

МОБИЛНЕ СОЦИЈАЛНЕ МРЕЖЕ – НОВИ РИЗИК ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

мр Звонимир Ивановић¹, Криминалистичко – полицијска академија, Београд
проф. др Божидар Бановић, Правни Факултет у Крагујевцу

Анстракт: Улога савремених телекомуникационих средстава сваким даном, у обичном животу, добија нове димензије. Орвелова 1984.год. има кулминацију у данашњем добу, разрада теме следи. У оваквом окружењу веома је значајно препознати добру праксу и адекватно спровести анализу сопствених могућности, потреба и адекватно акцептирати и прилагодити норме, којима се омеђавају простори за маневар. Аутори покушавају да дају преглед опасности које са собом носе поступања у социјалним мрежама уносећи у комплекс разматрања варијаблу мобилних телефонских мрежа и уређаја. Уводећи у разматрање и појам социјалне мобилне мреже, аутори покушавају да датом додају аналитички приступ, како кроз опасности које вребају у новом окружењу, тако и нормативном анализом. Феноменолошки аспект проблема друштвене појаве онлајн социјалних мрежа приказан је кроз анализу самог феномена уз ширење на нове садржаје, које он добија новим техничким иновацијама. Садржински нормативна анализа обухвата платформу ЕУ у датом окружењу и покушај компарације са прописима актуелним у датој области у Србији.

Кључне речи: социјалне мреже, мобилне социјалне мреже, законодавство социјалних мрежа, Интернет злоупотребе личних података, крађа идентитета

Увод

Савремени смарт телефони (или ПДА)² не користе се (или још боље немају за основну сврху) само за телефонирање, у смислу аудио везе, већ за најразличитије облике комуникације, али и web 2.0 апликације, наравно све уз постојећу и активну Интернет конекцију. Рапидан развој технологија и Интернета омогућио је неслућене интеракције људи, мењајући, скоро револуционарно, начин креирања односа међу људима али и односа људи са новим окружењем. У оквиру социјалних мрежа³ (Social Networking Sites СНС) развој великог броја апликација довео је до давања нових

¹ zvonimir.ivanovic@kpa.edu.rs

² Personal digital assistant или palmtop рачунар – рачунар за длан у буквалном преводу.

³ ЕНИСА дефинише социјалне мреже као „онлајн заједнице које омогућавају људима да преко изграђених „профила“ остварују контакте, комуницирају, да се сусрећу, размењују фотографије и видео записе са другим члановима те заједнице, са којима се веза у оквиру заједнице дозвољена (прихваћена), са њихове стране (дељена)“. Са функционалног становишта ЕНИСА социјалне мреже дели у две главне категорије: опште намене и „ниче“ соц. Мреже. Прве за основну смисао имају комуникацију и интеракцију корисника, размену мисли и идеја и свима је слободан приступ, оне гаје разноликост интереса (нпр. Facebook – али која све више нагиње у прву групу, Myspace, Badoo, Netlog). Друге дозвољавају корисницима посебне активности (LinkedIn,), пружајући прилике за склапање послова, остваривање пословних контаката, вршење пословних активности и сл. за више видети: Joseph Bonneau, Sören Preibusch, The privacy jungle: On the market for data protection in social networks, Eighth Workshop on the Economics of Information Security (WEIS 2009), 24–25 June 2009, доступан на <http://weis09.infosecon.net/files/156/index.html> (последњи пут приступљено 20.02.2010).

димензија социјалним интеракцијама, такође омогућио је и стварање великог простора и вештачког игралишта за социјалне експерименте. Присутност и мобилност на свим локацијама (зато јер су zgodни за ношење) оваквим уређајима просто не пружа никакву алтернативу, за остваривање инстант социјалних интеракција. Њихове техничке могућности, које су, сваким даном, све веће и ергономичније (нарочито „увек онлајн“ могућности), чине их веома примамљивим и зато се могу сматрати модерним облицима протеза у социјалним интеракцијама. Мобилне социјалне мреже⁴ (mobile social networking MSN) како их у новије време називају⁵ нуде се у, унапред припремљеним, веома примамљивим пакетима мобилних оператера уз врло честу јефтину понуду мобилних уређаја (иначе јако скупих, смарт (паметних) телефона) и пратећу доступност Интернета. Свеprisутна корисност оваквих уређаја, као и лако шеровање (дељење са другим корисницима) тренутних (путем ГПС технологија уграђених date уређаје) локација, информација, али и искустава о догађајима (могућност лајв видео стриминга у реалном времену), те могућност да, само једним кликом, остварите конекцију на Интернет чини их апсолутно примамљивим и незаменљивим у савременом окружењу. Значајно је поменути да је у питању само основна понуда оператера мобилне телефоније, ове описане могућности се могу унапредити и створити нове могућности за примену на овим телефонима куповином додатних услуга и програма, што наравно чини овакве уређаја још примамљивијим. Предикција је да до 2012.год. број корисника мобилних социјалних мрежа може достићи бројку од 770 милиона.

Према статистикама више од 100 милиона активних корисника, управо у тренутку док се ово пише, приступа Фејсбуку, путем мобилних апарата, а скоро сви мобилни корисници су за више од 50% активнији од оних, који не приступају путем мобилних апарата⁶. Постоји више од 200 мобилних оператора који промовишу једну од социјалних мрежа (у овом случају фејсбук) тренутно у више од 60 земаља у свету преко неке од својих понуда⁷.

Овако описани уређаји, јасно је, носе са собом велике опасности, од могућности да се приватни подаци пренесу неком другом злонамерном лицу и буду злоупотребљени на неслућене начине до простог злоупотребљавања пружених услуга (крађе услуга – импулса, квантификованог права на бесплатно коришћење Интернета и преко истог количински). Опасност долази и из недовољне обучености лица за коришћење њихових могућности, али већ и прост недостатак пажње корисника, може довести до веома високих трошкова на оваквом уређају. Недовољна пажња у коришћењу апликација социјалних мрежа путем мобилних телефона па, понекада, и

⁴ Прве генерације социјалних мрежа на мобилним мрежама јавиле су се 1999.год.

⁵ http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport доступан 20.02.2010.год дефинишу се као облици средстава комуникације који представљају комбинацију аудио и уређаје за пренос података путем мрежа укључујући и мобилну телефонију (целуларне уређаје), као и приватну и јавну ИП инфраструктуру. Под овим се подразумева и свеукупност елемената који неопходних за омогућавање („постовање и аплодовање“) и конзумирање (гледање, слушање или осећање) социјалних медија кроз мобилне мреже. Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), Mobile social networking, July- September 2008 – доступан на http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (последњи пут приступљени 20.02. 2010)

⁶ <http://www.facebook.com/press/info.php?statistics> доступан 16.02.2010.год

⁷ <http://www.facebook.com/press/info.php?statistics> доступан 16.02.2010.год

намерно недозвољено понашање може изазвати веома тешке последице по друге али и по самог корисника. Претходно описано може имплицирати и кривичну одговорност, нарочито у светлу додатног протокола уз Конвенцију о високотехнолошком криминалу⁸ зато треба потенцирати и на могућој одговорности корисника оваквих уређаја⁹. Па чак и уколико би 99,9% Интернет корисника који се налазе у овом тренутку на Интернету деловало из најбољих намера и потпуно легално, опет би остало 747.000 оних који би могли бити потенцијални извршиоци кривичних дела¹⁰.

Посебна проблематика долази у виду постојања веома квалитетних дигиталних доказа на Интернету о активностима корисника. Наиме, све што се на Интернету објави, уради или пропусти да се уради оставља свој траг, који се касније може употребити. Документовање и евидентирање вршења различитих активности на Интернету је веома лако, уз адекватне софтверске пакете и приступ серверима, свака радња предузета на Интернету оставља свој траг преко ИП адресе – локација и тачка приступа корисника. Поред ове информације, за један секунд, се може добити веома велики број информација о кориснику, и то на пример податак о томе: који је Интернет провајдер пружио услугу, приближна локација коришћења Интернета, па чак и тип и верзија Интернет претраживача корисника. Могуће је утврдити и прецизан временски ток радњи корисника. У скорије време рапидним развојем технологија телефонски апарати су постали средства која су веома опасна по своје кориснике због неслућених могућности које дају неким несавесним и малициозним лицима. Неки веб сајтови чак представљају конзоле за праћење и шпијунирање мобиних телефонских апарата. Након плаћања до 20\$ месечно могуће је остварити потпун приступ метама, које користе уређаје у питању. Од претплатника се тражи ИМЕИ¹¹ број телефона мете и број телефона претплатника. Након посете страници на којој се региструјете добијате програм који мора бити инициран на телефонском апарату мете. По активирању претплатник ће имати приступ следећим услугама¹²:

ГСМ локализацијама преко СМС (оне су нешто мање прецизније него ГПС, али опет дају оквирну позицију мете)

⁸ Текст Конвенције (на енглеском језику) доступан је на Интернет адреси: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, ЕТС 185. Последњи пут приступљено 21.01.2010. Уз ову конвенцију потписан је и додатни протокол ЕТС 189.

⁹ Најразличитије последице могу наступити у вези са последицама одавања личних података или уопште података на социјалним мрежама па тако имамо: у Великој Британији наставницу која се преко ФБ жалила на своје ђаке и која је као последицу објављивања истог на социјалној мрежи суспендована са посла (друга колегиница са којом је ова размењивала поруке о разреду на који се односи увреда - „лоши“ је кажњена за лакшу повреду радне обавезе) доступно на MailOnline, Teacher is suspended for jibe on Facebook about her class, <http://www.dailymail.co.uk/news/article-1202210/Teacher-suspended-jibe-Facebook-class.html> (последњи пут приступљено 20.02. 2010). Други пример је откриће лажног идентитета у виду једног од професора на ФБ, са којим су колеге и студенти размењивали приватне поруке и четовали делећи на тај начин приватне информације са лицем које се лажно представило, без за сада адекватно утврђеног мотива http://www.lastampa.it/web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5580&ID_sezione=38&sezione=News (последњи пут приступљено 20.02. 2010).

¹⁰ http://www.search.coe.int/tehis/search/redir.html?query=cybercrime&pr=Internet_D&prox=page&rorder=500&rprox=750&rdfreq=500&rwfreq=500&rlead=500&rdepth=250&sufs=1&order=r&mode=&opts=&cq=&sr=&u=http%3A/www.coe.int/t/DC/Files/Source/FS_cybercrime_en.doc

¹¹ Једна врста серијског броја телефонског апарата путем којег се он идентификује свакој мобилној мрежи, поред њега постоји и ИМСИ број, који је такође идентификујући.

¹² Доступан на сајту www.coe.int/cybercrime, 20.02.2010.god. Cybercrime current trends and threats, стр.48.

СМС и ММС копије сваке послате поруке (уколико би ово могли подвести под наше норме дефинитивно представља нарушавање неповредивости тајне писама¹³ па се поставља и питање кривичне одговорности у оваквим случајевима¹⁴)

Снимач говора који може снимати било које разговоре са тог апарата али и разговоре када телефон није активан у телефонском разговору (а да не помињемо могућност постављања питања кривичне одговорности и овде¹⁵)

Пресретање које омогућава слушање разговора у реалном времену са тог апарата (за овај случај важи претходна примедба)

Копију адресара и бројева телефона мете.

Посебан проблем представља надлежност наших правосудних органа у случајевима када су сервери и сајтови који ово омогућавају на територији друге државе, а још специфичнији уколико је у питању држава која није потписала Конвенцију о високотехнолошком (кибер) криминалу¹⁶ (на пример Андора, Турска, Монако, Русија (која је децидно 2009 одбила да се придружи потписницама) и Сан Марино). Но, доказивање извршења кривичних дела није једина тема овог рада, зато се морамо позабавити и показатељима чинилаца који могу помоћи превенцији извршења кривичних дела.

Превенција

Могу се, на крају, усвојити препоруке за кориснике социјалних мрежа за умањење ризика по приватност. Шест начина за постизање безбедности на социјалним мрежама су:

Не прихватајте искачуће прозоре или захтеве за програмима, осим уколико нисте опремљени веб скенером (програмом за скенирање оваквих искачућих програма).

Не предајте или не објављујте (постујте) своје личне податке

Мењајте шифру најмање једном месечно.

¹³ Тајност писама и других средстава општења прописана је Уставом Републике Србије (“Службени Гласник РС”, бр. 83/06,) у члану 41. Тајност писама и других средстава комуницирања је неповредива. Одступања су дозвољена само на одређено време и на основу одлуке суда, ако су неопходна ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом.

¹⁴ Чл. 142. КЗ РС (“Службени Гласник РС”, бр. 85/05, 107/05, 72/09, 111/09) Повреда тајности писма и других пошиљки. (1) Ко неовлашћено отвори туђе писмо, телеграм или какво друго затворено писмено или пошиљку или на други начин повреди њихову тајност или ко неовлашћено задржи, прикрије, уништи или другом преда туђе писмо, телеграм или другу пошиљку или ко повреди тајност електронске поште или другог средства за телекомуникацију, казниће се новчаном казном или затвором до две године. (2) Казном из става 1. овог члана казниће се и ко саопшти другом садржину коју је сазнао повредом тајности туђег писма, телеграма или каквог другог затвореног писмена или пошиљке или се том садржином послужи. (3) Ако дело из ст. 1. и 2. овог члана учини службено лице у вршењу службе, казниће се затвором од шест месеци до три године.

¹⁵ Неовлашћено прислушкивање и снимање Члан 143. КЗ РС:

(1) Ко посебним уређајима неовлашћено прислушкује или снима разговор, изјаву или какво саопштење који му нису намењени, казниће се новчаном казном или затвором од три месеца до три године. (2) Казном из става 1. овог члана казниће се и ко омогући непозваном лицу да се упозна са разговором, изјавом или саопштењем који су неовлашћено прислушкивани, односно тонски снимани. (3) Ако је дело из ст. 1. и 2. овог члана учинило службено лице у вршењу службе, казниће се затвором од шест месеци до пет година.

¹⁶ ЕТС 185. Ратификована од Србије 2009.год. Службени гласник РС 19/09; Србија је истовремено ратификовала и Додатни протокол уз Конвенцију.

Не дозвољавајте другима да приступају социјалним мрежама преко вашег уређаја

Немојте аутоматски памтити ваше шифре и најмање једном недељно бришите историју ваших Интернет претраживача.

Не прихватајте и немојте захтевати пријатељство од лица која не познајете.

Неки сматрају да је прва линија фронта против злоупотребе социјалних мрежа и својеврстан вид превенције подизање (повећање) јавне свести о ризицима којима су корисници Интернета и мобилних социјалних мрежа изложени.

Према истраживањима Софос групе¹⁷ у 2009.год. у априлу је пријављено 33,4% спама док је у децембру повећан број на 57%; фишинг (пецање) напади су са 21% у априлу порасли на 30% у децембру. Нарочито је опасан податак да је остварен скок пријаве злограма са 21,2% у априлу на 36% у децембру и још расте. Када посматрамо социјалне мреже и њихов однос према злоћудним програмима, о којима је претходно било речи, у вези истог периода видећемо следеће. Мајспејс (MySpace) наводи у априлу као једну од највећих опасности злоћудне програме у процентима 9,3%, док у децембру овај проблем достиже ниво од 14%. Твитер (Twitter) даје следеће податке за април 6,9% а у децембру 10%, Фејсбук (Facebook) 8,3% у априлу 11%, Линкедин (LinkedIn) 6,5% за април 6,5% а у децембру 8%.

Према скоријој анкети коју је спровео АВГ и Савет ЦМО мање од 1/3 корисника социјалних мрежа користе мере заштите онлајн¹⁸. 47% корисника мобилних социјалних мрежа је забринуто за рачунарске прекиде или ометања личних интеракција са пријатељима на социјалним мрежама¹⁹. 21% корисника (мобилних) социјалних мрежа прихвата захтеве за контактима који долазе од чланова који им нису познати, више од половине корисника пружају могућност својим цимерима да остваре приступ социјалним мрежама на својим уређајима, 26% њих шерују (деле) датотеке у оквиру социјалних мрежа²⁰. 64% корисника социјалних мрежа веома ретко или уопште не мења сопствене шифре на корисничким налозима на социјалним мрежама. 57% не прилагођавају актуелним условима карактеристике приватности својих налога на социјалним мрежама. Близу 20% корисника социјалних мрежа претрпело је или на неки начин дошло у контакт са облицима крађе идентитета, а 47% их је било или постајало жртвама злоћудних програма и 55% њих је видело фишинг нападе.

МСН се могу поделити²¹ у две групе „на столу“ и „са стола“. Прве су оне које су резултат партнерстава мобилних оператера или вајерлес телефонских мрежа и социјалних мрежа. Друга група се односи на оне који не остварују приступ социјалним мрежама кроз пакете оператера, већ нуде коришћење Интернета преко својих пакета а што се наплаћује кроз ковантификацију потрошених (пренетих) количина информација (што је скупља верзија); дакле нема отворених партнерства са социјалним мрежама. Многе социјалне мреже нуде своје услуге специјализоване и само за телефонске апарате (на тај начин дају сиромашније верзије Интернет страница како би свима омогућили приступ мрежи па чак и „старијим“ генерацијама телефонских апарата).

¹⁷ <http://www.sophos.com/> доступан 20.02.2010.год.

¹⁸ http://www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf доступан 20.02.2010.год.

¹⁹ http://www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf доступан 20.02.2010.год.

²⁰ http://www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf доступан 20.02.2010.год.

²¹ Ениса прави ову поделу што и условљава примењену терминологију

Илустрација могућих злоупотреба СНС може се видети у резултатима истраживања Sophos групе²² у којем је једна група истраживача у намери да прикаже недостатке социјалних мрежа креирала фиктивни лик гуме паткице у једном или гуме жабице, у другом истраживању, и пријавила се као пријатељ на социјалној мрежи одређеној групи људи. У овом истраживању дошло се до следећих резултата²³: 46% корисника фејсбука је прихватило захтев за пријатељство од потпуних странаца. 89% корисника двадесетогодишњака је открило своје датуме рођења без поговора. Скоро 100% корисника је разменило своје адресе електронске поште са потпуним странцима без имало сумње у добре намере истих. Између 30 и 40% корисника је разменило и податке о својим пријатељима, контактима и породици.

Софосова анкета открила је и да послодавци (што се може схватити и као специфичан вид превенције) ограничавају употребу Интернета од стране својих запослених у циљу приступа СНС. Тако је 50% запослених на контролисаној популацији спречено од стране послодаваца да путем комуникационих средстава остваре конекцију на ФБ не само због потреба заштите приватности (како физичких лица, тако и правних) већ и због оправданог страха од пада продуктивности²⁴. Послодавци су такође забринути и да запослени могу писати на ФБ или објављивати материјале, фотографије, видео записе којима се може нарушити пословни углед ових фирми. Наравно, све ово може бити и резултат неке врсте напада на социјалне мреже или кориснике СНС који су запослени код дотичног послодавца.

Методe и трендови експлоатације

Експлоатација и уновчавање социјалних мрежа подразумевају следеће економске варијабле²⁵ (и узимају следеће облике):

Адвертајзинг (оглашавање и маркетинг, засновано на корисниковим потребама и главним изворима прихода)

²² <http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/> Овај истраживачки подухват двојице ентузијаста Софоса представља наставак или се чак може рећи продужетак претходног пројекта у Великој Британији (у питању је само огранак исте фирме софоса само у ВБ) када је главну улогу одиграла гуме жабица. Наиме такозвани пројекат Фејсбук сонде обухвата креирање фиктивног лика неке умиљате дечије играчке која је потпуно безазлена (у том случају гуме зелене жабице Freddie Staur 1980), како не би изазвала сумњу корисника и понудити пријатељство на социјалној мрежи са истом што је врло умиљато али открива недостатке овакве активности. Овај продужетак је обухватио креирање фиктивних женских ликова (два Dinette Stonily педесет и нешто година старости а која је добила лик мачке која се игра и Daisy Feletin рођену 1988.год. са ликом гуме паткице) и ограничио се територијално на Аустралију, који су се појавили на нету и тражили пријатељство од по сто људи из њихове старосне групе. Након првих реакција постигао се исти резултат као у случају жабице 87 лица је прихватило пријатељство, али овог пута се отишло и даље петоро додатних људи се пријавило ниоткуда желећи пријатељство са једном од поменутих. Веома су интересантни резултати размене података „пријатеља“ након постајања пријатељем па тако у групи од 20 година и нешто старости сви (100%) су разменили или учинили доступним персоналне адресе електронске поште док су у старијој групи њих 87% учинили исто. Са друге стране телефонски број је одало 23% старијих и 7% млађих, млађи су податке о својим члановима породице и пријатељима одали у 46% а старији у 31% и 89% млађих пун датум рођења а 57% старијих.

²³ <http://www.sophos.com/security/topic/facebook.html> доступан 21.02.2010.год,

²⁴ <http://www.sophos.com/security/topic/facebook.html>

²⁵ http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en доступно 20.02.2010.год.

Премијум (уколико желе да добију више од обичних и основних услуга корисници морају да се пријаве за такве услуге и за то плаћају одређене месечне накнаде)

Донације (корисници дају донације за одржавање платформе)

Плаћање за коришћење (корисници морају платити како би користили или приступили појединим софистициранијим алаткама).

Процена је да ће у 2011.год. број корисника МСН порасти на 554 милиона која је извршена у спекулацији са податком да је пораст корисника мобилних телефонских мрежа у 2008.год. био у висини од 13,3%, са растућим трендом у 2012.год. вероватна бројка је 803 милиона, према пројектованом тренду раста броја мобилних претплатника за 2012.год. У Европи та бројка би требала достићи 134 милиона што би означавало да је сваки од пет мобилних апарата у Европи био, путем истог, и корисник социјалних мрежа²⁶. Све описано са собом носи и друге проблеме, јер више није једино питање шта корисник ради, већ и где је (лоциран обзиром да се најновији генерације телефона користе и за одређивање егзактне локације ГПС –ом).

Неопходно је напоменути да, генерално, социјалне мреже јесу изложене вишем ризику везаном за откривање корисникове приватности, његовог личног и професионалног живота. Ово је више случај са првом врстом мрежа коју смо приказали горе него са другом (тзв. професионалних социјалних мрежа) јер се на њима објављују информације и подаци који нису уско стручно везани за професију већ много приватније (нпр. оне које се тичу укуса, идеологију и искуства) а тиме и много лакше за злоупотребу. У погледу приватности МСН и СМ могу се одредити три правца напада (или нападача) у питању су:

Трећа лица, (која податке - корисничко име и лозинку, лица могу прибавити преваром – фишингом, или крађом мобилног телефона – ређе налажењем изгубљеног. Овакав приступ трећа лица могу остварити и без нарушавања било ког техничког или безбедносног правила у оним случајевима када корисник није правилно подесио правила безбедности профила.)

Остали корисници, (неопходно је са лицима која прихватате као пријатеље договорити да се многе приватне ствари не постују на социјалној мрежи уколико оне могу да открију приватне или да доведу до откривања приватних информација. Такође је неопходно, уколико дозволите неком другом да користи ваш профил како би приступио социјалној мрежи, да имате контролу над његовим активностима и степеном откривања приватних података)

Лица која раде на одржавању платформи или лица која раде апликације (корисници имају право да подесе у правилима о приватности круг лица која имају приступ подацима које они остављају на мрежи. Али понекада ова лица имају приступ многим подацима који су значајно приватни иако нису одговарајући правилима које је

²⁶ Nick Lane, Nicky Walton-Flynn, Freda Benlamlih (Informa Telecoms & Media), Mobile social networking – the paper was sponsored by Buongiorno and the research has been carried out by Informa Telecoms & Media, July-September 2008 – доступан на http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf (последњи пут приступљено 23.02.2010), The daily bit, Un fenomeno chiamato mobile social networking, September 2008, доступан на <http://www.thedailybit.net/index.php?method=section&action=zoom&id=2489> (21.02.2010.год.) и Lastampa.it, In Europa il social network piace sul cellulare, August 2008, available at http://www.lastampa.it/web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5054&ID_sezione=38&sezione=News (последњи пут приступано 22.02.2010.).

корисник поставио. У питању су програмске алатке или апликације које под изговором (или реалном) потребе за апликацију прикупљају приватне податке као на приемир ИП адресу, тип Интернет претраживача и сл.).

Што се методологије тиче, креденцијали (подаци о корисничком имену и шифри за приступ) за приступ МСН (или СМ) могу се прибавити на различите начине. Дакле, крађа идентитета се може остварити крађом креденцијала трајно, или привремено, кроз напад типа човек у средини²⁷ или крађом мобилног уређаја. Оног тренутка када нападач преузме контролу над рачуном корисника и почне постављати коментаре и приказивати и исказивати осећања као легитимни корисник, тада већ има могућност да за стално преузме тај налог и преко њега може почети да шири злоћудне програме (злограме) – путем социјалног инжењеринга²⁸. Овакав акт може имати веома значајна утицај на приватни и пословни живот лица чији идентитет на социјалној мрежи је на овај начин угрожен. У току 2009.год. у Шпанији је био пријављен већи број случајева крађа идентитета у Шпанији чије жртве су биле познате личности, (један политичар и један писац)²⁹. Њихови лажни профили су циркулисали по социјалној мрежи, са лажним мишљењима и коментарима у њихово име, наносећи им штету угледу и приватности.

Социјалне мреже могу остварити веома велики утицај на углед и приватност фирме. МСН услуге могу допринети свесном или несвесном цурењу поверљивих података из фирми, овакво цурење може проузроковати велике штете (чак и ненадокнадиве) привредним друштвима (поред физичких лица). Корисници могу доћи у посед података и фотографија које су неовлашћено објављене на неком од медија путем социјалних мрежа а чиме се шире некада и лажне вести и клевете о датој фирми³⁰. Тиме се могу остварити интенциона ширења лажних вести и информација у циљу подривања пословног угледа и бонитета фирме.

Овде није крај могућностима злоупотреба МСН. Обзиром да се новије генерације телефона у потпуним интегрисањима многих функција јављају са ГПС

²⁷ МИТМА Облик напада у којем извршилац користи свој рачунар као медиј за комуникацију са жељеним адресатом жртве уз остваривање потпуног надзора над свом комуникацијом жртве.

²⁸ Иначе социјалне мреже су веома плодно тле за ширење злограма, иначе иако не постоји ни један случај у којем је дошло до ширења злограма на МСН ове мреже имају специфичну карактеристику по којој могу посебно креиране облике злограма слати директно на мобилне апарате, уз то користећи и Wi-Fi и Bluetooth технологије за даље ширење. Они могу чак красти информације похрањене у МСН, или чак да инфилтрирају мобилни телефон како би прибавили похрањене информације у њему, посебна врста чак може користити проксије како би ширили инфекцију злограма контактирањем из мобилне социјалне мреже. Методологија ширења злограма је уобичајено следећа: обично је у питању сајт који је инфилтриран оваквим злограмама, и корисници, преко својих контаката, који су такође или инфилтрирани или жртве социјалног инжењеринга, кликну на линк који им је прослеђен – долазећи тако до инфилтрираног сајта, када се злограм даље шири (овај поступак се може одвијати и преко и-мејла – електронске поште). За више погледати http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-crosshairs-832?source=IFWNLE_nlt_sec_2009-08-17 доступан 21.02.2010.год.

²⁹ http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport стр.15. доступан 20.02.2010

³⁰ 2008.год. Вирџин Атлантик (Virgin Atlantic airlines) је отпустио својих 13 запослених због постављања некултурних коментара о својој компанији на ФБ. Бритиш ерлајнс је исте године спровео истрагу против својих запослених због постовања порука о путницима којима их карактеришу као „смрдљиве“. Сличне примере имамо и у Италији и Француској. Доступно на страници. http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport стр.23-4. доступан 20.02.2010

уређајима (мада чак ни ови уређаји нису неопходни за одређивање локације – то се може и преко мобилне мреже), могуће је преко нових апликација (френд фајндер, френд трекер и сл.) које се нуде корисницима МСН. Ове апликације функционишу на следећи начин: како би у сваком тренутку био упознат са кретањем својих пријатеља и они са корисниковим неопходно је да да пристанак на употребу неопходних карактеристика уређаја. Злоупотребе оваквих апликација су веома д широког дијапазона: од могућности уцене, отмице, физичког напада (када је најосетљивији) праћења и ухођења, а да не говоримо о могућностима злоупотребе рачуна о којима је већ разматрано на плану урушавања угледа и дисеминације приватних података.

Како се онда супроставити? Први корак мора ићи у правцу едукације корисника и свих учесника у дистрибуцији материјала и информација СНС и МСН, такође и оператери или администратори социјалних мрежа (па чак и они велики као ФБ или МС) морају прилагодити своја правила заштити приватности корисника и морају сносити одговорност за такву заштиту. Видећемо да је ЕУ већ повукла одређене кораке у том правцу. Наравно и државне институције морају учествовати на различитим нивоима у едукацији корисника али и својих припадника како би се адекватно одговорило изазовима. Поред помињаног значајно је изнети и класичне репресивне облике супростављања оваквим новим појавама. Мере које полиција може предузети у правцу сузбијања и спречавања ове појаве су споре али евентуално ефикасне, поред класичних овлашћења предвиђених Законом о кривичном поступку (ЗКП – ом)³¹ постоје и специјалне истражне методе предвиђене у чл.504.е за кривична дела предвиђена у чл.504а. а такође и мера Аутоматско рачунарско претраживање личних и других са њима повезаних података предвиђена је чл. 504љ. У овом тренутку нисмо у могућности да прикажемо прецизан домет оваквих норми, али у поређењу са одредбама Конвенције о ВТК, видимо да је наше процесно законодавство у великом заостатку у односу на просек Савета Европе, али и то ће се евентуално побољшати, обзиром да се ради на изменама ЗКП у том правцу³².

Европски пресек

Од око 283 милиона корисника у Европи, 211 милиона њих старијих од 15 година (уколико су се придржавали правила социјалних мрежа а што је дискутабилно) који приступају Интернету преко рачунара, посетили су СНС. Од описаних најмногољудније заступљена (у односу на укупну популацију) је Велика Британија – са 80% укупне популације присутне на Интернету (29 милиона корисника)³³. Најмање заступљена је Аустрија са 212000 или 49.7% укупне популације на Интернету. Међу социјалним мрежама у Европи водећа је Фејсбук, једно истраживање које је обухватило и анализу развоја социјалних мрежа указало је да је фејсбук остварила напредак у износу од 443%, за период децембра 2007. – децембар 2008.год а друго³⁴

³¹ ("Сл. лист СРЈ", бр. 70/2001 и 68/2002 и "Сл. гласник РС", бр. 58/2004, 85/2005, 115/2005, 85/2005, 49/2007, 20/2009 и 72/2009)

³² За више о дOMETИМА и стању у овој области погледати Комлен Николић, Л. Гвозденовић, Р. Радуловић, С. Милосављевић, А. Јерковић, Р. Живковић, В. Живановић, С. Рељановић, М. Алексић, И. Сузбијање вискотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца, АЕЦИД 2010, Београд.

³³ http://www.mediametrix.com/Press_Events/Press_Releases/2009/2/Social_Networking_France доступан 20.02.2010.год,

³⁴ http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport str.14

указује да су само три земље у Европи те које немају ФБ као водећу на листама социјалних мрежа (то су Немачка – где је 4, Португал – 3, и Русија – 7). О расту употребе мобилних телефона у примени на социјалним мрежама (као МСН) говори податак о повећању приступа социјалним мрежама путем мобилних апарата од скоро 200% од последњег квартала 2008. до последњег квартала 2009.год.³⁵. Као првих 5 активности на социјалним мрежама на Пан европском нивоу одређују се: слање порука или поште (56%), читање истих (50%), гледање фотографија (43%), постављање фотографија (31%), додавање пријатеља (24%), а остале активности су: пријем текстуалних упозорења (23%), гледање профила (15%), креирање или измена и ажурирање профила (13%), уношење видео записа (10%), учествовање у „собама за разговор“ (eng chat rooms), постовање на блоговима (7%)³⁶.

Регулисање материје у ЕУ

У ЕУ је заштита права на приватност регулисано директивама: ДПД директивом (Directive 95/46/EC) о заштити појединаца у погледу обраде личних података и премештања тих података, ОЈ L 281, 23.11.1995.

Овом директивом се дефинишу лични подаци као све информације које се односе на субјекат обраде тих података (као особа коју је могуће идентификовати или која чија су обележја већ позната, код нас је то физичко лице) а који указују на физичке, економске, културне или менталне факторе. Свака активност уперена на личне податке, као што је прикупљање, похрањивање или откривање представља обраду личних података, а чија сврха и средства су одређена од стране лица које је у поседу ових података (има фактичку власт над њима – Руковалац података) датих података (а које по закону може бити физичко или правно лице, јавни ентитет, агенција или било које друго тело)³⁷. Заштита личних података мора бити³⁸:

Правично и легални процесуирана

Подаци морају бити прикупљани за тачно одређене, легитимне сврхе и морају се користити само за те сврхе

Адекватно и релевантно везана за сврху у коју су подаци обрађивани

Подаци (који су одређени као лични) морају бити прецизни и ажурирани

Дати подаци морају бити чувани за онолико времена које је неопходно за остваривање сврхе њиховог обрађивања

Лични подаци могу бити обрађивани уколико³⁹:

Је субјекат података адекватно претходно обавештен о овој обради података и уколико је субјекат дао своју сагласност недвосмислено за прикупљање и даљу употребу тих података

Обраду података је могуће спровести само уколико је тако уговором одређено а у којем је странка субјекат података или уколико приступио уговору са субјектом података

³⁵ <http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/> доступан 20.02.2010.

³⁶ http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport стр.15.

³⁷ Чл. 2(а), (b) и (d), ДПД Директиве.

³⁸ Чл.6.

³⁹ Чл.7.

Правна обавеза захтева обраду података

Обрада података јесте неопходна у сврху очувања есенцијалних интереса субјекта података

Уколико је обрада података неопходна за извођење задатака од јавног интереса или је предузимана од стране неког органа јавне власти

Контролор података има законит интерес у обрађивању ових личних података; овај интерес мора бити адекватно избалансиран са правом на заштиту приватности субјекта обраде података.

Субјекат обраде података има право да:

Буде обавештен о било каквој обради његових података,

Приступа његовим подацима

Приговори употреби његових података на основу жалбе и законских основа

За описане обавезе постоји и прописан изузетак (за случај домаћинства) чл.3.(2) директиве. Дакле неће се примењивати обавезе везане за обраду личних података у две специфичне ситуационе околности:

- Сваком случају обраде која излази изван оквира јавне безбедности, одбране, кривично правне области које не спадају у област ингеренције ЕУ, а представљау национални прерогатив.
- У случају чисто личних или активности домаћинства

У појашњењу ове последње одредбе у рециталу 12 ДПД каже се да је када је у случају обраде података физичког лица спровођене од стране контролора физичког лица у извођењу активности које су искључиво личне (приватне) као на пример кореспонденција или похрањивање података о адресама и бројевима телефона контаката, мора бити искључена из примене принципа протекције ове директиве⁴⁰.

Директива је чл.29. успоставила Радну групу за заштиту као независну организацију (тело). Она се састоји од комесара за заштиту података сваке државе чланице, представника Комисије и представника тела и институција ЕУ. Задаци су:

Подршка јединственој примени националних мера усвојених на основу директиве

Давање мишљења о нивоу заштите Заједнице и трећих држава Европској комисији

Светодавна за Комисију ЕУ у погледу предложених амандмана на директиву ДПД, у односу на све додатне и специфичне мере за заштиту слобода и права грађана у вези обраде података

Давање мишљења на кодексе понашања донете на нивоу ЕУ

Мишљење Радне групе за заштиту бр. 5/2009

Сврха овог мишљења радне групе датог у јуну 2009.год. у вези мобилних социјалних мрежа је била да се провајдерима СМС пруже смернице у погледу

⁴⁰ Суд правде Европске заједнице (CJ) је примену принципа искључења домаћинства у случају Линдквист (Court of Justice, Case C-101/01, Criminal proceedings against Bodil Lindqvist, OJ C 7, 10.1.2004.) Госпођа Линдквист, радница локалне Шведске парохије је, без сагласности парохијана, а у религијске сврхе објавила личне податке и телефоне припадника парохије. Тужена је због нарушавања правила Закона о личним подацима. Суд је пронашао да примена изузетка домаћинства овде није примењива, обзиром да се односи само на активности које су предузете у оквиру приватног и породичног живота појединаца, а што очигледно није случај са обрађивањем података у облику објављивања на Интернет страници чиме су ови подаци постали доступни неодређеном броју лица.

техничких и организационих мера које морају предузети како би се одговорило стандардима легислативе ЕУ везане за заштиту података. Посебно ово мишљење је садржи смернице за провајдере у вези⁴¹:

Обавезе да упозоре кориснике СМС на ризике у вези приватности за њих и трећа лица у погледу учитавања (аплодовања) информација на СНС

Упозоре кориснике на могућност нарушавања приватности других лица у погледу учитавања података о њима

Саветују кориснике у погледу чињенице да је за учитавање фотографија других особа на овакве СНС неопходан њихов пристапак

Да понуде ергономски интерфејс са подразумеваним подешавањима која омогућавају кориснику да слободно и уз максималну личну контролу остваре надзор над сваким приступом садржини њиховог профила који је изван њиховог круга контаката у циљу умањивања ризика од незаконите обраде података од стране трећих лица.

Обезбеде линк на сајту за притужбе и жалбе адекватном телу за заштиту ових података

Обришу личне податке пружене од стране корисника приликом регистрације на СНС што је пре могуће или када корисник пожели да обрише налог; шта више уколико корисник пожели да за одређени временски период не користи овај налог, обавезу да се такав стави ад акта – као неактиван.

Посебан случај односи се и на примену ДПД директиве на Не ЕУ државе, нарочито у погледу технологија колачића⁴² у Интернет претраживачима, а што је примењиво на скоро све глобалне СНС. Радна група је дошла до закључка да се ДПД примењује у оваквим случајевима. Ову материју у ЕУ регулишу и:

Директива (Directive 2002/58/EC) која се односи на обраду личних података и и заштиту приватности у сектору електронских комуникација (e-privacy directive) OJ L 201, 31.7.2002. Европски Савет ЕУ је 26.10.2009, усвојио директиву којом се између осталог мењају и одредбе ове директиве (e-privacy directive). Оне се односе на обавезе Интернет провајдера да евидентирају и обавештавају о цурењу података и упадима у базе података компетентно национално тело.

Препорука Комисије о примени принципа приватности и заштите података код апликација које су подржане РФИД-ом, Радио фреквенцијском идентификацијом., OJ L 122, 16.5.2009.

Србија

У нашем законодавству видећемо да је веома сиромашно остварена заштита од могућих злоупотреба на МСН. Закон о заштити података о личности⁴³ у члану 3. Одређујући значење израза у овом закону наводи да:

Податак о личности 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

⁴¹ http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport стр.23-4. [доступан 20.02.2010](#) стр.31.

⁴² Којим се могу обрађивати подаци о локацији корисника и афинитетима а што у крајњој консеквенци може донети предност на тржишту одређеним компанијама и појединцима.

⁴³ Службени гласник РС бр. 97/08

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 (у даљем тексту: податак);

Физичко лице је 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 (у даљем тексту: лице);

Обрада података је 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 (у даљем тексту: обрада);

Подаци на које се закон не примењује одређују се у члану 5. (осим ако очигледно претежу супротни интереси лица):

1) података који су доступни свакоме и објављени у јавним гласилима и публикацијама или приступачни у архивама, музејима и другим сличним организацијама;

2) података који се обрађују за породичне и друге личне потребе и нису доступни трећим лицима;

3) података који се о члановима политичких странака, удружења, синдиката, као и других облика удруживања обрађују од стране тих организација, под условом да члан да писмену изјаву да одређене одредбе овог закона не важе за обраду података о њему за одређено време, али не дужи од времена трајања његовог чланства;

4) података које је лице, способно да се само стара о својим интересима, објавило о себи⁴⁴.

Закон у члану 8. Прописује када није дозвољена обрада. То су случајеви када:

1) физичко лице није дало пристанак за обраду, односно ако се обрада врши без законског овлашћења;

2) се врши у сврху различиту од оне за коју је одређена, без обзира да ли се врши на основу пристанка лица или законског овлашћења за обраду без пристанка;

3) сврха обраде није јасно одређена, ако је измењена, недозвољена или већ остварена;

4) је лице на које се подаци односе одређено или одредиво и након што се оствари сврха обраде;

5) је начин обраде недозвољен;

6) је податак који се обрађује непотребан или неподесан за остварење сврхе обраде;

7) су број или врста података који се обрађују несразмерни сврси обраде;

⁴⁴ Члан 6. Говори и о изузецима у случајевима обраде у историјске, статистичке или научноистраживачке сврхе

8) је податак неистинит и непотпун, односно када није заснован на веродостојном извору или је застарео.

Закон прописује и када је могућа обрада са пристанком у члану 10. након што га руковалац претходно обавести у смислу одредбе члана 15. лице може дати пуноважан пристанак за обраду овај пристанак се може опозвати. Такође прописује и случајеве дозвољене обраде без пристанка чл.12. да би се остварили или заштитили животни важни интереси лица или другог лица, а посебно живот, здравље и физички интегритет; у сврху извршења обавеза одређених законом, актом донетим у складу са законом или уговором закљученим између лица и руковаоца, као и ради припреме закључења уговора; у другим случајевима одређеним овим законом или другим прописом донетим у складу са овим законом, ради остварења претежног оправданог интереса лица, руковаоца или корисника. Орган власти по члану 13. обрађује податке без пристанка лица, ако је обрада неопходна ради обављања послова из своје надлежности одређених законом или другим прописом у циљу остваривања интереса националне или јавне безбедности, одбране земље, спречавања, откривања, истраге и гоњења за кривична дела, економских, односно финансијских интереса државе, заштите здравља и морала, заштите права и слобода и другог јавног интереса, а у другим случајевима на основу писменог пристанка лица.

Обавештавање лица на које се подаци односе, односно друго лица о обради од стране Руковаоца регулише се чланом 15.⁴⁵

Посебно се регулишу питања нарочито осетљивих података чланом 16. У питању су подаци који се односе на националну припадност, расу, пол, језик, вероисповест, припадност политичкој странци, синдикално чланство, здравствено стање, примање социјалне помоћи, жртву насиља, осуду за кривично дело и сексуални живот. Они се могу обрађивати само на основу слободно датог пристанка лица, осим када законом није дозвољена обрада ни уз пристанак. Изузетно, подаци који се односе на припадност политичкој странци, здравствено стање и примање социјалне помоћи, могу се обрађивати без пристанка лица, само ако је то законом прописано. Тада обрада мора бити посебно означена и заштићена мерама заштите. Пристанак за обраду нарочито осетљивих података даје се у писменом облику, који садржи ознаку податка који се обрађује, сврху обраде и начин његовог коришћења. Могућ је опозив пристанка на обраду података.

Лице има право да захтева да га руковалац истинито и потпуно обавести о томе:

⁴⁵ Пре прикупљања, упознаје се о:

- 1) свом идентитету, односно имену и адреси или фирми, односно идентитету другог лица које је одговорно за обраду података у складу са законом;
- 2) сврси прикупљања и даље обраде података;
- 3) начину коришћења података;
- 4) идентитету лица или врсти лица која користе податке;
- 5) обавезности и правном основу, односно добровољности давања података и обраде;
- 6) праву да пристанак за обраду опозове, као и правне последице у случају опозива;
- 7) правима која припадају лицу у случају недозвољене обраде;
- 8) другим околностима чије би несаопштавање лицу на које се односе подаци, односно другом лицу било супротно савесном поступању.

Обавеза из става 1. овог члана не постоји када такво упознавање, с обзиром на околности случаја, није могуће или је очигледно непотребно, односно непримерено, а нарочито ако је лице на које се односе подаци, односно друго лице већ упознато са тиме или ако лице на које се подаци односе није доступно.

- 1) да ли руковаоца обрађује податке о њему и коју радњу обраде врши;
- 2) које податке обрађује о њему;
- 3) од кога су прикупљени подаци о њему, односно ко је извор података;
- 4) у које сврхе обрађује податке о њему;
- 5) по ком правном основу обрађује податке о њему;
- 6) у којим збиркама података се налазе подаци о њему;
- 7) ко су корисници података о њему;
- 8) које податке, односно које врсте података о њему користе;
- 9) у које сврхе се користе подаци о њему;
- 10) по ком правном основу користи податке о њему;
- 11) коме се подаци преносе;
- 12) који подаци се преносе;
- 13) у које сврхе се подаци преносе;
- 14) по ком правном основу се подаци преносе;
- 15) у ком временском периоду се подаци обрађују. Лице по чл.20. има право да од руковаоца захтева да му стави на увид (оно обухвата право на преглед, читање и слушање података, као и прављење забележака) податке који се на њега односе. Лице има право да од руковаоца по члану 21. захтева копију податка који се на њега односи. Лице има право да од руковаоца захтева исправку, допуну, ажурирање, брисање података, као и прекид и привремену обуставу обраде. Могуће је и ограничавање ових права оно је регулисано чл 23. Орган који врши надзор над применом овог закона је Повереник за информације од јавног значаја. Резултат примене овог закона и ингеренције повереника као и њихов домаћај познате су јавности⁴⁶. Дакле оквири су релативно квалитетно дати, али многи проблеми опстају. За нас је значајно да се у овим оквирима не може говорити о кривичној одговорности физичких а камо ли правних лица, што је у блиској будућности веома битно.

КЗ регулише ову материју прописујући кривично дело Неовлашћено прикупљање личних података чланом 146. Садржина овог члана је следећа: (1) Ко податке о личности који се прикупљају, обрађују и користе на основу закона неовлашћено прибави, саопшти другом или употреби у сврху за коју нису намењени, казниће се новчаном казном или затвором до једне године.(2) Казном из става 1. овог члана казниће се и ко противно закону прикупља податке о личности грађана или тако прикупљене податке користи. (3) Ако дело из става 1. овог члана учини службено лице у вршењу службе, казниће се затвором до три године. Ова одредница није превише оштра, нарочито ако посматрамо ово кривично дело у светлу његових карактеристика. Наиме дело спада у групу лакших кривичних дела за које се спроводи скраћени поступак и за која је прописана могућност, одлагања кривичног гоњења, као и могућност изрицања кривичних санкција без главног претреса. Дакле овде у ствари и отпада примена специјалних истражних метода и описаних мера из чл.504 е и љ. Самим тим се и поставља питање оправданости њиховог прописивања за оваква дела.

⁴⁶ Повереник може по закону може:

- 1) наредити да се неправилности отклоне у одређеном року;
- 2) привремено забранити обраду која се обавља супротно одредбама овог закона;
- 3) наредити брисање података прикупљених без правног основа.

Повереник је дужан да поднесе прекршајну пријаву због повреда одредаба овог закона.

И у вези појединих могућих злоупотреба у оквиру МСН КЗ прописује и Неовлашћено објављивање и приказивање туђег списка, портрета и снимка чланом 145. (1) Ко објави или прикаже спис, портрет, фотографију, филм или фонограм личног карактера без пристанка лица које је спис саставило или на кога се спис односи, односно без пристанка лица које је приказано на портрету, фотографији или филму или чији је глас снимљен на фонограму или без пристанка другог лица чији се пристанак по закону тражи и тиме осетно задре у лични живот тог лица, казниће се новчаном казном или затвором до две године. (2) Ако дело из става 1. овог члана учини службено лице у вршењу службе, казниће се затвором до три године. Ово дело инкриминише обавезу коју смо видели да имају провајдери по праву ЕУ да обавезно упозоре кориснике СНС када објављују фотографије других лица на социјалној мрежи. Поново се јавља проблем осетног задирања у приватни живот што представља фактичко питање сваког случаја засебно. Иначе све примедбе дате у претходном параграфу за дело из чл. 46. КЗ важе и за овај случај.

Закључак

Након свега наведеног не можемо се отети утиску да смо у овој материји веома рањиви. Не само да би могли да унапредимо законодавство у овом погледу, обзиром да претендујемо на положај државе кандидата за чланство у ЕУ, већ морамо подићи и ниво свести у друштву у погледу ове проблематике. Неки кораци које смо предузели на плану регулације материје у датој области у погледу Интернет провајдера и њихових обавеза кроз сарадњу са државним органима били су неминовни, али и вишеструко корисни. Ипак то су само подзаконски акти, морамо се угледати на веома висок стандард који ЕУ поставља, морамо много потпуније и свеобухватније заћи у материју. Управо то је један од разлога због којих су разматрана легислативна решења ЕУ. Не гајимо илузије да можемо постићи овај ниво и стандарде преко ноћи али наравно да је неопходно да у сваком тренутку имамо узоре и мустре које можемо пратити, а за тако нешто нема бољег од ЕУ. Неопходно је подвући потребу да се обзиром на велику брзину развоја технологија и законодавство, као и одговори државе у глобалу, морају прилагођавати новонасталим околностима. Све говори у правцу усвајања многих одредби и законодавних решења других држава а и то не сме бити некритичко аутоматско преузимање. Поред тога постоји обавеза имплементирања решења из Конвенције о ВТК⁴⁷, но реално, можда нисмо довољно информационо развијени за имплементацију свих решења, али неопходно је поступно и плански реализовати сегменте проблема. Уколико се стратешки добро осмисли овакав подухват се може веома квалитетно (што не значи и брзо) спровести у дело.

⁴⁷ Нарочито у светлу негативног извештаја Савета Европе о одредбама „новог“ ЗКП који до дана данашњег није ступио на снагу.

Литература:

1. Acquisti, A. Gross, R. (2009). Predicting Social Security numbers from public data. Proceedings of the National Academy of Sciences, 106 (27), 10975-10980.
2. Boyd, D. (2008). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. MacArthur Foundation Series on Digital Learning - Youth, Identity, and Digital Media Volume. (pp. 119-142). Cambridge. MIT Press
3. Gilbert, Eric, Karahalios, Karrie, and Sandvig, Christian. (2008). The Network in the Garden: An Empirical Analysis of Social Media in Rural Life. ACM CHI 2008. April. April 5-10, Florence Italy
4. Комлен Николић, Л. Гвозденовић, Р. Радуловић, С. Милосављевић, А. Јерковић, Р. Живковић, В. Живановић, С. Рељановић, М. Алексић, И. (2010) Сузбијање вискотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца, АЕЦИД, Београд
5. Takahashi, T. (2008). Mobile Phones and Social Networking Sites: Digital Natives' Engagement with Media in Everyday Life in Japan. Media, Communication & Humanity. London, England. September 21-23

Интернет извори:

<http://weis09.infosecon.net/files/156/index.html>
http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf
<http://www.facebook.com/press/info.php?statistics>
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
<http://www.dailymail.co.uk/news/article-1202210/Teacher-suspended-jibe-Facebook-class.html>
http://www.mediametrix.com/Press_Events/Press_Releases/2009/2/Social_Networking_France доступан 20.02.2010.год,
<http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/>
http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport
http://www.lastampa.it/web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=5054&ID_sezione=38&sezione=News
http://www.infoworld.com/d/security-central/hackers-put-social-networks-such-twitter-in-crosshairs-832?source=IFWNLE_nlt_sec_2009-08-17
<http://www.sophos.com/>
<http://www.thedailybit.net/index.php?method=section&action=zoom&id=2489>
http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en
http://www.search.coe.int/taxis/search/redir.html?query=cybercrime&pr=Internet_D&prox=page&rorder=500&rprox=750&rdfreq=500&rwfreq=500&rlead=500&rdepth=250&sufs=1&order=r&mode=&opts=&cq=&sr=u=http%3A//www.coe.int/t/DC/Files/Source/FS_cybercrime_en.doc
http://www.avg.com.au/files/media/avg_socialsecurity_2009-08-26_au.pdf
<http://www.sophos.com/security/topic/facebook.html>
http://www.telecoms.com/wp-content/uploads/2009/05/buongiorno_final-fmt_nl-3110-f.pdf

Abstract: In ordinary life the roles of modern means of communication get new dimensions every day. Orwell's 1984. has culminated in today's age, but final outcome is yet to come. In such an environment it is very important to identify good practices and implement an adequate analysis of our own capabilities, needs and therefore adequately accept and adapt the norms, which are making the space to maneuver. The authors are trying to present the dangers overview that social networks are carrying by entering in a complex elaboration the variables of mobile telephone networks and devices. By introducing the concept of mobile social networks, the authors attempt to add analytical approach, through the dangers lurking in the new environment, and by normative analysis. Phenomenological aspect of the social problem of online social networks is shown through analysis of the phenomenon with the expansion to its new content, which it gets by a new technology innovations. Contents normative analysis consists of displaying of the EU platform in the field and attempt comparisons with the current regulations in a given field in Republic of Serbia.

Keywords: social networks, mobile social networks, social networks legislation, internet misuse of personal data, identity theft