5, 2001, http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf, претражено 03. 07. 2015. године
149. Прља, Драган, Дилигенски , Андреј: „Фејсбук и заштита података у ЕУ”, Страни правни живот 3/2012, Институт за упоредно право, Београд, стр. 190-220, http://www.comparativelaw.info/spz20123.pdf, претражено 12. 06. 2014. године
150. Прља, Драган, Ивановић, Звонимир, Рељановић, Марио: „Кривична дела високотехнолошког криминала”, Институт за упоредно право, Београд, 2011.
151. Прља, Драган, Рељановић, Марио, Ивановић, Звонимир: „Интернет право“, Институт за упоредно право, Београд, 2012.
152. Прља, Драган, Рељановић, Марио: „Високотехнолошки криминал – упоредна искуства”, Страни правни живот бр.3/09, Београд, стр.161-184, http://www.comparativelaw.info/spz20093.pdf, претражено 15. 09. 2015. године

153. Протрка, Никола, Грубер, Кристијан, Салопек, Данко: „Сувремени начини пријављивања искоришћавања или злостављања дјеце путем интернета“, 4th International Scientific and Professional Conference „Police College Research Days in Zagreb“, 2015, str. 646-661, http://www.researchgate.net/profile/Nikola_Protrka/publication/275519088_Suvremeni_naini_prijavljivanja_iskoritavanja_ili_zlostavljanja_djece_putem_interneta__Modern_methods_of_reporting_exploitation_or_abuse_of_children_via_the_Internet/links/553e20640cf2522f1835ee79, претражено 23. 08. 2015. године

154. Путник, Ненад, Гаврић, Невена: „Мере и стратегије заштите информационих система од високотехнолошког криминала”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 217-226 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21.07.2015. године

155. Радновић, Бранислав, Илић, Милена, Радовић, Немања: „Економски сајбер криминал у Србији – аспект заштите интернет потошача”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012. , стр. 129-142, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

156. Radwanick, Sarah: „Young European Women Spent Most Time on Social Networks“, ComScore Insights, јуни 2011, http://www.comscore.com/Insights/Data-Mine/Young-European-Women-Spent-Most-Time-on-Social-Networks, претражено 12. 06. 2014. године

157. Ранђеловић, Драган, Бајагић, Младен, Царевић, Бојана: „Интернет у функцији тероризма”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 317-330, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

158. Roberts, Lynne: „Cyber-Victimisation in Australia:Extent, Impact on Individuals and Responses“, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan036070.pdf, претражено 01. 12. 2014. године

159. Rodriguez, A., Carlos: “Cyber terrorism – A rising threath in the Western hemisphere”, Fort Lesley J. McNair, Washington DC, 2006, http://www.library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf, претражено 17. 07. 2015. године

160. Roller, Emma: „This is what secton 215 of the Patriot Act does“, www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html, претражено 09. 04. 2015. године

161. Ромић, Миодраг; Грбић-Павловић Николина: Међународноправни документи којима се уређује област високотехнолошког криминала, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 193-206, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године

162. Rushe, Dominic: “Icelandic MP Fights US Demand for Her Twitter Account Details“, The Guardian, January 8, 2011, http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages, приступ 04. 08. 2012. године

163. Самчовић, Андреја: „Безбедност друштвених мрежа са освртом на Twitter“, INFOTEH-JAHORINA Vol. 12, 2013, стр. 860 – 863, http://infoteh.etf.unssa.rs.ba/zbornik/2013/radovi/RSS-5/RSS-5-9.pdf, претражено 06. 08. 2015. године

164. Sacco, N. Lisa: “The Violence Against Women Act: Overview, Legislation, and Federal Funding”, https://fas.org/sgp/crs/misc/R42499.pdf, претражено 16. 01. 2015. године

165. Schement,Jorge Reina, Curtis, Terry: “Tendencies and tensions of the information age: The production and distribution of information in the United States”, New Brunswick, N.J.: Transaction Publishers, 1995, https://books.google.rs/books?id=PzlLOqLko5cC&pg=PR4&lpg=PR4&dq=T

endencies+and+tensions+of+the+information+age:+The+production+and+distribution+of+information+in+the+United+States%22,+New+Brunswick,+N.J.:+Transaction+Publishers,+1995&source=bl&ots=m-IJ9Z-5XE&sig=iEzjOOcvhpLvlXy9EAH1lM71OIA&hl=sr&sa=X&ei=j7HHVP63JKnlywO2z4CIBw&ved=0CCcQ6AEwAg#v=onepage&q=Tendencies%20and%20tensions%20of%20the%20information%20age%3A%20The%20production%20and%20distribution%20of%20information%20in%20the%20United%20States%22%2C%20New%20Brunswick%2C%20N.J.%3A%20Transaction%20Publishers%2C%201995&f=false, претражено 15. 01. 2015. године

166. Schjolberg, Stein, Hubbard, M. Amanda: „Harmonizing National Legal Approaches on Cybercrime“, стр.3, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity , Document: CYB/04, 2005, http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf, претражено 29. 11. 2014. године
167. Schjolberg, Stein: „The History of Global Harmonization on Cybercrime legislation - The Road to Geneva“, децембар 2008, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf , претражено 20. 11. 2013. године
168. Schjolberg, Stein: „The history of cybercrime 1979-2014“, Cybercrime research Institute vol.9, 2014, str. 44, https://books.google.rs/books?id=hmiWBQAAQBAJ&pg=PA44&lpg=PA44&dq=The+High+Tech+Subgroup+of+the+G-8%27s+Senior+Experts+on+Transnational+Organized+Crime&source=bl&ots=K0vra34c11&sig=EvmCdwB-v-xHd5x9jDv0Ct86_qE&hl=sr&sa=X&ved=0CCYQ6AEwAWoVChMIgKzOprm6xwIVRT0aCh2yxAOC#v=onepage&q=The%20High%20Tech%20Subgroup%20of%20the%20G-8's%20Senior%20Experts%20on%20Transnational%20Organized%20Crime&f=false, претражено 20. 08. 2015. године
169. Shah, Mahmood: “Online Social Networks: Privacy Threats and Defenses”, Springer, vol. XVI, 2013, http://www.springer.com/978-3-7091-0893-2, претражено 12. 02. 2015. године

170. Shahi, Afshin: „Iran's digital war", Daily News Egypt – вест од 27.07.2008.године, http://dailystaregypt.com/article.aspx?ArticleID=15313, претражено 10. 08. 2012. године
171. Sheridan P.Lorraine, Grant,T.: "Is cyberstalking different?", Psychology, Crime & Law, volume 13 no.6, 2007, стр.627-640, http://www.tandfonline.com/doi/full/10.1080/10683160701340528 , претражено 02. 03. 2013. године
172. Sieber, Ulrich: „Legal Aspects of Computer-related crime in the Information society- COMCRIME Study", The European Comission, 1998, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, претражено 04. 12. 2014. године
173. Симовић, Владимир: „Социјални и правни контекст рачунарства", Висока школа струковних студија за информационе технологије, Београд, 2010.
174. Синђелић, Жарко: „Право на приватност – кривичноправни, кривичнопроцесни и криминалистички аспекти, докторска дисертација, Београд, 2012., www.doiserbia.nb.rs/phd/university. aspx?-BG20107404sinđelić, претражено 22. 10. 2015. године
175. Спалевић, Жаклина: „Карактеризација психолошког злостављања у cyber простору", INFOTEH-JAHORINA Vol.12, March 2013, infoteh.elf.unssa.rs.ba/zbornik/2013/radovi/RSS-3/RSS-3-9.pdf. претражено 14. 12. 2015. године
176. Спасић, Видоје: „Актуелна питања у области сајбер криминала", Билтен судске праксе Врховног суда Србије, Београд: Intermex, 2006. - бр. 1 (2006), стр. 107-130
177. Спасић, Видоје: „Неки аспекти приватности у сајберспејсу", Зборник Правног факултета у Нишу, Ниш: Правни факултет, 2005. - бр. 46 (2005), стр. 207-228
178. Спасић, Видоје: „Онлајн безбедност", Зборник Правног факултета у Нишу, Ниш: Правни факултет, Центар за публикације, 2010. - бр. 56 (2010), стр. 77-102
179. Спасић, Видоје, Васић, Александра: „Стеганографија у функцији заштите података на Интернету", Зборник Правне инфраструктурне

основе за развој економије засноване на знању, Крагујевац: Правни факултет, 2012, стр. 257-274

180. Spinello, Richard:"Privacy and Social Networking Technology", International Review of Information Ethics Vol. 16 (12/2011), стр.44, http://www.i-r-i-e.net/inhalt/016/spinello.pdf, претражено 01. 03. 2013. године
181. Стевановић, Ивана: „Кривична дела везана за искоришћавање деце у порнографске сврхе злоупотребом рачунарских система и мрежа (међународни и домаћи кривичноправни оквир)", ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 27-41
182. Stocking, Ben: „Vietnam Internet users fear Facebook blackout", Associated Press – вест од 17. 11. 2009. године, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/11/17/international/i033256S37.DTL, претражено 10. 08. 2012. године
183. Сулер, Џон: „Ефекат онлајн дезинхибиције", Е-волуција, бр.11, 2005, http://www.bos.rs/cepit/evolucija/html/11/e-dezinhibicija.htm, претражено 28. 10. 2015. године
184. Сурцо, Рамо: „Право на приватност с посебним освртом на интернетску друштвену мрежу Facebook", www.rijaset.ba/.../05_pravo_na _privatnos..., претражено 20. 10. 2015. године
185. Szde,Yu: „Анализа узрока понашања на facebooku, тест сајбер профилисања", www.defendologija-banjaluka.com/defendologija33/2srp.pdf, претражено 09. 12. 2015. године
186. Шетка, Гојко; Ратковић, Жељко: „Високотехнолошки криминал у Републици Српској", Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., стр. 207-216, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, претражено 21. 07. 2015. године
187. Шурлан, Тијана: Међународноправна заштита права на приватност, www.spmisao.rs/mp-content/uploads/2014/03-tijana-surlan-pdf. претражено 28. 10. 2015. године

188. Тањевић, Наташа: „Компјутерски криминал − правна заштита на националном нивоу", Безбедност - Часопис Министарства унутрашњих послова Републике Србије, број 1-2/2009, 2009, стр. 152-166

189. Taylor, Chris: "Social networking 'utopia' isn't coming", CNN интернет емисија од 27. 6. 2011.године, http://articles.cnn.com/2011-06-27/tech/limits.social.networking.taylor_1_twitter-users-facebook-friends-connections?_s=PM:TECH, претражено 10. 08. 2012. године

190. The Computer Crime: Criminal Justice Resource Manual, US Department of Justice/ National Institute of Justice/Office of Justice Programs, уредник Donn B. Parker, 1979 - друго издање из 1989. године, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf, претражено 29. 11. 2014. године

191. Thomson, Judith Jarvis: "The Right to Privacy", Philosophy and Public Affairs, vol.4, стр. 295–314, 1975, http://www.eecs.harvard.edu/cs199r/readings/thomson1975.pdf, претражено 18. 02. 2015. године

192. Tjaden, Patricia: "The crime of stalking: How big is the problem?", National Institute of Justice - Research preview, Washington DC, National Institute of Justice, 1997

193. Tjaden, Patricia, Thoennes, Nancy: "Stalking in America: Findings from the National Violence Against Women Survey", Washington DC, National Institute of Justice and US Departman of Jusice, 1998

194. Tjapa, Anju, Kumar, Raj: "Cyberstalking: Crime and Challenge at the Cyberspace", International journal of Computing and Business Research, vol.2 issue 1, 2011, стр. 5, http://www.researchmanuscripts.com/PapersVol2N1Jan2011/1.pdf, претражено 02. 03. 2013. године

195. Томић, Наташа, Петровић, Далибор: „Друштвено умрежавање и заштита приватности корисника интернета", XXVII Симпозијум о новим технологијама у поштанском и телекомуникационом – PosTel 2009, Београд, http://postel.sf.bg.ac.rs/downloads/simpozijumi/POSTEL2009/RADOVI%20PDF/Menadzment%20procesa%20u%20postanskom%20i%20telekomuikacion

om%20saobracaju/9.%20N.%20Tomic,%20D.%20Petrovic.pdf, претражено 05. 08. 2015. године

196. Tracy, Lutgen-Sandvik, Alberts Nightmares, Demons and Slaves, Exploring the Painful Metaphors of Workplace Bullying, 2006, Sage Publications - Management Communication Quarterly, 20(2)
197. Урошевић, Владимир, Уљанов, Сергеј, Вуковић, Радоје: „Полиција и високотехнилошки криминал– Примери из праксе и проблеми у раду МУП-а Републике Србије“, Министарство унутрашњих послова Републике Србије, http://www.singipedia.singidunum.ac.rs/attachment.php?attachmentid=1042&d=1278689423, претражено 12. 10. 2015. године
198. Utz, Sonja, Kramer, C. Nicole: “The privacy paradox on social network sites revisited: The role of individual characteristics and group norms”, Cyberpsychology: Journal of Psychosocial Research on Cyberspace, volume 3, number 2, article 1, 2009, http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1, претражено 10. 12. 2014. године
199. Vandebosch, Heidi, Van Cleemput, Katrein: “Defining cyberbullying: a qualitative research into the perceptions of youngsters”, CyberPsychology & Behavior, 2008, volume 11, number 4, стр. 499-503, http://thecyberbullyingproblem.wikispaces.com/file/view/33985751.pdf, претражено 13. 03. 2015. године
200. Видановић, Иван: „Речник социјалног рада“, Удружење стручних радника социјалне заштите Србије, Друштво социјалних радника Србије, Асоцијација центра за социјални рад Србије, Унија Студената социјалног рада, 2006, Београд, стр. 437-438
201. Viégas, B. Fernanda: “Blogger’s expectations of privacy and accountability: An initial survey”, Journal of Computer–Mediated Communication, volume 10, number 3, 2005, http://jcmc.indiana.edu/vol10/issue3/viegas.html, претражено 23. 05. 2014. године
202. Вугделија, Наталија, Савић, Ана, Савић Срђан: „Безбедност рачунарских система у савременом електронском пословању”, http://infoteh.etf.unssa.rs.ba/zbornik/2011/radovi/E-III/E-III-10.pdf, претражено 06. 08. 2013. године

203. Вујновић, Андреа: "Како информацијско-комуникацијска технологија утјече на женска права", Vox Feminae 3-8/11/2015, http://www.voxfeminaes.net/feministyle/item/7420-kako-informacijsko-kominikacijska-tehnologija-utječe-na-ženska-prava, претражено 02. 11. 2015. године

204. Вулетић, Дејан: „Трговина људским органима у сајбер простору", ТЕМИДА – часопис о виктимизацији, људским правима и роду, бр. 3, година 12, септембар 2009, стр. 63-74

205. Wagner, R. Abraham: "Fighting Terror in Cyberspace, Terrorism and the internet: use and abuse", https://books.google.rs/books?id=yf83KZZbeQIC&pg=PA1&lpg=PA1&dq=Wagner,+A.,+R.:+%22Fighting+Terror+in+Cyberspace,+Terrorism+and+the+internet:+use+and+abuse&source=bl&ots=OcEV_qWD_5&sig=o4qzKdNYafWWEKAby_yuksVhApM&hl=sr&sa=X&ved=0ahUKEwj3yIvsoOrJAhVC1RoKHSU6DMQQ6AEIITAB#v=onepage&q=Wagner%2C%20A.%2C%20R.%3A%20%22Fighting%20Terror%20in%20Cyberspace%2C%20Terrorism%20and%20the%20internet%3A%20use%20and%20abuse&f=false, претражено 17. 07. 2015. године

206. Weimann, Gabriel: „ Cyber terrorism - How Real Is the Threat?", Special report 119, United States Institute of Peace, Washington, DC, 2004, http://www.usip.org/files/resources/sr119.pdf, претражено 17. 07. 2015. године

207. Westin, Alan.: "Privacy and Freedom", Bodley Head, London, 1970, http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr, претражено 18. 02. 2015. године

208. Williams, R.Kirk, Guerra, G.Nancy:"Prevalence and predictors of internet bullying", Journal of Adolescent Health, 2007; volume 41 number 6, стр.S14-S21, http://www.slideshare.net/WCT-Law/fp-58-prevalence-and-predictors-of-internet-bullying , претражено 14. 03. 2015. године

209. Wilson, Clay: "Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress", CRS Report for Congress, 2005, http://fpc.state.gov/documents/organization/45184.pdf, претражено 17. 07. 2015. године

210. Wilson, Debbie et al.:"Fraud and Technology Crimes: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources, Home Office Online Report, 2006, стр. 8, http://webarchive.nationalarchives.gov.uk/20110220105210/rds.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf , претражено 04. 11. 2012. године

211. Willard, E.Nancy:"Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threats, and Distress", Champaign, IL: Research Press; 2007, https://books.google.rs/books?id=VyTdG2BTnl4C&pg=PP6&lpg=PP6&dq=Cyberbullying+and+Cyberthreats:+Responding+to+the+Challenge+of+Online+Social+Cruelty,+Threats,+and+Distress&source=bl&ots=u5DlZGvo8v&sig=7dA7kdGtX-4VrWUMqychrTkYLk8&hl=sr&sa=X&ei=Fb8FVbbgJsfVavKLgYgO&ved=0CEsQ6AEwBQ#v=onepage&q=Cyberbullying%20and%20Cyberthreats%3A%20Responding%20to%20the%20Challenge%20of%20Online%20Social%20Cruelty%2C%20Threats%2C%20and%20Distress&f=false, претражено 14. 03. 2015. године

212. Willard, Nancy: "An Educator's Guide to Cyberbullying and Cyberthreats", http://miketullylaw.com/library/cbcteducator.pdf, претражено 13. 03. 2015. године

213. Wolak, Janis, Mitchell, Kimberly, Finkelhor, David: "Internet Crimes Against Minors: The Response of Law Enforcement", Washington, DC: National Center for Missing & Exploited Children, 2003, https://www.ncjrs.gov/App/abstractdb/AbstractDBDetails.aspx?id=202909, претражено 23. 03. 2015. године

214. Wolak, Janis, Mitchell, Kimberly, Finkelhor, David: "Online Victimization of Youth: Five Years Later", Washington, DC: National Center for Missing & Exploited Children, 2006., http://www.unh.edu/ccrc/pdf/CV138.pdf, претражено 27. 03. 2015. године

215. Урошевић, Владимир: „Нигеријска превара у Републици Србији", часопис Безбедност, бр. 3, 2009, http://www.mup.gov.rs/cms/resursi.nsf/Nigerijska_prevara.pdf, претражено 17. 01. 2014. године

216. Yar, Majid: "Cybercrime and society", SAGE Publications, London, 2006.

217. Yar, Majid: "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", European Journal of Criminology, October 2005 vol. 2 no. 4, стр. 407-427, http://www.sagepub.in/upm-data/27202_6.pdf, претражено 28. 08. 2015. године

218. Ybarra, L.Michaele, Espelage, L.Dorothy, Mitchell, J.Kimberly:"The co-occurrence of Internet harassment and unwanted sexual solicitation victimization and perpetration: associations with psychosocial indicators", Journal of Adolescent Health, 2007; volume 41, стр. S31-S41, http://www.ncbi.nlm.nih.gov/pubmed/18047943, претражено 14. 03. 2015. године

219. Ybarra, L.Michaele, Mitchell, J.Kimberly:"Prevalence and frequency of Internet harassment instigation: implications for adolescent health", Journal of Adolescent Health, 2004, volume 41 number 2, стр. 189-195, http://www.unh.edu/ccrc/pdf/CV157.pdf, претражено 14. 03. 2015. године

220. Ybarra, L.Michaele, Diener-West, Marie, Leaf, J.Phillip:"Examining the overlap in Internet harassment and school bullying: implications for school intervention", Journal of Adolescent Health, 2007; volume 41, стр. S42-S50, http://www.wthlawfirm.com/for-parents/links/examining-overlap-internet-harassment-school-bullying/ ,претражено 14. 03. 2015. године

221. Zona, A. Michael, Sharma, S. Krunal. , Lane, C. John: "A comparative study of erotomanic and obsessional subjects in a forensic sample," Journal of Forensic Sciences, volume 38, 1993, стр. 894-903.

222. Zucker, Susan: " Cyber Forensics: Part II", National Clearinghouse for Science, Technology and the Law at Stetson University, College of Law, http://www.ncstl.org/evident/Jan08Zucker, претражено 28. 08. 2015. године

223. Жикић, Биљана: „О online комуникацији: интервју са др Снјежаном Миливојевић", Српски културни центар "Данило Киш", http://dkis.si/o-online-komunikaciji-intervju-sa-prof-dr-snjezanom-milivojevic/, претражено 08. 11. 2015. године

224. Жунић-Павловић, Весна, Ковачевић-Лепојевић, Марина, Ментус, Татјана: „Негативне последице социјалног умрежавања на интернету", Комуникација и људско искуство – тематски зборник радова, Филозофски факултет Универзитета у Нишу, 2013, стр. 137-150

225. Жунић Павловић, Весна, Ковачевић Лепојевић, Марина: „Интерперсонално насиље у „cyber“простору”, Истраживања у специјалној педагогији, факултет за специјалну едукацију и рехабилитацију, Београд, 2009.
226. Жене за живот без насиља: приручник за волонтерке СОС телефона, Београд: Буфала Бил, 2. издање, 1999.

Законски, правни документи и документи међународних организација

1. Акциони план за заштиту критичне информационе инфраструктуре „Заштита Европе од бројних кибернетичких напада и ометања: побољшати спремност, безбедност и отпорност“ – Communication on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, secuirty and resilience”, 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, претражено 21. 11. 2014. године
2. Глобална платформа о сајбер сигурности Међународне телекомуникационе уније (Global Cybersecurity Agenda (GCA) of the International Telecommunication Union), www.itu.int/osg/csd /cybersecurity/gca, претражено 11. 11. 2014. године
3. Директива 2002/58/ЕС о обради података о личности и заштити приватности у сектору електронских комуникација – Директива о приватности и електронским комуникацијама (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, 2002, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN, претражено 21. 11. 2014. године и 18. 02. 2015. године
4. Директива 95/46/ЕС Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046, 1995, претражено 18. 02. 2015. године и http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012, претражено 18. 02. 2015. године
5. Директива 97/66/ЕС Европског парламента и Савета о обради података о личности и заштити приватности у телекомуникационом сектору

(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML, претражено 18. 02. 2015. године

6. Directive 2013/40/EU of the European Parliament and of the Council 12.8.2013., Offical Journal of the European Union 218/8, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040, претражено 19. 08. 2015. године
7. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024, претражено 17. 08. 2015. године
8. Директива Савета Европске заједнице о правној заштити компјутерских програма (Council Directive of 14.may 1991. On the legal proctection of computer Programs) са обавезном применом у државама чланицама ЕУ почев од 01.01.1993. године, Службени лист Европске заједнице бр. Л 122/42“ од 17. 05. 1991. године.
9. Додатни протокол уз Конвенцију Савета Европе о високотехнолошком криминалитету бр.185 који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених путем компјутерских система (Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems), 2005., http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, претражено 09. 07. 2014. године
10. Европска Конвенција о људским правима (Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5)), http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm, претражено 12. 05. 2014. године
11. Европска конвенција за заштиту људских права и основних слобода (Рим, 1950), („Службени лист СЦГ“ Међународни уговори бр.9/2003)
12. ENISA Position Paper No.1: Security Issues and Recommendations for Online Social Networks, 2007, http://www.enisa.europa.eu/publications/archive/

security-issues-and-recommendations-for-online-social-networks, претражено 19. 03. 2015. године

13. European Parliament resolution on harassment at the workplace (2001/2339(INI)), A5-0283/2001, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:077E:0138:0141:EN:PDF, претражено 03. 05. 2013. године
14. Закон о ауторским и сродним правима („Службени гласник РС“ бр. 104/2009, 99/2011 и 119/2012).
15. Закон о ауторском и сродном праву Републике Косово – Закон бр. 04-L-065 од 18. 11. 2011. године, доступно на http://www.kuvendikosoves.org/common/docs/ligjet/Zakon%20o%20autorskom%20i%20srodnom%20pravu.pdf
16. Закон о електронском документу („Службени гласник РС“ 51/2009)
17. Закон о електронским комуникацијама („Службени гласник РС” бр. 44/2010, 60/2013 – одлука УС и 62/2014)
18. Закон о електронској трговини (“Службени гласник РС“ 41/2009 и 95/2013)
19. Закон о електронском потпису („Службени гласник РС” бр.135/2004)
20. Закон о заштити интернет приватности деце Сједињених Америчких Држава - The Children's Online Privacy Protection Act (COPPA), http://www.coppa.org/coppa.htm, претражено 12. 08. 2013. године
21. Закон о злонамерним комуникацијама Велике Британије (The Malicious Communications Act), 1988. са изменама и допунама из 2003.године, http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf, претражено 14. 01. 2015. године
22. Закон о заштити података о личности („Службени гласник РС” бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012)
23. Закон о интернет компјутерској превари Сједињених Америчких Држава - 18 U.S. Code § 1030 - Computer Fraud and Abuse Act (CFAA), http://www.law.cornell.edu/uscode/text/18/1030, претражено 02. 11. 2014. године
24. Закон о јавном информисању и медијима („Службени гласник РС” бр. 83/14)

25. Закон о компјутерском криминалитету Алжира (Cybercrime Bill for Algeria), https://algerianreview.wordpress.com/2010/01/09/algeria-cybercrime-law/, претражено 20. 11. 2014. године
26. Закон о компјутерском криминалу Аустралије - Malicious Communications Act 1988,http://www.neiladdison.pwp.blueyonder.co.uk/law/malcomm.htm, претражено 02. 11. 2014. године
27. Закон о компјутерском криминалитету Боцване (Cybercrime Bill for Botswana) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus2012/presentations/Octopus_2012_Botswana.pdf, претражено 20. 11. 2014. године
28. Закон о компјутерском криминалу Велике Британије - Malicious Communications Act 1988, http://www.legislation.gov.uk/ukpga/1988/27/contents/enacted, претражено 02. 11. 2014. године
29. Закон о компјутерском криминалу Холандије - Computer Crime Act (Wet computercriminaliteit), http://www.ejcl.org/143/art143-10.pdf, претражено 02. 11. 2014. године
30. Закон о компјутерском криминалитету Уједињених Арапских Емирата (United Arabic Emirates federal cyber crimes law (Law No. 2 of 2006 Concerning Combating Information Technology Crimes)), 2006, http://www.lexology.com/library/detail.aspx?g=1d072cdf-3cd5-4ad9-8c54-28c045057d02, претражено 20. 11. 2014. године
31. Закон о компјутерском криминалитету Уганде (The Computer Misuse Bill), http://www.hingx.org/Share/Details/774, 2008 - ревидиран 2011, претражено 20. 11. 2014. године
32. Закон о министарствима Републике Србије („Службени гласник РС" бр. 44/2014, 14/2005 и 52/2015)
33. Закон о оптичким дисковима („Службени гласник РС" 52/2011)
34. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС" бр.61/2005 и 104/2009)
35. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима („Службени гласник РС" бр.32/2013)

36. Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине („Службени гласник РС” бр. 46/2006 и 104/2009 - др.закони)
37. Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система („Службени гласник РС”, бр. 19/2009)
38. Закон о потврђивању Европске конвенције о сузбијању тероризма (“Службени лист СРЈ – Међународни уговори“ бр. 10/2001)
39. Закон о потврђивању Конвенције Савета Европе о борби против трговине људима („Службени гласник РС”, бр. 19/2009)
40. Закон о потврђивању Конвенције о високотехнолошком криминалу („Службени гласник РС”, бр. 19/2009)
41. Закон о потврђивању Конвенције Уједињених нација против транснационалног организованог криминала и допунских протокола („Сл.гласник СРЈ – Међународни уговори“, бр. 6/2001)
42. Закон о потврђивању Конвенције о заштити деце од сексуалне експоатације и сексуалног злостављања („Службени гласник РС – Међународни уговори“ бр. 1/10)
43. Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података („Сл.лист СФРЈ – Међународни уговори“ бр. 1/92, „Сл.лист СЦГ-Међународни уговори, бр.11/2005-др.закон и „Сл. галсник РС – Међународни уговори“ бр. 98/2008-др. Закон и 12/2010)
44. Закон о потврђивању Конвенције Савета Европе о спречавању тероризма („Службени гласник Републике Србије – Међународни уговори бр. 19/2009)
45. Закон о потврђивању међународне конвенције о заштити извођача, произвођача фонограма и установа за радио-дифузију (“Сл. Лист СФРЈ – Међународни уговори”, бр. 13/2002)
46. Закон о потврђивању WIPO уговора о ауторском праву (“Сл. Лист СФРЈ – Међународни уговори”, бр. 13/2002)
47. Закон о приватности електронских комуникација Сједињених Америчких Држава - 18 U.S. Code § 2510-22 - Electronic Communications

Privacy Act of 1986 (ECPA), http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119, претражено 02. 11. 2014. године

48. Закон о ратификацији Бернске конвенције за заштиту књижевних и уметничких дела ("Сл.лист СФРЈ", бр. 14/75 и "Сл. Лист СФРЈ – Међународни уговори", бр. 4/86 - уредба)
49. Закон о ратификацији Конвенције Ун о правима детета ("Службени лист СФРЈ" – Међународни уговори бр. 15/90, „Службени лист СРЈ"- Међународни уговори бр. 4/96 и 2/97)
50. Закон о слободном приступу информацијама од јавног значаја („Службени гласник РС" бр. 120/2004, 54/2007, 104/2009 и 36/2010)
51. Закон о спречавању злостављања на раду ("Сл. гласник РС", бр. 36/2010)
52. Закон о тајности података ("Службени гласник РС" бр. 104/2009)
53. Закон о услугама информатичког друштва Републике Косово – Закон бр. 04-L-094 од 02. 04. 2012. године, доступно на http://www.kuvendikosoves.org/common/docs/ligjet/Zakon%20o%20uslugama%20informatickog%20drustva.pdf
54. Законик о кривичном поступку Републике Косово – Законик бр. 04/ L-123 од 13. 12. 2012. године, доступно на http://projuris.org/Zakoni_Kosova/Zakonik_o_krivicnom_postupku_2012.pdf, претражено 29. 07. 2015. године
55. Законик о кривичном поступку („Службени гласник РС" бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014)
56. Законот на кривичната постапка („Службен весник на Република Македонија" број 150/2010, 100/2012.)
57. Identity Theft Assumption and Deterrence Act - the Identity Theft Act; U.S. Public Law 105-318, https://www.ftc.gov/node/119459, претражено 12. 08. 2015. године
58. Казнени закон Републике Хрватске („Народне новине", бр. 125/11, 144/12 и 56/15,61/15), доступно на http://www.zakon.hr/z/98/Kazneni-zakon , претражено 23. 07. 2015. године
59. Казненски законик Републике Словеније („Уредни лист РС", шт. 50/2012), http://projuris.org/Zakoni_Slovenije/Krivicni_zakonik_Slovenije-precisceni_tekst_2012.pdf, претражено 21. 11. 2014. године

60. Конвенција Међународне организације рада (МОР) бр. 182 о најгорим облицима дечјег рада („Службени лист СФРЈ – Међународни уговори”, бр. 8/03)
61. Конвенција о правима детета („Службени лист СФРЈ – Међународни уговори”, бр. 15/90)
62. Конвенција Савета Европе о борби против трговине људима (Council of Europe Convention on Action against Trafficking in Human Beings – CETS No. 197.), http://conventions.coe.int/Treaty/EN/Treaties/Word/197.doc, претражено 17. 06. 2014. године
63. Конвенција Савета Европе о високотехнолошком криминалу бр. 185 (Convention on Cybercrime CETS No. 185), 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, и http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG претражено 07. 11. 2014. године
64. Конвенција Савета Европе о заштити појединаца од аутоматске обраде личних података ЦЕТС бр. 108 (Council of Europe Convention on Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108), http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, , претражено 09. 07. 2014. године
65. Кривични закон Босне и Херцеговине („Службени гласник Босне и Херцеговине“ бр. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07,8/10, 47/14, 22/15, 40/15)
66. Кривични закон Брчко Дистрикта Босне и Херцеговине (“Службени гласник БД БиХ бр. 10/03, 6/05, 21/10, 47/11, 52/11 и 9/13)
67. Кривични закон Краљевине Шпаније, 1995. са изменама и допунама из 2012. године, http://www.legislationline.org/download/action/download/id/5160/file/Spain_Criminal_Code_Codigo_Penal.pdf, претражено 18. 01. 2015. године
68. Кривични закон Републике Пољске (Kodeks karny), 1997 са изменама и допунама из 2011. године, http://www.legislationline.org/download/action/download/id/4286/file/POLAND_CC_am2012_%20PL.pdf претражено 16. 01. 2015. године

69. Кривични законик Републике Косово – Закон бр. 04/L-129 од 19. октобра 2012. године, доступно на http://projuris.org/Zakoni_Kosova/Krivicni_zakonik_2012.pdf , претражено 29. 07. 2015. године
70. Кривични закон Републике Српске (“Службени гласник РС бр. 49/03, 108/04, 37/06, 70/06, 73/10, 01/12 и 67/13)
71. Кривични закон Федерације Босне и Херцеговине (“Службене новине Ф БиХ бр. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14)
72. Кривични законик Републике Србије („Службени гласник РС” бр.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 и 104/2013)
73. Кривични законик Црне Горе („Службени лист РЦГ“, бр. 70/2003, 13/2004, 47/2006 и „Службени лист ЦГ“ бр. 40/2008, 25/2010, 32/2011, 40/2013 и 56/2013.)
74. Кривичниот законик на Република Македонија („Службен весник на Република Македонија“ број 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08 , 139/08 , 114/09, 51/11, 135/11, 185/2011, 142/2012, 166/2012, 55/2013)
75. Закон о злонамерним комуникацијама Велике Британије - Malicious Communications Act 1988, http://www.legislation.gov.uk/ukpga/1988/27/contents/enacted, претражено 02. 11. 2014. године
76. Закон о злонамерним комуникацијама Велике Британије (The Malicious Communications Act), 1988. са изменама и допунама из 2003.године, http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf, претражено 14. 01. 2015. године
77. Међународна конвенција за превенцију свих облика расне дискриминације („Службени лист СФРЈ“ бр. 6/1967)
78. Међународни пакт о грађанским и политичким правима (1966.) (“Службени лист СФРЈ“ бр. 7 од 04. 02. 1971. године)
79. Начела Г-8 поводом заједничке борбе против међународног организованог криминала која се односе на међународни приступ сачуваним компјутерским подацима, http://www.g8.utoronto.ca/adhoc/crime99.htm, Анекс 1 (Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow October 19-20, 1999, Annex 1.), http://www.g8.utoronto.ca/adhoc/crime99.htm, претражено 07. 11. 2014. године

80. Оквирна одлука о нападима на информационе системе Комисије европских заједница (Framework Decision on attacks against information systems of the Commission of the European Communities), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222 &from=EN, претражено 12. 11. 2014. године
81. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2002., United Nations Secretariat - Office of the United Nations High Commissioner for Human Rights, http://www.ohchr.org/english/law/crc-sale.htm, претражено 15. 11. 2014. године
82. Повеља Европске Уније о основним правима (енгл. Charter of fundamental rights of the European Union), http://www.europarl.europa.eu/charter/ pdf/text_en.pdf, претражено 15. 05. 2015. године
83. Правилник о правилима понашања послодаваца и запослених у вези са превенцијом и заштитом од злостављања на раду ("Сл. гласник РС", бр. 62/2010)
84. Препорука Међународне организације рада (МОР) бр. 190 о забрани и хитној акцији за укидање најгорих облика дечјег рада („Службени лист СФРЈ – Међународни уговори", бр. 8/03)
85. Препорука Савета Европе о криминалитету везаном за рачунаре бр. 9 (Council of Europe Computer-related crime Recommendation No. R (89) 9), 1989., http://www.oas.org/juridico/english/89-9&final%20Report.pdf, претражено 07. 11. 2014. године и 29. 11. 2014. године
86. Препорука Савета Европе бр. 95 о заштити појединаца у поступку обраде личних података и њиховог слободног преношења - Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, усвојена 11. 09. 1995. године, http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp , претражено 07. 11. 2014. и 29. 11. 2014. године
87. Препорука Савета Министара Савета Европе CM/Rec(2012)4 државама чланицама која се односи на заштиту људских права на друштвеним мрежама (Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social

networking services), 2012, https://wcd.coe.int/ViewDoc.jsp?id=1929453, претражено 09. 07. 2014. године

88. Препорука бр. P(97)20 Комитета министара државама чланицама (30. 09. 1997.), www.coe.int/t/dghl/standardsetting/media/doc/translations/serbian/Rec (1997)o2o&ExpMem_sb.pdf , претражено 02. 12. 2012. године
89. Препорука Организације држава Америке (Organization of American States (OAS)), 2002., http://www.oas.org/juridico/english/cyber.htm, претражено 12. 11. 2014. године
90. Препорука Савета Европе о трговини људским органима у Европи бр.1611 из 2003. године, (Council of Europe Recommendation 1611 – Trafficking in organs in Europe), http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta03/EREC1611.htm, претражено 17. 06. 2014. године
91. Приручник УН о спречавању и контроли компјутерског криминала (United Nations Manual on the Prevention and Control of Computer-related Crime), 1994, http://www.uncjin.org/Documents/EighthCongress.html, претражено 11. 11. 2014. године
92. Протокол за превенцију, сузбијање и кажњавање трговине људима посебно женама и децом који допуњује Конвенцију против организованог међународног криминала („Сл.гласник СРЈ – Међународни уговори“, бр. 6/2001)
93. Резолуција Европског Савета бр. 2002/C43/02 о заједничком приступу и посебним акцијама у домену мрежне и информатичнке безбедности – European Council Resolution on a common approach and specific actions in the area of network and information security (2002/C43/02), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022&from=EN, претражено 21. 11. 2014. године
94. Резолуција Европског Савета бр. 2007/C 68/ –European Council Resolution 2007/C 68/01, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007G0324(01)&from=EN, претражено 21.11.2014.године
95. Резолуција Савета Европе 2007/C 68/01 - Стратегија сигурног информационог друштва Европе (Council Resolution 2007/C 68/01 - Strategy for a Secure Information Society in Europe – “Dialogue, partnership,

and empowerment"), 2007, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007G0324%2801%29, претражено 09. 07. 2014. године

96. Резолуција Уједињених Нација 65/230 (UN General Assembly resolution 65/230), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement, 2010., претражено 12. 11. 2014. године
97. Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационе технологија (UN resolution A/res/55/63 on combating the criminal misuse of information technologies), 2000., http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, претражено 11. 11. 2014. године
98. Резолуција Уједињених Нација A/res/56/121 о борби против злоупотребе информационих технологија (UN resolution A/res/56/121 on combating the criminal misuse of information technologies), 2002., http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, претражено 20. 08. 2015. године
99. Резолуција 2007/20 од 26.7.2007.године, www.un.org/.../ecosoc/.../2007 /Resolution%2020, претражено 25. 04. 2015. године
100. Ревидирана Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационе технологија (UN resolution A/res/55/63 on combating the criminal misuse of information technologies), 2001., http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf, претражено 11. 11. 2014. године
101. Резолуција Уједињених Нација о законодавству у области компјутерског криминалитета (UN resolution on computer crime legislation), http://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf, претражено дана 11. 11. 2014. године
102. Резолуција Уједињених Нација (тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације (UN Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation),

http://www.uri.edu/artsci/wms/hughes/ppr.htm, претражено 05. 03. 2015. године

103. Стратегија за безбедно информационо друштво у Европи – Strategy for a Secure Information Society in Europe "Dialogue, partnership, and empowerment", http://ec.europa.eu/information_society/doc/com2006251.pdf, претражено 21. 11. 2014. године
104. Стратегија развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС" бр. 51/2010)
105. The UK Fraud Act 2006, http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf, претражено 12. 08. 2015. године
106. Туниска агенда бр.WSIS-05/TUNIS/DOC/6(Rev. 1) за информатичко друштво (Tunis agenda но. WSIS-05/TUNIS/DOC/6(Rev. 1) for the information society), 2005, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, претражено 12. 11. 2014. године
107. Устав Републике Србије ("Службени гласник РС" бр. 98/2006)
108. Факултативни протокол уз Конвенцију о правима детета о продаји деце, дечјој проституцији и дечјој порнографији („Службени лист СРЈ – Међународни уговори", бр. 22/02)
109. Comprehensive Study on Cybercrime – Draft, United Nations office on drugs and crime, Vienna, February 2013, United Nations, New York 2013, str. Ix, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, претражено 12. 10. 2014. године
110. CRIMINAL CODE (STALKING) AMENDMENT ACT 1999 - Act No. 18 of 1999, https://www.legislation.qld.gov.au/LEGISLTN/ACTS/1999/99AC018.pdf, претражено 16. 01. 2015. године
111. Шангајска Конвенција о борби против тероризма, сепаратизма и екстремизма (The Shanghai Convention on combating terrorism, separatism and extremism), 2001, http://eurasiangroup.org/files/documents/conventions_eng/The_20Shanghai_20Convention.pdf, претражено 20. 11. 2014. године

Интернет извори

Домаћи интернет извори

1. 24 сата, http://www.24sata.rs/specijal/it/vest/veca-privatnost-profile-novih-korisnika-i-cover-slike-videce-samo-prijatelji/137514.phtml, претражено 26. 05. 2014. године
2. 55% домаћинстава у Србији поседује рачунар, 47,5 одсто интернет, http://teslio.com/blog/post/tbloger/3865, претражено 27. 09. 2012. године
3. APIS Security consalting, Компјутерски криминалитет, http://www.apisgroup.org/sec.html?ид=29, претражено 20. 11. 2013. године
4. „Afera pištolj" i govor mržnje na internetu ("Affair gun" and hate speech on Twitter), Novi media centar „Liber", www.blogopen.rs/afera-pistolj-i-govor-mržwe-na-tviteru-prema-kihot_ex_of_djvucicevic-istrazivanje, претражено 05. 12. 2015. године
5. Балканист, http://balkanist.net/bcs/siepa-leaks/ , претражено 19. 12. 2013. године
6. Блам тужилаштва за сајбер криминал, http://www.samo-opusteno.info /forum/tehnologija/blam-tuzilastva-za-sajber-kriminal/, претражено 06. 08. 2012. године
7. Блиц – дневна новина од 06. 08. 2012. године, http://www.blic.rs/Vesti/Svet/269975/Predao-se-kralj-spamova-na-Fejsbuku, претражено 06. 08. 2012. године
8. Блиц – дневна новина од 23. 08. 2012. године, http://www.blic.rs/Vesti/Hronika/338974/Ubica-iz-Nisa-spremao-i-trece-vencanje, претражено 23. 08. 2012. године
9. Блиц – дневна новина од 13. 10. 2012. године,www.blic.rs, дневна новина „Блиц" од 13. 10. 2012. , претражено 13. 10. 2012. године
10. Блиц – дневна новина од 25. 12. 2012. године, www.blic.rs, дневна новина „Блиц" од 25. 12. 2012. , претражено 25. 12. 2012. године
11. Блиц – дневна новина од 10. 12. 2013. године,www.blic.rs, дневна новина „Блиц" од 10. 12. 2013. , претражено 10. 12. 2013. године
12. Блиц – дневна новина од 11. 02. 2014. године, www.blic.rs, дневна новина „Блиц" од 11. 02. 2014. , претражено 11. 02. 2014. године

13. Блиц – дневна новина од 23. 04. 2014. године, www.blic.rs, дневна новина „Блиц” од 23. 04. 2014. , претражено 23. 04. 2014. године
14. Блиц – дневна новина од 11. 12. 2014. године, http://www.blic.rs/Vesti/Drustvo/518514/DRZIMO-SRBIJU-U-SACI-Hakeri-tvrde-da-su-ukrali-JMBG-gotovo-svih-gradjana, претражено 11. 12. 2014. године
15. Блиц – дневна новина од 12. 12. 2014. године, http://www.blic.rs/Vesti/Drustvo/518714/KAKO-SU-HAKERI-DOSLI-DO-NASIH-PODATAKA-Upali-u-spiskove-partija, претражено 12. 12. 2014. године
16. Блиц – дневна новина од 14. 01. 2015. године, http://www.blic.rs/Vesti/Hronika/526500/SAZNAJEMO-Uhapseni-tinejdzeri-koji-su-objavljivali-zasticene-podatke, претражено 14. 01. 2015. године
17. Блиц – дневна новина од 01. 02. 2015. године, www.blic.rs, претражено 01. 02. 2015. године
18. Број Twitter корисника у Србији , http://zsteva.info/blog/2009/01/29/broj-twitter-korisnika-u-srbiji/, претражено 10. 08. 2012. године
19. Вечерње новости – дневна новина од 11. 04. 2012. године, http://www.novosti.rs/vesti/naslovna/aktuelno.291.html:375140-Tuzilastvo-Haker-primao-novac-za-obaranje-sajtova, претражено 06. 08. 2012. године
20. Годишњи извештај о раду Центра за безбедни интернет – Србија у 2013. години, http://kliknibezbedno.rs/files/materijali/Klikni%20bezbedno%20publikacija.pdf, претражено 01. 10. 2015. године
21. Годишњи извештај о раду Центра за безбедни интернет – Србија у 2014.-2015. години, http://kliknibezbedno.rs/files/materijali/Klikni-bezbedno-publikacija-2015_1440332559.pdf, претражено 01. 10. 2015. године
22. Друштвене мреже: Cyber криминал лани порастао за 90 посто, http://www.24sata.info/tehnologija/internet/53981-Drustvene-mreze-Cyber-kriminal-lani-porastao-posto.html, претражено 06. 08. 2013. године
23. Економски портал, http://www.ekonomskiportal.com/instagram-najbrze-rastuca-drustvena-mreza/, претражено 12. 07. 2014. године
24. Жене за живот без насиља: приручник за волонтерке СОС телефона”, Београд: Буфала Бил, 2.издање, 1999.
25. Заштита информационих система, www.fms-tivat me/PREDAVANJA 3 god/ZIS8.pdf, претражено 25. 08. 2015. године

26. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Podignuta-optuznica-protiv-kralja-spama-zbog-fisinga-i-spama-na-Facebook-u.html, претражено 06. 08. 2012. године
27. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Novinar-portparol-Anonimusa-osudjen-na-pet-godina-zatvora.html, претражено 26. 01. 2015. године
28. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Hapsenja-u-zemljama-EU-zbog-koriscenja-trojanaca-za-daljinski-pristup.html, претражено 26. 01. 2015. године
29. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Najveca-policijska-akcija-protiv-kriminala-na-mracnom-internetu-ugaseno-410-sajtova-17-osoba-uhapseno.html, претражено 26. 01. 2015. године
30. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Zbog-hakovanja-suosnivac-Pirate-Bay-osudjen-na-3-5-godine-zatvora.html, претражено 26. 01. 2015. године
31. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Vodja-grupe-koja-je-za-12-sati-ukrala-9-miliona-dolara-sa-bankomata-osudjen-na-11-godina-zatvora.html, претражено 26. 01. 2015. године
32. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Autor-ozloglasenog-hakerskog-alata-Blackshades-izjasnio-se-nevinim-pred-sudom.html , претражено 26. 01. 2015. године
33. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Zbog-malvera-Blackshades-uhapseno-100-ljudi-u-16-zemalja.html, претражено 26. 01. 2015. године
34. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Prvo-hapsenje-zbog-Heartbleed-baga.html , претражено 26. 01. 2015. године
35. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Covek-izvrsio-samoubistvo-zbog-pretnje-policijskog-malvera.html, претражено 26. 01. 2015. године

36. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Poverovao-policijskom-virusu-i-sam-se-predao-policiji-zbog-decije-pornografije.html, претражено 26. 01. 2015. године
37. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Kako-je-FBI-uz-pomoc-fisinga-i-malvera-identifikovao-osumnjicenog-za-pretnje-bombaskim-napadima.html, претражено 26. 01. 2015. године
38. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Pet-godina-zatvora-zbog-fising-prevara.html, претражено 26. 01. 2015. године
39. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/38-godina-zatvora-zbog-kradje-identiteta.html, претражено 26. 01. 2015. године
40. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Haker-koji-je-ucenjivao-americku-Miss-Teen-i-druge-zene-osudjen-na-18-meseci-zatvora.html, претражено 26. 01. 2015. године
41. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Haker-na-Facebook-u-objavio-ukradene-seksualno-eksplicitne-fotografije.html, претражено дана 26. 01. 2015. године
42. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Optuznica-za-upad-u-Gmail-nalog-supruge-krivicno-delo-ili-privatna-stvar.html, претражено 26. 01. 2015. године
43. Информација – сазнајте више о компјутерској безбедности, http://www.informacija.rs/Sajber-hronika/Clan-foruma-Carder-su-osudjen-na-20-godina-zatvora.html , претражено 26. 01. 2015. године
44. Интернет магазин „Ваш психолог“, www.vaspsiholog.com/tag/histionski - poremećaj licnosti/, претражено 19. 12. 2015. године
45. Кликни безбедно, http:/kliknibezbedno.rs/sr/centar-za-bezbedni-internet.1.51.html, претражено 02.02.2016. године
46. Кликни безбедно, http://kliknibezbedno.rs/sr/gruming.1.137.html, претражено 15. 07. 2015. године

47. Кликни безбедно, http://kliknibezbedno.rs/sr/ pornografija-iz-osvete.1.118 .html , претражено 15. 07. 2015. године
48. Компутерски криминал/ИПФ-радна база, http://promocije.net/proba/ krivicno-pravo/materijalno-krivicno-pravo/kompjuterski-kriminal/, претражено 19.02.2016. године
49. Курир- дневна новина од 30. 09. 2011. године : „Ексклузивно: Србин који је разбио Фејсбук“, http://www.kurir.rs/ekskluzivno-srbin-koji-je-razbio-fejsbuk-clanak-113719, претражено 14. 08. 2012. године
50. Misija OEBS-a u Srbiji, www.osce.org/sr/serbia, претражено 15. 08. 2015. године
51. Недељне информативне новине НИН – „Ловци на тајне поруке терористе“, бр. 3387 од 26. 11. 2015. године, стр. 19-21, http://www. nin.co.rs
52. Независно удружење новинара Србије, www.nuns.rs/info/news/9672/ PRVA-PRESUDA-ZA-MOBING.html, претражено 05. 05. 2013. године
53. Нишке вести, http://www.niskevesti.info/hronika/vesti/krvni-delikti/578-preko-qfejsbukaq-do-velike-tragedije , претражено дана 16. 08. 2012. године
54. Нови магазин од 21.04.2015.године, http://www.novimagazin.rs/vesti/nvo-proganjanje-treba-da-bude-krivicno-delo, претражено 22. 10. 2015. године
55. Новости магазин, www.novosti.rs/.../aktuelno291.html., претражено 01. 12. 2015. године
56. Повереник - www.poverenik.rs. Pravni okvir. Međunarodni dokumenti, претражено 12. 10. 2015. године
57. Пословни портал Economy, http://www.economy.rs/ , претражено 27. 09. 2012. године
58. Прва пресуда за мобинг: професор злостављао асистента, http://www.vesti-online.com/Vesti/Hronika/279839/Prva-presuda-za-mobing-Profesor-zlostavljao-asistenta, претражено 05. 05. 2013. године
59. Приручник за заштиту деце и младих од сајбер насиља и примену у редовном наставном програму основних и средњих школа - “Tagged”, Инцест траума центар Београд, 2013, http://kliknibezbedno.rs/files/ materijali/ITC%20-%20Tagged%20Manual%202013.pdf, претражено 01. 10. 2015. године

60. Регулаторна агенција за електронске комуникације и поштанске услуге, www.ratel.rs, претражено 25. 08. 2015. године
61. Регулаторно тело за електронске медије, http://www.rra.org.rs/cirilica, претражено 25. 08. 2015. године
62. Реконструкција – Женски фонд, http://www.rwfund.org/kriticne-teme/izvori-epistemologije-kriticki-zivot/edvard-snouden/, претражено 08. 04. 2015. године
63. Републички завод за статистику Републике Србије, http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2, претражено 09. 02. 2015. године
64. Сајбер криминал у порасту, http://www.novimagazin.rs/vesti/sajber-kriminal-u-porastu/ , претражено 10. 02. 2014. године
65. Say Serbia, http://sayserbia.com/ , претражено 07. 06. 2014. године
66. Say Serbia, http://sayserbia.com/forum/categories/foreigner-reviews/listForCategory, претражено 07. 06. 2014. године
67. Say Serbia, http://sayserbia.com/forum/categories/foreigner-reviews/listForCategory, претражено 07. 06. 2014. године
68. Say Serbia, http://sayserbia.com/main/authorization/privacyPolicy, претражено 07. 06. 2014. године
69. Say Serbia, http://sayserbia.com/main/authorization/termsOfService, претражено 07. 06. 2014. године
70. SAY SERBIA: Ovo je srpska verzija Fejsbuka, http://www.telegraf.rs/hi-tech/internet/894983-srbija-dobija-svoj-fejsbuk-koji-se-zove-say-serbia, претражено 07. 06. 2014. године
71. Србија данас Магазин, www.srbijadanas.com/clanak/akcija-argmagedon-uhapseni-osumnjiceni-za-distribuciju-dečije-pornografije-12-05-2015, www.novosti.rs/.../aktuelno291.html., претражено 01. 12. 2015. године
72. Srbija dobila „svoj Facebook“ – Say Serbia, http://www.b92.net/tehnopolis/vesti.php?yyyy=2013&mm=12&nav_id=786328, претражено 07. 06. 2014. године
73. Све више зависника од друштвених мрежа, Интернет магазин Мондо од 29. 01. 2012. године, http://www.mondo.rs/s232269/Magazin/Sve_vise_zavisnika_od_drustvenih_mreza.html, претражено 12. 05. 2013. године

74. Удружење “Стоп мобинг” - Ко су мобери, , www.mobing.rs, претражено 07. 05. 2013. године
75. Удружење “Стоп мобинг”, http://www.mobing.rs/news.php, претражено 20. 04. 2013. године и 03. 05. 2013. године
76. Удружење “Стоп мобинг”, http://mobing.rs/articles.php?article_id=6, претражено 03. 05. 2013. године
77. Удружење “Стоп мобинг”, http://www.mobing.rs/articles.php?article_id=17, претражено 03. 03. 2015. године
78. ФБ чува обрисане фотографије, http://www.b92.net/tehnopolis/vesti.php?nav_id=465257&fs=1, претражено 07. 08. 2012. године
79. Фејсбук - Политика о коришћењу података: Информације добијене од корисника, Registration information, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године
80. Фејсбук - Политика о коришћењу података:Информације добијене од корисника, Information that is always publicly available, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године
81. Фејсбук - Политика о коришћењу података: Информације добијене од корисника, How we use the information we recieve, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године
82. Фејсбук - Политика о коришћењу података:Информације добијене од корисника, Deleting and deacrivating your account, http://www.facebook.com/about/privacy/your-info#inforeceived, претражено 04. 08. 2012. године
83. Фејсбук Србија, http://www.fejsbuksrbija.com/, претражено 15. 02. 2015. године
84. Фејсбук Србија, http://www.fejsbuksrbija.com/facebook-kompanija-trazi-promenu-adrese-sajta-facebooksrbija-com/informacije/1785.html, претражено 15. 02. 2015. године
85. Фејсбук Србија, http://www.fejsbuksrbija.com/neces-me-vise-tagovati/uputstva/1975.html, претражено 15. 02. 2015. године
86. Фејсбук Србија, http://www.fejsbuksrbija.com/jos-jednom-podesite-svoje-sigurnosne-podatke/uputstva/1491.html, претражено 15. 02. 2015. године

87. Фејсбук Србија, http://www.fejsbuksrbija.com/brisanje-facebook-naloga/uputstva/1412.html, претражено 15. 02. 2015. године
88. Фејсбук Србија, http://www.fejsbuksrbija.com/facebook-lazni-profil-prijava/uputstva/1336.html, претражено 15. 02. 2015. године
89. Фејсбук Србија, http://www.fejsbuksrbija.com/kako-nam-kradu-lozinke/uputstva/850.html, претражено 15. 02. 2015. године
90. Фејсбук Србија, http://social-networking-websites-review.toptenreviews.com /google--review.html, претражено 11. 07. 2014. године

Страни интернет извори

1. News – "Sacked for Calling Job Boring on Facebook", 2009. http://news.sky.com/skynews/Home/UK-News/Facebook-Sacking-Kimberley-Swann-From-Clacton-Essex-Sacked-For-Calling-Job-Boring/Article/200902415230508Sky, претражено дана 29. 04. 2013. године
2. 12. конгрес УН у вези с превенцијом криминала и кривичног правосуђа (12th UN Congress on Crime Prevention and Criminal Justice), 12–19. 4. 2010, стр.6, https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf, претражено 12. 08. 2015. године
3. 30 Things You Absolutely Need To Know About Instagram, http://www.searchenginejournal.com/30-things-absolutely-need-know-instagram/85991/, претражено 12. 07. 2014. године
4. 6 Things Everyone Should Know About Instagram, http://thesocialu101.com/6-things-everyone-should-know-about-instagram/, претражено 12. 07. 2014. године
5. About Spokeo, http://www.spokeo.com/blog/about, претражено 12. 08. 2012. године
6. ACTA: Updated Analysis of the Final Version, https://www.laquadrature.net/en/acta-updated-analysis-of-the-final-version, претражено 22. 08. 2015. године
7. Africa Union www.africa-union.org, претражено 12. 11. 2014. године и http://www.au.int/, претражено 23. 07. 2015. године

8. All About Phishing, http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp, претражено 07. 09. 2012. године
9. Arab League Online, www.arableagueonline.org, претражено 20. 11. 2014. године
10. Asia's Child Sex Victims Ignored, BBC, 2000, http://news.bbc.co.uk/1/hi/world/asia-pacific/926853.stm, претражено 07. 09. 2014. године
11. Asian Pacific Economic Cooperation (APEC), www.apecsec.org, претражено 12. 11. 2014. године
12. Association of Southeast Asian Nations (ASEAN), www.aseansec.org, претражено 12. 11. 2014. године
13. Bebo, http://www.bebo.com/faq, претражено 06. 06. 2014. године
14. Bebo, http://social-networking-websites-review.toptenreviews.com/bebo-review.html, претражено 06. 06. 2014. године
15. Beyond Facebook: 74 Popular Social Networks Worldwide, http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide, претражено 12. 11. 2014. године
16. Bio., http://www.biography.com/people/edward-snowden-21262897, претражено 03. 03. 2015. године
17. Brazilian Prosecutors Seek to Sue Google, MSNBC, 2006, http://msnbc.msn.com/id/14622759/, претражено 12. 09. 2014. године
18. British Crime Survey, 2003, http://www.usak.org.tr/istanbul/files/bcs25.pdf, претражено 04. 11. 2012. године.
19. Canadian Department of Justice, http://canada.justice.gc.ca/en/news/nr/2007/doc_32178.html, претражено 15. 08. 2015. године
20. Canadian Internet Policy and Public Interest Clinic – CIPPIC, https://cippic.ca/, претражено 14. 06. 2015. године
21. China's Facebook Status: Blocked, ABC News – вест од 08. 07. 2009. године, http://abcnews.go.com/blogs/headlines/2009/07/chinas-facebook-status-blocked/, претражено 10. 08. 2012. године
22. Computer Crime Research Center: Fraud in the Internet, http://www.crime-research.org/articles/Internet_fraud_0405/, претражено 02. 11. 2013. године
23. ComScore, http://www.comscore.com/ , претражено 12. 06. 2014. године и 05. 08. 2012. године

24. Government Requests For Twitter Users' Personal Information Raise Serious Constitutional Concerns, Says ACLU, ACLU – American Civil Liberty Union, 2011, http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu, претражено 12. 08. 2012. године
25. Corporate Alliance to End Partner Violence - Stalking, http://www.caepv.org/getinfo/facts_stats.php?factsec=9, претражено 06. 03. 2012. године
26. Council of Europe – Action against Terrorism, http://www.coe.int/t/dlapil/codexter/default_EN.asp, претражено 12. 12. 2015. године
27. Council of Europe, Cons.Ass; Twenty-First Ordinary session (Third Part), Text adopted (1970); Council of Europe, Collected Texts, Strasbourg, 1979; https://books.google.rs/books?isbn=9041102663, претражено 02. 11. 2015. године
28. Council Of Europe - Opinion Of The Committee Of Experts On Terrorism (Codexter) For The Attention Of The Committee Of Ministers On Cyber terrorism And Use Of Internet For Terrorist Пurposes, http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/4_theme_files/Cyberterrorism.asp#TopOfPage, претражено 07. 10. 2013. године
29. Council of Europe – Treaty Office, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, претражено 09. 11. 2014. године, 31. 07. 2015. године и 16. 08. 2015. године
30. CSE tracks millions of downloads daily: Snowden documents, http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120, претражено 08. 04. 2015. године
31. Cyber-extortion results in prison sentence - Net4TV Voice News Staff, http://www.reformation.com/CSA/RobertHarveyAlexander2.htm, претражено 24. 03. 2015. године
32. Cyber Angels, http://www.cyberangels.org/, претражено 01. 11. 2012. године и 01. 03. 2013. године
33. Cyberbullying Research Center, http://cyberbullying.us/cyberbullying_glossary.pdf, претражено 11. 03. 2014. године
34. Cybercrime on social networks continues to climb, http://www.net-security.org/secworld.php?id=11464, претражено 04. 10. 2013. године

35. Cyberbullying and Harrasment, http://www.netce.com/coursecontent.php?courseid=1127, претражено 20. 09. 2013. године
36. Cybercrime Convention Comitee – T-CY Guidance Note #4, Identity theft and phishing in relation to fraud, Council of Europe, 2013, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7096, претражено 20. 09. 2015. године
37. Cyber Crime Law, http://www.cybercrimelaw.net/AU.html, претражено 20. 11. 2014. године
38. DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, 2005, http://www.globalsecurity.org/military/library/policy/army/other/tradoc-dcsint-hbk_1-02-2005.pdf , претражено 24. 10. 2015. године
39. Decision of Defendant's F.R.CRIM. 29(c) Motion, Case UNITED STATES of America, Plaintiff, v. Lori DREW, Defendant. No. CR 08–0582–GW. | Aug. 28, 2009, http://stanford.edu/~jmayer/law696/week1/United%20States%20v.%20Drew.pdf, претражено 03. 01. 2015. године
40. Друштвена мрежа која спаја Србе и пријатеље Србије: Наши сусједи добили свој Facebook, http://www.index.hr/black/clanak/quotdrustvena-mreza-koja-spaja-srbe-i-prijatelje-srbijequot-nasi-susjedi-dobili-svoj-quotfacebookquot/715359.aspx, претражено 07. 06. 2014. године
41. Electronic Frontier Foundation, The Anti-Counterfeiting Trade Agreement – ACTA, https://www.eff.org/issues/acta, претражено 20. 08. 2015. године
42. Electronic Privacy Information Center: "The Amy Boyer case", 2006, Electronic Privacy Information Center Web site http://www.epic.org/privacy/boyer/ , претражено 06. 03. 2015. године
43. EDRi: Protecting digital freedom, https://edri.org/ACTAfactsheet/, претражено 22. 08. 2015. године
44. European Commision – Digital Agenda for Europe, http://ec.europa.eu/digital-agenda/, претражено 15. 11. 2012. године
45. European Commission - Special Eurobarometer 404: CYBER SECURITY REPORT, 2013., http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf, претражено 15. 07. 2015. године

46. European Union Agency for Network and Information Security, http://www.enisa.europa.eu/
47. European Union Law – Data Retention Directive, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, претражено 09. 04. 2015. године
48. Everything you need to know about PRISM, http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet, претражено 08. 04. 2015. године
49. Facebook '09 revenue neared $800 mn: Sources - The Economic Times, http://economictimes.indiatimes.com/topic/infotech-internet-Facebook-09-revenue-neared-800-mn-Sources-articleshow-6063819, претражено 10. 09. 2012. године
50. Facebook – newsroom, http://newsroom.fb.com/, претражено 10. 09. 2012. године
51. Facebook: A new battleground for cyber-crime, http://www.euractiv.com/infosociety/facebook-new-battleground-cyber-news-222406, претражено 29. 04. 2013. године
52. Facebook, https://www.facebook.com/about/basics, претражено 29. 11. 2014. године
53. Facebook, https://www.facebook.com/about/basics/how-others-interact-with-you/, претражено 29. 11. 2014. године
54. Facebook, Twitter users vulnerable to cyber crimes, http://www.thehindu.com/sci-tech/internet/article99159.ece, претражено 29. 04. 2013. године
55. Financial times, http://lexicon.ft.com/Term?term=social-network , претражено 07. 06. 2014. године
56. Find Law UK, http://blogs.findlaw.co.uk/solicitor/2011/08/computer-crime-hacker-uses-facebook-to-steal-35k-from-neighbours.html, претражено 26. 01. 2015. године
57. First ASEAN Plus Three Ministerial Meeting on Transnational Crime (AMMTC+3), http://www.asean.org/communities/asean-political-security-community/item/joint-communique-of-the-first-asean-plus-three-ministerial-meeting-on-transnational-crime-ammtc3-bangkok-10-january-2004, претражено 12. 11. 2014. године

58. Government Requests For Twitter Users' Personal Information Raise Serious Constitutional Concerns, Says ACLU, ACLU – American Civil Liberty Union, 2011, http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu, претражено 12. 08. 2012. године
59. How to Defend Yourself Against Identity Theft, http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp, претражено 17. 09. 2012. године
60. Инстаграм, http://instagram.com/about/faq/, претражено 12. 07. 2014. године
61. 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, претражено 12. 08. 2012. године
62. Internet Governance Forum, http://www.intgovforum.org/cms, претражено 28. 08. 2015. године.
63. Internet Identity Theft, http://articles.winferno.com/computer-fraud/internet-identity-theft, претражено 17. 09. 2012. године
64. Internet Rights and Principles Dynamic Coalition (IRP): Internet rights & Principles Charter - Internet rights & Principes, http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet-English_4thedition.pdf, претражено 06. 08. 2015. године
65. International Working Group on Data Protection in Telecommunications, http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt, претражено 12. 09. 2015. године
66. Интерпол, http://www.interpol.int/Crime-areas/Terrorism/Counter-Terrorism-Fusion-Centre, приступ 12. 12. 2015. године
67. ITU releases 2014 ICT figures: Mobile-broadband penetration approaching 32 per cent, Three billion Internet users by end of this year – подаци Специјализоване Агенције Уједињених Нација (ITU), http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.VTy_iiGqqkr , претражено 24. 04. 2015.године
68. Јутарњи лист, www.jutarnji.hr, претражено 22. 09. 2015. године.

69. Kids Health, http://kidshealth.org/parent/positive/talk/cyberbullying.html, претражено 10. 09. 2012. године
70. LinkedIn, https://www.linkedin.com/job/, претражено 10. 07. 2014. године
71. LinkedIn - Политика приватности, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, претражено 04. 08. 2012. године
72. Megan Meier Case, http://stanford.edu/~jmayer/law696/week1/United%20States%20v.%20Drew.pdf, претражено 03. 01. 2015. године
73. Megan Meier Foundation, http://www.meganmeierfoundation.org/megans-story.html, претражено 03. 01. 2015. године
74. Microsoft Safety & Security Center, http://www.microsoft.com/security/online-privacy/social-networking.aspx, претражено 17. 08. 2013. године
75. Министарство унутрашњих послова Републике Хрватске, http://www.mup.hr/UserDocsImages/topvijesti/2012/lipanj/Zastitimo%20djecu%20na%20internetu.pdf, претражено 28. 09. 2015. године
76. My Space, http://www.myspace.com/johnhollywoodpierce/blog/546361330, претражено 16. 01. 2015. године
77. Myra Hamilton: Objavljivanje detalja iz života deteta predstavlja pitanje privatnosti, извор: TheConversation.com - 25. 12. 2013. , http://partners-serbia.org/privatnost/aktuelno/myra-hamilton-objavljivanje-detalja-iz-zivota-deteta-predstavlja-pitanje-privatnosti/, претражено 06. 03. 2014. године
78. Национални центар за несталу и злостављану децу (National Center for Missing and Exploited Children), http://www.missingkids.com/home, претражено 10. 05. 2014. године
79. National Infrastructure Protection Plan, http://www.dhs.gov/national-infrastructure-protection-plan, претражено 24. 10. 2015. године
80. Net Crimes, http://www.netcrimes.net/Amy%20Lynn%20Boyer_files/liamsite.htm, претражено 27. 11. 2014. године
81. Out-Law news: „Phishing kits banned by new Fraud Act“, http://www.out-law.com/page-7469, претражено 12. 08. 2015. године
82. Одбор за праћење приватности и грађанских слобода (The Privacy and Civil Liberties Oversight Board - PCLOB), https://www.pclob.gov/, претражено 09. 04. 2015. године

83. OECD Guidelines for the Security of Information Systems and Networks: towards a culture of security, http://www.oecd.org/sti/ieconomy/15582260.pdf, претражено 12. 12. 2015. године
84. OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, Ministerial background report: DSTI/CP (2007)3/FINAL, http://www.oecd.org/sti/40644196.pdf, претражено 10. 11. 2015. године
85. Office of the Privacy Commissioner – OPC, https://www.priv.gc.ca/index_e.ASP, претражено 14. 06. 2015. године
86. Online photos can reveal our private data say experts, BBC News, 2011, http://www.bbc.co.uk/news/technology-14386514, претражено 12. 08. 2012. године
87. Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo, претражено 08. 04. 2015. године
88. Orkut, https://support.google.com/orkut, претражено 11. 07. 2014. године
89. Oxford dictionaries, http://www.oxforddictionaries.com/definition/english/social-network , претражено 07. 06. 2014. године
90. Patricia Arquette quits Facebook after alleged cyberstalking, http://www.digitalspy.co.uk/showbiz/news/a344419/patricia-arquette-quits-facebook-after-alleged-cyberstalking.html, претражено 28. 10. 2011. године
91. Pew Research Center, http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/ , претражено 07. 02. 2015. године
92. Please Rob Me, http://pleaserobme.com/, претражено 10. 09. 2012. године
93. Приручник за родитеље – Глухи телефон, www.petzanet.hr/.../MODUL_4_roditelji-2_4.pdf. претражено 19. 12. 2015. године
94. Privacy: Stanford Encyclopedia of Philosophy, 2002, http://plato.stanford.edu/entries/privacy/, претражено 16. 02. 2015. године
95. Project Bullrun – classification guide to the NSA's decryption program, http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide, претражено 08. 04. 2015. године
96. Quit Stalking Me – Report a Cyberstalker, http://quitstalkingme.com, претражено 02. 07. 2014. године

97. Recommendations to the European Council Europe and the global information society, http://channelingreality.com/Digital_Treason/Brussels_1995/ Bangemann_report.pdf, претражено 04. 12. 2014. године
98. Report and Guidance on Privacy in Social Network Services - ”Rome Memorandum” - 43rd meeting, 3-4 March 2008, Rome (Italy), http://www. datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf, претражено 12. 09. 2015. године
99. Resmburg v. Docusearch, http://caselaw.findlaw.com/nh-supreme-court/ 1132429.html, претражено 27. 11. 2014. године
100. Савети за искључивање географског означавања на мобилним телефонима (“Tips to Turn Off Geo-Tagging on Your Cell Phone“), ABC news, 2010, http://abcnews.go.com/Technology/celebrity-stalking-online-photos-videos-give-location/story?id=11443038#.T603t8WkfTo , претражено 12. 08. 2012. године
101. Shanghai Cooperation Organisation (SCO), www.sectsco.org, претражено 20. 11. 2014. године
102. Сигурносни ризици друштвених мрежа - Хрватска академска и истраживачка мрежа, www.cert.hr, претражено 17. 03. 2015. године
103. Службене web странице Европске Уније, www.europa.eu
104. Слобода на интернету и говор мржње online: медијска политика и интернет у БИХ, Internews u BIH, Sarajevo, 2014, http://internews.ba/ sites/default/files/resursi/Govor%20mrznje%20na%20internetu.pdf, претражено 02. 12. 2015. године
105. Social Bakers, http://www.socialbakers.com/facebook-statistics/serbia, претражено 11. 07. 2014. године
106. Social network, http://www.computerhope.com/jargon/s/socinetw.htm, претражено 08. 06. 2014. године
107. Social network, http://dictionary.reference.com/browse/social+network , претражено 07. 06. 2014. године
108. Social network, http://www.webopedia.com/TERM/S/social_network.html, претражено 07. 06. 2014. године
109. Social networking, http://www.investopedia.com/terms/s/social-networking. asp, претражено 07. 06. 2014. године, http://www.investopedia.com /terms/s/social-networking.asp , претражено 07. 06. 2014. године

110. Social networking, http://www.techterms.com/definition/socialnetworking, претражено 07. 06. 2014. године
111. Social networking site, http://www.webopedia.com/TERM/S/social_networking_site.html , претражено 07. 06. 2014. године
112. Sophos, http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/, претражено 19. 12. 2012. године
113. State wants MySpace to raise minimum age, Reuters, 2006, http://www.rapidnewswire.com/5036-myspace-0245.htm, претражено 29. 12. 2013. године
114. Стив Рамбам - Приватност је мртва – преболите то, Google video, http://www.documentary24.com/privacy-is-dead-get-over-it--317/, претражено 08. 08. 2012. године
115. Stop ACTA, http://www.stopacta.info/, претражено 20. 08. 2015. године
116. Stop Cyberbullying, www.stopcyberbullying.org
117. StopCyberbullying.org: "How It Works", http://www.stopcyberbullying.org/how_it_works/index.html, претражено 13. 03. 2015. године
118. STUDY: Kids Try To Access Social Networks Nearly Twice As Much As Porn Sites, http://www.adweek.com/socialtimes/kaspersky-lab-study-kids-parental-control/422432, претражено 10. 01. 2015. године
119. Ten Reasons Why Someone is Stalking You Online, http://quitstalkingme.com/2011/07/28/ten-reasons-why-someone-is-stalking-you-online/, претражено 02. 07. 2014. године
120. The Anti-Counterfeiting Trade Agreement – ACTA, https://www.eff.org/files/filenode/acta1105_en.pdf, претражено 20. 08. 2015. године
121. The Association of Southeast Asian Nations, http://www.asean.org/communities/asean-political-security-community/item/joint-communique-of-the-28th-asean-chiefs-of-police-conference-brunei-darussalam-25-29-may-2008, претражено 12. 11. 2014. године
122. The Brief History of Social Media: Where people interact freely, sharing and discussing information about their lives, http://www2.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html, претражено 07. 02. 2015. године

123. The FBI – Common Fraud Schemes: Internet Fraud, http://www.fbi.gov/scams-safety/fraud/internet_fraud , претражено 03. 05. 2013. године
124. The First Interpol Training Seminar for Investigators of Computer Crime, Paris, December 7-11, 1981, видети http://cybercrimelaw.net/documents/Strasbourg.pdf, претражено 08. 11. 2014. године
125. The Library of Congress, http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1966:, претражено 16. 01. 2015. године
126. The Mobbing Encyclopaedia, Bullying; Whistleblowing; The Definition of Mobbing at Workplaces, adresa: http://www.leymann.se/English/12100E.HTM, претражено 07. 09. 2012. године
127. The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979, видети http://cybercrimelaw.net/documents/Strasbourg.pdf, претражено 01. 11. 2014. године
128. The United States Department of Justice, http://www.justice.gov/criminal/cybercrime/intl.html, претражено 16. 04. 2014. године
129. The evolution of privacy on Facebook, http://mattmckeon.com/facebook-privacy/, претражено 17. 02. 2014. године
130. Top 10 Internet Frauds, National Fraud Information Center, http://www.nclnet.org/, претражено 14. 11. 2014. године
131. Top 10 Social Networking Sites, http://news.discovery.com/tech/top-ten-social-networking-sites.html, претражено 05. 08. 2012. године
132. Твитер - Политика приватности - Скупљање,коришћење и измена корисничких података, https://twitter.com/privacy, приступ 04. 08. 2012. године
133. Ultrascan Advanced Global Investigations, http://www.ultrascan-agi.com/, претражено 12. 03. 2015. године
134. United Nations Office on Drugs and Crime, Tenth UN Congress on the Prevention of Crime and Treatment of Offenders ”Crime and Justice: Meeting the Challenges of the Twenty-first Century”, http://www.uncjin.org/Documents/congr10/4r3e.pdf, претражено 12. 12. 2014. године и http://www.unodc.org/congress/en/previous/previous-10.html, претражено 12. 08. 2015. године

135. United Nations Office of Drugs and Crime, 2008, www.undoc.org/en/about-undoc/index, претражено 15. 08. 2015. године
136. University of Toronto - G8 Information Centre, http://www.g8.utoronto.ca/, претражено 07. 11. 2014. године
137. Unmasking the Five Eyes' global surveillance practices, http://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices, претражено 08. 04. 2015. године
138. Us National Homeland Security - Presidential Policy Directive / PPD-8: National Preparedness, http://www.dhs.gov/presidential-policy-directive-8-national-preparedness, претражено 24. 10. 2015. године
139. U.S. v. Romero, 189 F.3d. 576 (7th Cir. 1999), http://openjurist.org/189/f3d/576/united-states-of-america-v-richard-romero, претражено 12. 09. 2014. године
140. U.S. v. White, Case No. IP99-CR-0005-01-M/F (S.D. Ind.1999), http://www.casebriefs.com/blog/law/criminal-procedure/criminal-procedure-keyed-to-israel/arrest-search-and-seizure/united-states-v-white/, претражено 12. 09. 2014. године
141. Вијести online, http://www.vijesti.me/vijesti/u-bijelom-polju-silovana-djevojcica-napasnik-je-namamio-preko-fejsbuka-clanak-34026/, претражено 10. 08. 2012. године
142. Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking, Women's Aid Federation of England, 2014, www.womensaid.org.uk, претражено 08. 01. 2015. године
143. WHOA- Working to Halt Online Abuse, http://www.haltabuse.org/resources/laws/texas.shtml, претражено 16. 01. 2015. године
144. Women's Aid conference links online abuse to off-line violence against women, Women's Aid, September 2013, www.womensaid.org.uk/stalking-links, претражено 21. 03. 2015. године
145. Work force, www.workforce.com, претражено 29. 04. 2013. године
146. Workplace Bullying Institute, http://www.workplacebullying.org/individuals/problem/definition/, претражено 20. 04. 2013. године
147. World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm, претражено 07. 11. 2014. године

ПРИЛОЗИ

Биографија аутора

Вида Вилић рођена је 14.06.1979. године, у Нишу, где је 2004. године завршила студије на Правном факултету Универзитета у Нишу. Као судијски приправник у Општинском суду у Нишу (2004 - 2007) положила је правосудни испит (2007). Била је запослена као правни саветник у Регионалном центру ProCredit Bank a.д. Београд у Нишу; а затим у Служби за послове Скупштине Града као самостални стручни сарадник на пословима припреме и одржавања седница Скупштине Града Ниша и седница радних тела Скупштине (2008 – 2011). Од 01.07.2011. године ради на Клиници за стоматологију Ниш као помоћник директора за правне послове.

У научним и стручним часописима објавила је више радова из области права, криминологија и виктимологије и учествовала у раду научних и стручних скупова, јавних трибина, округлих столова, радионица, едукативних семинара. Учествовала је и у значајном броју пројеката који су промовисали људска права, борбу против насиља у породици, заштиту жена од насиља, женско здравље и сл. (родне студије, Правна клиника за заштиту права жена – пружање бесплатне правне помоћи женама, Световалиште за жене оболеле од рака дојке), реформу правних студија, предузетништво жена, право Европске уније.

Једна је од оснивачица и чланица *Женског истраживачког центра за едукацију и комуникацију Ниш*, била је председница *Европског удружења студената права ELSA – Локална група Ниш* и нишког огранка *Младих правника Србије*, активна је чланица *Виктимолошког друштва Србије* и чланица *Етичког одбора Института за јавно здравље.*

Прилог 1 - ИЗЈАВА О АУТОРСТВУ

Изјављујем да је докторска дисертација, под насловом

ПОВРЕДА ПРАВА НА ПРИВАТНОСТ ЗЛОУПОТРЕБОМ ДРУШТВЕНИХ МРЕЖА КАО ОБЛИК КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

која је одбрањена на Правном факултету Универзитета у Нишу:

- резултат сопственог истраживачког рада;
- да ову дисертацију, ни у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;
- да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се објаве моји лични подаци, који су у вези са ауторством и добијањем академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада, и то у каталогу Библиотеке, Дигиталном репозиторијуму Универзитета у Нишу, као и у публикацијама Универзитета у Нишу.

У Нишу, _____.

Потпис аутора дисертације:

_____

Др Вида М. Вилић

Прилог 2 - ИЗЈАВА О ИСТОВЕТНОСТИ ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

Наслов дисертације:

ПОВРЕДА ПРАВА НА ПРИВАТНОСТ ЗЛОУПОТРЕБОМ ДРУШТВЕНИХ МРЕЖА КАО ОБЛИК КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Изјављујем да је електронски облик моје докторске дисертације, коју сам предао/ла за уношење у **Дигитални репозиторијум Универзитета у Нишу,** истоветан штампаном облику.

У Нишу, _____.

Потпис аутора дисертације:

_____

Др Вида М. Вилић

Прилог 3 - ИЗЈАВА О КОРИШЋЕЊУ

Овлашћујем Универзитетску библиотеку „Никола Тесла“ да у Дигитални репозиторијум Универзитета у Нишу унесе моју докторску дисертацију, под насловом:

ПОВРЕДА ПРАВА НА ПРИВАТНОСТ ЗЛОУПОТРЕБОМ ДРУШТВЕНИХ МРЕЖА КАО ОБЛИК КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Дисертацију са свим прилозима предао/ла сам у електронском облику, погодном за трајно архивирање.

Моју докторску дисертацију, унету у Дигитални репозиторијум Универзитета у Нишу, могу користити сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons), за коју сам се одлучио/ла.

1. Ауторство **(CC BY)**
2. **Ауторство – некомерцијално (CC BY-NC)**
3. Ауторство – некомерцијално – без прераде **(CC BY-NC-ND)**
4. Ауторство – некомерцијално – делити под истим условима **(CC BY-NC-SA)**
5. Ауторство – без прераде **(CC BY-ND)**
6. Ауторство – делити под истим условима **(CC BY-SA)**

У Нишу, _____.

Потпис аутора дисертације:

_____

Др Вида М. Вилић