UDK: 343.45:004.738.5

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

ПРИВАТНОСТ КОРИСНИКА ДРУШТВЕНИХ МРЕЖА

***Апстракт**: 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 да се они налазе. Управо својом популарношћу и великим бројем корисника, друштвене мреже су створиле својеврстан "надзор" над свакодневним активностима људи, њиховим навикама, њиховим кретањем и дружењем. Сама чињеница да је личне податке могуће сакупљати, похрањивати, дистрибуирати, умножавати, објављивати и чинити доступним широком кругу лица, створила је несигурност и осећај недовољне заштићености. Приватност на Интернету подразумева право на личне информације - чување, употреба, обезбеђење од трећих лица и приказивање личних информација преко Интернета, као и идентификационе информације које се односе на посетиоца одређене Интернет странице. 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. Најчешће злоупотребе и повреде приватности коришћењем података, који се налазе на друштвеној мрежи, су: крађа идентитета, прогањање и узнемиравање, манипулација личним подацима, који се односе на запошљавање, злоупотреба фотографија на Интернету и др. 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.*

***Кључне речи**: друштвене мреже, приватност на Интернету, злоупотреба права на приватност, манипулација личним подацима, заштита приватности на друштвеним мрежама.*

Увод

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 да се они налазе. Неке од Интернет апликација су довеле у питање приватност, отварајући расправе, да ли је код друштвених мрежа заправо реч о комерцијалном интересу, или о стварању нових комуникација и повезивању људи широм планете. Управо својом популарношћу и великим бројем корисника, друштвене мреже су створиле својеврстан "надзор" над свакодневним активностима људи, њиховим навикама, њиховим кретањем и дружењем.

Интернет се данас користи у већини земаља света, а сваким даном расте и број његових корисника. Према подацима о обиму коришћења Интернета, од 2000. до 2005. године, употреба Интернета је повећана за око 160% и процењује се да око 938 милиона људи на неки начин има приступ Интернет мрежи.[1] Број корисника је веома велики у многим земљама у свету: у Северној Америци, око 158 милиона корисника, у Европи, 95 милиона корисника, Азији 90 милиона корисника, Јужној Америци 14, и у Африци 3 милиона корисника.[2] Овај број је у сталном порасту: према истраживањима, само у Русији тај број је последњих година повећан са 3,5 на 8 милиона активних Интернет корисника.[3]

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 лица 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". 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 IP адреса које нису могле да препознају, ни ко је пошиљалац, нити

1 World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm приступ 20.9.2012.године

2 ibid.

3 ibid.

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. *buggs*) 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 суптилном експлоатацијом корисникових жеља и потреба.[4]

Појам и најчешће коришћене друштвене мреже

Модерни свет Интернета значајно је промењен настанком друштвених јавних мрежа. 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. Ову привилегију је имао ограничен број лица, који су најширем броју корисника презентовали информације значајне за велики број лица.

У данашње време, друштвене мреже представљају начин за повезивање људи широм планете. Уз помоћ друштвених мрежа, свет је у могућности да визуализује везе између појединаца.[5] Чак иако вредност ових веза не осликава у потпуности реалан живот и стварне односе, друштвене мреже нам помажу да сазнамо везе између људи, како би их боље разумели и утврдили међусобну повезаност.[6]

Друштвена (социјална) мрежа најчешће се дефинише као друштвена структура, састављена од појединаца (или организација) који се називају „чворови“, а који су повезани с једним или више специфичних типова међузависности, као што су: вредности, визије, идеје, финансијски интереси, пријатељство, сродство, заједнички интерес, финансијска

4 Spinello, R.:”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 1.3.2013.године

5 Fred Stutzman, Ph.D. student and teaching fellow, School of Information and Library Science at UNC Chapel Hill, USA, navedeno kod Strickland, J.: Top 10 Social Networking Sites, http://news.discovery.com/tech/top-ten-social-networking-sites.html, приступ 5.8.2012.године

6 Ibid.

размена, недопадање, сексуални односи или односи поверења, знања или престижа[7].

Користећи друштвене мреже, појединци стварају јавне или полујавне профиле у оквиру правила саме мреже, праве списак корисника с којима желе да контактирају и размењују информације, одржавају већ створене односе унутар друштвене мреже.[8] Сама друштвена мрежа дозвољава корисницима да направе сопствене презентације и личне профиле, који сви заједно чине „друштво пријатеља, рођака, колега" који се међусобно налазе у интеракцији.[9]

Све друштвене мреже функционишу преко **сервиса за друштвену мрежу**, који представља 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.

Први облици сервиса за друштвену мрежу јављају се деведесетих година XIX века, попут соба за ћаскање, где је више корисника могло ћаскати међусобно. На некима је био дозвољен приступ само преко регистрације, док је код других било потребно само имати надимак (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: они, поред првобитне улоге у комуникацији, имају улогу маркетинга, промовишући друге веб-сајтове и низ различитих услуга.

У огромном простору комуникација, издвојило се десет најпопуларнијих и најкоришћенијих друштвених мрежа данашњице.

- MySpace – иако није најстарија друштвена мрежа, утицала је на формирање многих данас још популарнијих друштвених мрежа. Ова Мрежа је прва инкорпорисала много различитих Интернет услуга у један јединствени облик, омогућавајући корисницима прегледно, несметано и брзо комуницирање и доступност великог броја различитих садржаја. Сви регистровани кориснички профили на MySpace имали су

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

8 Spinello, R.:"Privacy and Social Networking Technology", International Review of Information Ethics Vol. 16 (12/2011), стр.42, http://www.i-r-i-e.net/inhalt/016/spinello.pdf, претражено 1.3.203.године

9 Ibid.

на располагању следеће опције комуницирања: могућност објављивања блогова, новости и ажурирања личних статуса, чиме је створен веома детаљан и богат профил појединца. Корисницима је такође било омогућено да објављују и шаљу фотографије, видео снимке и музику, као и да створе различите интересне групе, којима и други корисници могу да се прикључе.

- Orkut – представља друштвену мрежу чији је власник Google, иако се мрежом управља из Бразила. Према анализама, које је спровела аналитичка кућа comScore, више од 20 милиона Бразилаца су током 2008. године били посетиоци ове друштвене мреже, док је у истом периоду MySpace посетило само 893.000 Бразилаца[10]. Ова друштвена мрежа је популарна и у Индији, и Индијци представљају 17% укупног броја корисника.[11]

- 51.com – друштвена мрежа која, за разлику од осталих, нема за циљ да створи једно глобално друштво, већ је усмерена само на једну географску циљну групу – на Кину. Током 2008. године ова мрежа имала је 120 милиона чланова у Кини[12]. Регистровани чланови ове друштвене Мреже могу да персонализују странице свог профила, постављају фотографије и пишу блогове.

- Friendster - 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. Популарност ове друштвене мреже данас је много мања, али она и даље важи за посећенију друштвену мрежу у САД и Азији.

- Skyrock – 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 (*chat rooms*) 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[13].

- Hi5 – друштвена мрежа, која је 2008. године представљала мрежу која се најбрже ширила – само у периоду јануар-јуни 2008. године

10 http://www.comscore.com/, приступ 5.8.2012.године
11 Ibid.
12 Ibid.
13 Ibid.

Hi5 је користило 78% укупног броја регистрованих корисника свих друштвених мрежа[14]. Hi5 је настао у Сан Франциску у САД 2003. године, а већ до 2005.године имао је око 10 милиона регистрованих чланова. 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 Мексика и латиноамеричких земаља.

- YouTube - представља виртуелно место, где је могуће постављати музику и видео снимке, а не само блогове и слике, као на класичним друштвеним мрежама. Корисници могу да комуницирају преко писања коментара и гледања/слушања музике, па тако сваки регистровани члан може да има свој профил, да поставља или коментарише музику, да уписује које год информације жели. Јединственост ове Мреже се огледа у могућности влогинга (*video logging – vlogging*) који представља паралелу блогингу (*blogging*) – регистровани чланови комуницирају и размењују поруке преко музике коју објављују.

- LinkedIn – Ова друштвена мрежа има за циљ да повеже пословне људе широм света, како би они били продуктивнији и успешнији. Иако је ова друштвена мрежа дизајнирана само за професионалне кориснике, процењује се да их има око 35 милиона.[15] На овој Мрежи је могуће успоставити контакт с послодавцима који нуде запослење, пронаћи потенцијалне клијенте за пословну сарадњу, сарађивати на различитим пројектима кроз "виђење" у виртуелним собама и сл.

- Twitter – друштвена мрежа која је једним делом веб сајт, а делом јавна мрежа, Твитер је виртуелно место осмишљено за креирање профила, пласирање информација и прављење група "обожаватеља", који вас у том вирутуелном простору "прате" (енгл. *follow*), исто као што неко прати њих. Основан 13. јула 2006. године, Твитер 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 (engl. *microblogging*) и све више добија на популарности. Твитер је изузетно популаран међу познатим личностима, јер представља могућност јефтине, а популарне рекламе. 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

14 Ibid.
15 Ibid.

круга пријатеља, док је услуга у старту подешена тако да шаље уносе свима, који се на њих пријаве. Од марта 2009. године, Твитер је забележио раст популарности у свету. До 2011. године, регистровано је око 300 милиона корисника.[16] Број, тренутно активних регистрованих корисника из Србије, је тешко проценити, познато је да их је 2009. године било најмање око три стотине.[17]

- Facebook (FB) – Марк Цукерберг (Mark Zuckerberg) није могао да замисли шта ће направити, када је 2004. године питао своје колеге на Харварду да покушају да направе виртуелну Интернет заједницу, у којој ће моћи да себе представе, потраже друге и позову остале особе 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“ (енгл. *Ivy League*). После неког времена, чланство је омогућено свим студентима и средњошколцима, а на крају је омогућено свим особама које имају 13 или више година.

Фејсбук 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 особама. Такође, особе могу додавати пријатеље, слати им поруке, а могу и убацивати нове податке у своје профиле, како би обавестили пријатеље о себи.

Фејсбук је 2006. године постао отворена мрежа, позивајући људе широм света да, уписивањем само e-mail адресе, постану део ове заједнице. Поред размењивања личних информација и стварања профила, креиран је револуционарни програмски интерфејс (енгл. *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)[18] имала више од 10 милиона регистрованих посетилаца. Приход основачима од коришћења ове друштвене Мреже (реклама и видео-игрица), у току 2011. године,

16 Taylor, Chris (27. 6. 2011.). „Social networking ‘utopia’ isn’t coming“. CNN, http://articles.cnn.com/2011-06-27/tech/limits.social.networking.taylor_1_twitter-users-facebook-friends-connections?_s=PM:TECH, приступ 10.8.2012.године

17 Zsteva (January 29th, 2009). „Број твиттер корисника у Србији“, http://zsteva.info/blog/2009/01/29/broj-twitter-korisnika-u-srbiji/, приступ 10.8.2012.године

18 Ibid.

износио је 4.27 милијарди долара,[19] а број корисника је до краја 2011. године порастао на 600 милиона.

Према подацима са сајта, Фејсбук данас има око 750 милиона активних корисника широм света.[20] У неким земљама, као што су Сирија,[21] Кина,[22] Вијетнам,[23] и Иран,[24] приступ овој Интернет страници је повремено блокиран, а исто је учињено и на бројним радним местима, како запослени не би трошили време на посету сајта.[25] Један од проблема је представљало поштовање приватности корисника, које је неколико пута доведено у питање.

Приватност корисника друштвених мрежа

Убрзани развој технологије омогућио је све бржу обраду података и ефикасно функционисање, доступност бројних информација, истовремено обезбеђујући појединцу да као део огромне базе података остане „анониман". У циљу борбе против свих видова компјутерског криминалитета, било је 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.

Међутим, примери указују и на другу страну напретка. Управо овакав вид „улажења у траг" извршиоцима различитих облика Интернет (*cyber*) криминалитета довео је до све чешћих глобалних ***напада на приватност***, чији је циљ злоупотреба информација о појединцу.

19 „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 , приступ 10.9.2012.године

20 http://newsroom.fb.com/, приступ 10.098.2012.године

21 Khaled Yacoub Oweis (Fri Nov 23, 2007 4:54pm). „Syria blocks Facebook in Internet crackdown". Reuters , http://www.reuters.com/article/2007/11/23/us-syria-facebook-idUSOWE37285020071123, приступ 10.8.2012.године

22 „China's Facebook Status: Blocked". ABC News. 8. 7. 2009., http://abcnews.go.com/blogs/headlines/2009/07/chinas-facebook-status-blocked/, приступ 10.8.2012. године

23 Ben Stocking (17. 11. 2009.). „Vietnam Internet users fear Facebook blackout". Associated Press, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/11/17/international/i033256S37.DTL, приступ 10.8.2012.године

24 Afshin Shahi (27. 7. 2008.). „Iran's digital war". Daily News Egypt, http://dailystaregypt.com/article.aspx?ArticleID=15313, приступ10.8.2012.године

25 Robert Benzie (3. 5. 2007.). „Facebook banned for Ontario staffers". TheStar.com, http://www.thestar.com/News/article/210014, приступ 10.8.2012.године

На основу тих информација, могуће је идентификовати појединца и детаље из његовог живота, припадност групи, свакодневно кретање и понашање – једноставно, могућа је реконструкција 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,[26] као и идентификационе информације, које се односе на посетиоца одређене Интернет странице. Велики број експерата из области виртуелне безбедности и приватности верују да приватност не постоји: „Приватност је мртва – преболите то“, према мишљењу Стива Рамбама, приватног детектива у области Интернет приватности.[27]

Приватност у виртуелном простору може да се дефинише и као „ограничени приступ личним подацима/ограничена контрола личних података“.[28]

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.

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“).

Приватност се, у складу са наведеним, може дефинисати као „стање брижљиво ограниченог приступа личним подацима“.[29] Свако поступање, другачије од описаног, представља злоупотребу права на приватност, а сакупљање осетљивих личних података о некоме, без

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

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

28 Tavani and Moor, 2001., наведено код Spinello, R.:”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 1.3.203.године

29 Spinello, R.:”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 1.3.203.године

његове сагласности и знања, може за циљ да има манипулацију тим подацима.

Најбољи начин за заштиту приватности, свих Интернет корисника, је примена принципа 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.

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 питањем 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.

Заштита података, по дефиницији коју даје Џозеф Катаначи (Joseph Cannataci),[30] значи заштиту појединца од злоупотребе или неадекватне употребе личних података од стране неког лица, приватне организације или државе. У вези са заштитом приватности података поставља се низ питања функционалног, организационог и безбедносног карактера, као што су: ограничавање располагања одређеним врстама података, обавеза давања информација државним органима од стране недржавних субјеката, обавештавање грађана о њиховим подацима, технички стандарди система, стручност лица која обрађују податке, мере обезбеђења хардвера, софтвера, и сл.

Приватност на друштвеним мрежама зависи и од степена контроле, коју корисник друштвене мреже има над приступом и употребом личних података.[31]

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

31 http://sr.wikipedia.org/wiki/, приступ 4.8.2012.године

Углавном сви сајтови, са којих 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.[32] 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.

Повреда права на приватност корисника друштвених мрежа и манипулација личним подацима

Већа популарност сајтова за друштвено умрежавање довела је до интензивнијег разматрања заштите приватности. Спокео (енгл. *Spokeo*) не представља класичну друштвену мрежу, али представља претраживач за повезивање лица, која користе 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.[33]

Интересантан пример могуће злоупотребе друштвене мреже за извршење неког другог кривичног дела представљају подаци дати 2010. године на Интернет порталу www.PleaseRobMe.com, када је приказан преглед свих профила корисника Твитера, 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.[34] Пошто су све информације најчешће јавне и садрже кућну адресу корисника друштвене мреже, заинтересована лица лако

32 Bangeman, E. 2010. Report: Facebook caught sharing secret data with advisers,http://arstechnica.com/tech-policy/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers/, приступ 4.8.2012.године

33 About Spokeo, http://www.spokeo.com/blog/about, приступ 12.8.2012.године

34 http://pleaserobme.com/, pristup 10.9.2012.godine

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, 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.

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 злоупотребом информационих система, може се на разне начине манипулисати. Најчешћи појавни облици компјутерског криминалитета су: компјутерске крађе, компју -терске 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.[35]

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

1) Крађа идентитета састоји се у неовлашћеном коришћењу личних података (датум рођења, тренутно пребивалиште, број телефона, занимање, пријатељи, личне слике), који су постали јавно доступни.[36] 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. Велики број сервиса за друштвене мреже чува личне податке о корисницима, како их корисник не би поново уносио када нпр. следећи пут купује преко Интернет,а или посећује одређени веб сајт. Ово представља добар начин да се приступи туђим личним информацијама, па то често користе хакери и крадљивци идентитета, како би на нелегалан начин дошли до приступа банковним

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

36 Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case). страна 8, http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, приступ 4.8.2012.године

рачунима и кредитним картицама и са њих пребацили средства на своје рачуне или куповали, користећи туђ новац.[37]

2) **Прогањање и узнемиравање** путем коришћења Интернет мреже (енгл. *cyber stalking*) дефинише се као упорно и циљано злостављање појединца путем електронских начина комуникације.[38] 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. 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.

3) Манипулација личним подацима који се односе на запошљавање представља такав вид повреде приватности, када послодавци, приликом избора лица које ће запослити, проверавају кандидате претраживањем друштвених мрежа. Послодавци користе друштвене мреже и за проверавање својих запослених: 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.[39]

4) **Злоупотреба фотографија на Интернету** представља такав облик повреде приватности, када се неовлашћено користе и приказују фотографије са налога корисника друштвених мрежа, без њихове сагласности. 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 с неким или проследи. На пример, Фејсбук задржава право да објави корисничке информације, или да их подели са другим компанијама, адвокатима, судовима, државним службама итд. уколико сматра да је то неопходно.[40]

37 Цит. према Internet Identity Theft, http://articles.winferno.com/computer-fraud/internet-identity-theft, приступ 17.9.2012.године

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

39 Ibid.

40 У чланку објављеном у „АБЦ вестима" (енгл. 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. Технологија препознавања лица може бити искоришћена за приступ личним подацима особе. Истраживачи Карниги Мелон Универзитета (енгл. Carnegie Mellon University) су комбиновали скениране слике и

Повреда права на приватност најчешће се врши у оквиру друштвених мрежа, као што су Фејсбук, Твитер и LinkedIn.

а) Фејсбук

Корисник који жели да креира налог на **Фејсбуку** мора да наведе своје име, e-mail адресу, датум рођења и пол.[41] Ови подаци, укључујући и профилну слику корисника, корисничко име и лозинку постају доступни свима на Интернету.[42] Сваки пут када се корисник улогује на свој профил, када прегледава туђи профил, потражи одређену страницу или пријатеља, кликне на оглас, који се налази на страници, користи било коју апликацију и сл. Фејсбук добија, прикупља и чува ове податке, а уколико корисник објави фотографију, или видео запис, Фејсбук бележи и време, датум и место на коме је фотографија, или видео запис настао. Подаци се прикупљају и складиште, без обзира како и одакле су послати на профил (да ли су послати са рачунара, мобилног телефона, или било ког другог уређаја са кога је могуће приступити Фејсбуку).

Наведене информације које је Фејсбук сакупио[43] постају доступне великом кругу лица: пријатељима корисника, свим корисницима ове Мреже, а уколико се опција не искључи, биће доступне и маркетиншким партнерима с којима Фејсбук сарађује, оглашивачима који купују рекламни простор, као и ауторима видео игара и апликација на Фејсбуку. Оснивачи Фејсбука су одмах и објаснили сврху коришћења личних података корисника: ради сигурности производа и услуга Фејсбука, заштите права интелектуалне својине Фејсбука 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

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 Више о овоме. Online photos can reveal our private data say experts, BBC News, 2011, http://www.bbc.co.uk/news/technology-14386514, приступ 12.8.2012. године

41 Фејсбук - Политика о коришћењу података:Информације добијене од корисника, Registration information, http://www.facebook.com/about/privacy/your-info#inforeceived, приступ 4.8.2012.године

42 Фејсбук - Политика о коришћењу података:Информације добијене од корисника,Information that is always publicly available, http://www.facebook.com/about/privacy/your-info#inforeceived, приступ 4.8.2012.године

43 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, приступ 4.8.2012.године

дељења заједничких слика, за решавање техничких проблема и начина побољшања саме услуге. [44]

Како би Фејсбук 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. Сама правила Фејсбука су таква да подстичу кориснике да откривају што више личних података, и да на тај начин сами руше своју приватност.

У полиси о коришћењу услуга наведено је да је корисник и даље власник свих информација, да је у могућности да забрани Фејсбуку коришћење личних информација и података, или да захтева да му се име не спомиње, како би идентификација била спречена. Интересантно је да већина корисника Фејсбука 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.

Када би неки корисник хтео да деактивира свој налог, политика Фејсбука 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, 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, Фејсбук је почео да користи тзв. Бикон програм (енгл. *Beacon program*), који је имао за задатак да пријављује Интернет активности корисника разним другим корисницима и рекламним агенцијама, што је разбеснело милионе корисника ове друштвене мреже.[45] На тај начин, свака куповина, коју би преко Интернета неки Фејсбук корисник обавио, 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 с његовом активности, нити да под подешавањима, која се односе на приватност, корисник ову опцију не може никако да трајно искључи, или бар привремено блокира. Фејсбук је тек 2009. године престао са коришћењем овог програма, тек

44 Ibid.

45 Видети: Фејсбук - Политика о коришћењу података:Информације добијене од корисника,Deleting and deacrivating your account, http://www.facebook.com/about/privacy/your-info#inforeceived, приступ 4.8.2012.године

након бројних критика Електронског информационом центра за заштиту приватности (*Electronic Privacy Information Center – EPIC*).[46]

Фејсбук 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, Фејсбук је 2010. године променио своју политику приватности, омогућавајући корисницима да подешавањима свог корисничког налога утичу на доступност и видљивост личних података.

Упркос напретку у чувању приватности које Фејсбук пласира, и даље постоји неколико „слабих тачака" које угрожавају приватност личних података корисника ове друштвене мреже. Нпр. приликом претраге одређеног имена преко Google претраживача, прва опција која се добија као резултат претраге је комплетан Фејсбук 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.[47]

б) Твитер

Када корисник креира или реконструише Твитер налог, обавезан је да остави неке податке о себи: име, корисничко име, лозинку и е-адресу. Сервери на Твитеру аутоматски евидентирају све податке (тзв. дневник података), креиране од стране корисника.[48] Дневник података може да садржи информације као што су IP адреса, тип претраживача, посећене странице, оператер мобилне телефоније корисника, најчешћи претраживани термини, интеракција са сајтом Твитера, апликацијама и рекламама. Твитер 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 с трећим лицима.[49]

46 Spinello, R.:"Privacy and Social Networking Technology", International Review of Information Ethics Vol. 16 (12/2011), стр.43, http://www.i-r-i-e.net/inhalt/016/spinello.pdf, претражено 1.3.203.године

47 Ibid.

48 Твитер - Политика приватности - Скупљање,коришћење и измена корисничких података, https://twitter.com/privacy, приступ 4.8.2012.године

49 Видети: Rushe, Dominic (January 8, 2011). „Icelandic MP Fights US Demand for Her Twitter Account Details", *The Guardian*, http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages, приступ 4.8.2012.године

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. Интересантан је случај Бригите Јорнсдотр (Birgitta Jonsdottir), посланице у парламенту Исланда и некадашњег волонтера Викиликса (WikiLeaks), која тренутно води судски спор са америчким правосудним системом, због покушаја да се искористе њене приватне поруке, које је слала и примала на Твитеру, 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 с обичним људима, који се из неког разлога нађу у сличној ситуацији?[50] Твитер 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.

Што се тиче „трговине" прикупљеним подацима од корисника, Твитер задржава право да прода све сакупљене информације, ако дође до промене власника мреже. Када је налог на Твитеру деактивиран, он се не брише 30 дана, након овог периода почиње процес брисања налога, што може да потраје и до недељу дана.[51]

в) LinkedIn

Као и приликом регистрације на Фејсбук или Твитер, 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 IP адресе, при чему је могуће добити и IP адресу корисника, тип коришћених претраживача, оперативни систем, који се користи и адресе свих посећиваних сајтова, у којима су уграђене технологије LinkedIn платформе.

50 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, приступ 12.8.2012.године

51 Твитер - Политика приватности - Скупљање,коришћење и измена корисничких података, https://twitter.com/privacy, приступ 4.8.2012.године

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[52]. LinkedIn се ограђује од неовлашћеног коришћења личних података на следећи начин: „Личне информације корисника биће безбедне у складу с индустријским стандардима и технологијама. Пошто Интернет није околина која је 100% сигурна, не можемо да гарантујемо или обезбедимо сигурност било које информацује, коју поставите на LinkedIn. Не постоји гаранција да информацијама неће бити приступано, да неће бити копиране, мењане, подељене са другима или уништене".[53]LinkedIn чува податке, све док је кориснички налог активан.

Подаци о регистрованим корисницима или информације које су објављивали корисници могу бити у следећим случајевима подељени с 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.

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,
- IP 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.

52 ЛинкедИн - Политика приватности, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, приступ 4.8.2012.године

53 ЛинкедИн - Политика приватности, Security, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, приступ 5.8.2012.године

Уместо закључка: могућности за заштиту приватности на друштвеним мрежама

Проналазак и развој компјутера представља резултат фасцинантног 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, зависност од коришћења компјутера може да буде искоришћена и за вршење кривичних дела.

С повећањем употребе Интернета и броја корисника, повећавају се и могућности за злоупотребу Интернет мреже. Смањење ризика од злопупотребе Интернета могуће је једино развијањем јединствених стандарда за коришћење Интернета и доношењем и применом одговарајућих закона, којима се инкриминишу понашања везана за злоупотребу Интернета. Закони којима се забрањује компјутерски криминалитет треба да буду веома флексибилни и да прате свакодневни развој компјутерске технологије и иновација.

Да би се смањио број злоупотреба друштвених мрежа и угрожавање права на приватност корисника друштвених мрежа, неопходно је створити одговарајуће законске механизме и правну регулативу за откривање и санкционисање ових друштвено неприхватљивих 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. 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 с 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.[54]

Уколико узмемо у обзир шта приватност представља и колико је исправно нечије приватне податке и информације делити с другима, намеће се питање: на који начин популарне друштвене мреже морају да поштују императив морално одговорног понашања, а на који начин сами корисници морају да воде рачуна о заштити своје приватности.

54 http://www.microsoft.com/security/online-privacy/social-networking.aspx, приступ 17.8.2012. године

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.

Значајан је избор сајтова, линкова и Интернет страница, с којих стижу поруке с друштвених мрежа. Сајтови треба да буду изабрани с 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.

Да 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 с познатим корисницима. „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“ (енг. *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 објављивати превише личних података и фотографија, 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 с децом о опасностима с

друштвених мрежа, и да деци помогну да на сигуран начин приступају друштвеној мрежи.

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,[55] 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.

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[56] 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, e-mail адресе или корисничког имена на друштвеној мрежи. Google такође даје могућност да се направи и "Google Alert" - аларм који ће кориснику послати информацију на адресу електронске поште, сваки пут када се на Интернету помене његово име или неки од личних података.

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 друштвених мрежа уз повећану пажњу, стално праћење и контрола од стране администратора и корисника само су најзначајнији фактори превентивног деловања.

55 Лица које мрежу одржава и које води рачуна о заштити права корисника, *прим. аут.*

56 www.google.com

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 *on line* напада на приватност и тиме утицали на смањење велике „тамне бројке" компјутерског криминалитета.

Литература

About Spokeo, http://www.spokeo.com/blog/about, pristup 12.8.2012. godine

Afshin Shahi (27. 7. 2008.). „Iran's digital war". Daily News Egypt, http://dailystaregypt.com/article.aspx?ArticleID=15313, pristup10.8.2012.godine

Bangeman, E. 2010. Report: Facebook caught sharing secret data with advisers, http://arstechnica.com/tech-policy/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers/, pristup 4.8.2012.godine

Ben Stocking (17. 11. 2009.). „Vietnam Internet users fear Facebook blackout". Associated Press, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/11/17/international/i033256S37.DTL, pristup 10.8.2012.godine

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

China's Facebook Status: Blocked. ABC News. 8. 7. 2009., http://abcnews.go.com/blogs/headlines/2009/07/chinas-facebook-status-blocked/, pristup 10.8.2012.godine

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 , pristup 10.9.2012.godine

Fejsbuk - Politika o korišćenju podataka:Informacije dobijene od korisnika, Registration information, http://www.facebook.com/about/privacy/your-info#inforeceived, pristup 4.8.2012.godine

Fejsbuk - Politika o korišćenju podataka:Informacije dobijene od korisnika,Information that is always publicly available, http://www.facebook.com/about/privacy/your-info#inforeceived pristup 4.8.2012.godine

Fejsbuk - Politika o korišćenju podataka:Informacije dobijene od korisnika,How we use the information we recieve, http://www.facebook.com/about/privacy/your-info#inforeceived, pristup 4.8.2012.godine

Fejsbuk - Politika o korišćenju podataka:Informacije dobijene od korisnika,Deleting and deacrivating zour account, http://www.facebook.com/about/privacy/your-info#inforeceived, pristup 4.8.2012.godine

Fred Stutzman, Ph.D. student and teaching fellow, School of Information and Library Science at UNC Chapel Hill, USA, navedeno kod Strickland, J.: Top 10 Social Networking Sites, http://news.discovery.com/tech/top-ten-social-networking-sites.html, pristup 5.8.2012.godine

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, pristup 12.8.2012.godine

Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case). strana 8, http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, pristup 4.8.2012.godine

http://www.bbc.co.uk/news/technology-14386514, приступ 12.8.2012. године

http://pleaserobme.com/, pristup 10.9.2012.godine

http://sr.wikipedia.org/wiki/, pristup 4.8.2012.godine

http://www.comscore.com/, pristup 5.8.2012.godine

http://newsroom.fb.com/, pretraženo dana 10.08.2012.godine

http://www.microsoft.com/security/online-privacy/social-networking.aspx, pristup 17.8.2012. godine

Internet Identity Theft, http://articles.winferno.com/computer-fraud/internet-identity-theft, pristup 17.9.2012.godine

Khaled Yacoub Oweis (Fri Nov 23, 2007 4:54pm). „Syria blocks Facebook in Internet crackdown". Reuters , http://www.reuters.com/article/2007/11/23/us-syria-facebook-idUSOWE37285020071123, pristup 10.8.2012.godine

Konstantinović Vilić, S, Nikolić Ristanović V., Kostić M.: Kriminologija, Pelikan print, Niš, 2009., s.182,183.

LinkedIn - Politika privatnosti, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, pristup 4.8.2012.godine

Robert Benzie (3. 5. 2007.). „Facebook banned for Ontario staffers". TheStar.com, http://www.thestar.com/News/article/210014, pristup 10.8.2012. godine

Rushe, Dominic (January 8, 2011). „Icelandic MP Fights US Demand for Her Twitter Account Details", *The Guardian*, http://www.guardian.co.uk/

media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages, pristup 4.8.2012.godine

Spinello, R.:"Privacy and Social Networking Technology", International Review of Information Ethics Vol. 16 (12/2011), стр.41-46, http://www.i-r-i-e.net/inhalt/016/spinello.pdf, страниці приступљено 1.3.2013.године

Stiv Rambam - Privatnost je mrtva – prebolite to, Google video, http://www.documentary24.com/privacy-is-dead-get-over-it--317/, pristup 8.8.2012.godine

Taylor, Chris (27. 6. 2011.). „Social networking 'utopia' isn't coming". CNN, http://articles.cnn.com/2011-06-27/tech/limits.social.networking.taylor_1_twitter-users-facebook-friends-connections?_s=PM:TECH, pristup 10.8.2012.godine

Tviter - Politika privatnosti - Skupljanje,korišćenje i izmena korisničkih podataka, https://twitter.com/privacy, pristup 4.8.2012.godine

World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm pristup 20.9.2012.godine

www.google.com

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

Zsteva (January 29th, 2009). „Broj twitter korisnika u Srbiji",http://zsteva.info/blog/2009/01/29/broj-twitter-korisnika-u-srbiji/, pristup 10.8.2012.godine

Prof. Miomira Kostić, LL.D
Full Professor,
Faculty of Law, University of Niš

Vida Vilić, LL.B.
PhD Student,
Faculty of Law, University of Niš

THE PRIVACY OF SOCIAL NETWORKS' USERS

Summary

One of the most powerful innovations in the short history of the Internet *is the emergence and development of social networks, which enable diverse forms of communication between people worldwide. Considering their popularity and a vast number of users, social networks have taken control over the users' daily activities, their habits, interests and social contacts. Given the availability of personal information which can be easily collected, stored, distributed, copied, published and made available to a wide range of other people, there is a a general sense of insecurity and lack of protection for Internet users.*

Internet privacy implies the right to privacy of one's personal information in terms of storing, using, securing personal data against third parties, displaying personal information via the Internet and disclosing information on the identity of visitors of certain websites. One of the major issues in the contemporary society is the reasonable extent and justification for collecting and distributing personal data via the Internet, as well as the and the scope of rights of other social network users to dispose of another's personal data. The most common forms of abuse and violation of Internet privacy by using one's personal data stored on a social network are: identity theft, cyber stalking and harassment, manipulation of personal data pertaining to employment, photograph abuse, etc. Taking into account the huge number of users, the availability of personal data, open communication between users, as well as a lack of relevant legal provision and regulations both at the national and international level, social networks are superb hiding places for the perpetrators of various types of cybercrime.

Key words: *social networks, Internet privacy, abuse of the right to privacy, personal data manipulation, privacy protection on social networks.*