Проф. др Весна Балтезаровић*
Факултет за културу и медије
Универзитет „Дон Незбит“
Београд
Др Радослав Балтезаровић

СЛОБОДА НА ИНТЕРНЕТУ И ЊЕНЕ ПОСЛЕДИЦЕ

Сажетак: Интернет је несумњиво један од најпровокативнијих социолошких и психолошких феномена. За интернет се говори да представља слободну мрежу на којој се повезују посрнули комуникатори који се не налазе у реалном свету. Међутим, слободно дружење и сурфовање по онлајн простору не пролази без остављања трагова. Сваки корисник даје податке о себи, некад као услов да би могао да присуствује траженим апликацијама, када свесно на то пристаје, некад размењујући податке са другим учесницима мреже, несвесно да мрежа „све памти“, да подаци остају депоновани чак и у случају када уклоне свој профил. Све чешће смо суочени са крађама података и идентитета од стране криминалних хакерских група. Ова дела углавном пролазе некажњено јер је интернет, као „слободна“ мрежа, често изван законске контроле. Сајбер безбедност је изазов који ће морати регулаторно да се реши што пре. То доводи до дуализма у решавању ове проблемастике. Проблем настаје због могућности да се решавањем питања безбедности с једне стране, наруши заштита приватности на интернету с друге стране.

Кључне речи: ИНТЕРНЕТ, КОМУНИКАТОРИ, СЛОБОДНА МРЕЖА, ПОДАЦИ, ХАКЕРИ, БЕЗБЕДНОСТ.

¹ Контакт: vbaltezarevic@nezbit.edu.rs

Увод

Појава интернета разбила је на комаде комуникациону традицију. Формиран је сурогат свет са атрибутима аутентичне заједнице у коме се разговара, интелектуално надмудрује, тргује и заљубљује. У овом свету се траже пријатељи и играју игре (Rheingold, 1994).

Психолози сматрају да човек, као друштвено биће има сталну потребу за другим људима јер своје индивидуално „ја” најбоље остварује у друштву са другим људима и сталном међусобном комуникацијом (Каличанин & Петровић, 2011: 6) Привлачност интернета потенцирана је могућношћу да се утоли глад за комуникацијом, али и да се пласирају информације и оформе различите дискуссионне групе за размену мишљења, вести, и за извештавање о догађајима који су из било којих разлога тој публици значајни. Интернет тако даје широк избор информационих извора, а то утиче на привлачење и задржавање публике (Балтезаревић & Балтезаревић, 2015: 148).

Интернет је посебно атрактиван због осећаја слободе коју нуди сајбер комуникаторима: буди ко хоћеш, представи се како хоћеш и остани на мрежи колико хоћеш. Нема санкција и нема ограничења. На мрежи те чекају пријатељи!

Да ли је баш тако? Интернет је омогућио људску интеракцију у простору, који није простор, у времену које је заглављено негде између компјутерских програма и сусрете са људима који нису људи већ „позајмљени измишљени ликови”. Интернет јесте умрежавање, али виртуелног друштва и виртуелних пријатеља. Информације које се налазе на порталима су често непроверене, а омогућена је и анонимност учесника која може да буде параван за различита криминогена понашања. Знатан део медијског онлајн простора још увек није обухваћен правном регулативом што доводи до бројних кршења људских права, али и до озбиљних криминалних радњи које остају изван домета закона.

Употреба интернета представља интерактиван процес у коме учествују корисници са особеним обележјима на једној страни и виртуелни простор са својим специфичностима на другој страни. Код онлајн веза импресија о другој особи, преко интернета, се формира на основу оних информација које нам та особа сама даје. Онлајн комуникатор се захваљујући могућности контроле и пласирања информација, које зависе од њега, осећа лагодније и опуштеније *јер он је оно што је рекао да јесте*. Тако драж сурфовања онлајн простором ствара илузију слободе која је без стега и без притисака на располагању људима за разлику од реалног света у коме морају да се повинују правилима социјалне групе и да мисле и раде само оно што група прихвата као модел понашања. Ма како дубока

била заблуда да се по виртуелном граду шетају неки други људи, реални свет и виртуелне заједнице су насељене истим појединцима чији су основни интереси, потребе и мотивације заједнички за оба света. Интернет је једини медиј на коме нема цензуре. Али, на интернету, у виртуелном простору су људи који осећајући слободу, не ретко пређу у комуникациону анархију у одсуству аутоцензуре. У таквим понашањима где се прекорачују сопствене слободе, долази до угрожавања туђих слобода.

Сада се враћамо питању: да ли је интернет слободан медиј? Само залуђени идеалисти могу да дају потврдан одговор. Ако би се повели за тим да интернет препустимо његовим корисницима у потпуности, врло брзо би у виртуелном свету „отпочели глобални виртуелни ратови”. Ако се слобода поистовети са игнорисањем правила која владају у реалном свету, добијамо њену супротност: анархију и кршење туђих права. Интернет често представља „бојно поље за различите интересе, гледишта и идеје” (Samoriski, 2012:14) и уколико желимо слободан интернет треба да се омогући да интернет буде заштићен од свих девијантних понашања.

Интернет је мрежа која се стално мења и измиче дефиницији. Његов значај за људе само ће се увећавати, а имајући у виду брзину његовог развоја, изгледа да немамо још много времена да одлучимо на којим ће се основама и вредностима он базирати (Весић, 2005).

Међутим, никако не смемо да заборавимо да интернет није оаза у којој су посетиоци у потпуности заштићени и безбедни. *Google* покушава да пронађе решење како би стао на пут лажним онлајн идентитетима који се често користе за претње и агресивно понашање. Решавање проблема аватара под псеудонимима и лажним именима је једна од могућности за успостављање безбедности на интернету. С друге стране појачана контрола интернета, због безбедности, сукобљава се са правом на анонимност корисника. Тако се ова два аспекта коришћења интернета крећу у распону од потпуне слободе до потпуне контроле.

1. Сајбер замке

Нови медији са собом доносе многобројне сигурносне проблеме. Због тога је изражена потреба регулације и утврђивања механизма којима ће се осигурати поверљивост, интегритет, и доступност података.

Интернет се најчешће користи за социјалну интеракцију. Међутим, за ту изузетну количину садржаја по правилу не постоји контрола објављивања, па је знатан део садржаја на интернету неверодостојан или пропагандних обележја, случајно или намерно искривљен, док се за приступ богатијим изворима вредних садржаја често захтева плаћање (Сарачевић, 2000).

Сигурност на интернету је још увек без потпуне праве заштите. Подаци које корисници остављају током свакодневног коришћења интернета представљају претњу по сигурност. Подаци који се једном оставе на мрежи остају и опстају чак и ако корисник интернета заборави на њих. Осим учес- талих крађа података, отворена су и многа друга питања о сигурности на интернету због различитих врста замки које дочекују посетиоце.

1.1. Хакерски напади

Хакерски напади, попут оних на нуклеарну електрану у Јужној Коре- ји и компанију Сони, затим крађа милиона података корисника сервиса електронске поште (*Yahoo* и *Google*), показују да је криминал на интернету територијално свеобухватан и да је увек широких размера јер се про- стире толико колико је простран интернет. Све чешће се дешавају крађе идентитета, злоупотреба платних картица, али и угроженост малолет- ника од увлачења у ланац педофилије, као и многе друге криминогене радње. Процењује се да ће сајбер криминал да крене у правцу претњи и изнуда, тако што ће хакери уцењивати власнике компјутера, из којих су уношењем вируса, украли податке, да ће податке задржати док власник података не плати тражену суму.

У последње време најпознатије су две врсте хакера: „хакер црни шешир“ (*black hat hacker*) и „хакер бели шешир“ (*white hat hacker*). Називе су добили по ликовима из старих вестерн филмова у којима су „лоши момци“ носили црне шешире, а „добри момци“ беле шешире. Карактеристика и једних и других је да су добро упознати са ИТ технологијом и да им знање омогућава да продру у мрежу и појединачне компјутере и да креирају вирусе. Међутим, док „црни шешир хакер“ то ради са намером да се неовлашћено докопа података или да уништи базе и онлајн садржаје, углавном из криминогених побуда, „бели шешир хакер“ није концентрисан на злонамерне нападе и крађу података, већ указује на сигурносне пропусте и упозорава власнике рачунара на њихо- во постојање и покушава да спречи штетно деловање „браће по шеширу“. Осим поменутих хакера, познати су и „плави шешир хакери“ (*blue hat hacker*) који су у ствари безбедносни стручња- ци који су ангажовани за откривање и санирање безбедносних пропуста и „сиви шешир хакери“ (*gray hat hacker*) који обављају како злонамерне, тако и корисне хакерске послове, зависно од тога ко их ангажује (Chandrika, 2014).

Слика 1: Шта мотивише хакера?
(Kahn, 2014)

Слика 1. показује резултате истраживања које је у току 2014. године спровела софтвер компанија *Thycotic* о томе шта хакери мисле о себи и о својим активностима. Преко 50% испитаника тврди да нису у томе због новца, већ само из забаве. Само 18% је рекло да су мотивисани финансијском добити и 29% тврди да се хакерисањем баве вођени моралним разлозима који их мотивишу да разоткрију истину о разним питањима. Најинтересантнији податак је свакако тај што 86% хакера не верују да ће икада морати да се суоче са последицама за своје поступке, односно да су изнад закона (Kahn, 2014).

1.2. Насиље преко интернета

Насиље преко интернета (*cyberbullying, online harassment, Internet violence*) је намеран покушај наношења штете кроз манипулацију или нарушавање односа с другима (Cetin et al, 2011), континуираним непријатељским понашањем појединца или групе према другој особи путем комуникационих технологија као што су мејл, мобилни телефон, СМС поруке, инстант порука, личних веб сајтова, блогова. Сајбер насиље подразумева све облике психичког узнемиравања који се преносе из реалног света у онлајн свет.

Интернет је омогућио анонимност комуникаторима како би се остварила „лакоћа“ комуникације. Међутим, анонимност истовремено представља и „окидач“ за губитак самоконтроле код нестабилних личности. Одсуство друштвене одговорности олакшава вршење насиља. Облици насиља на интернету имају широк дијапазон агресивног и непријатељског понашања. То могу да буду претеће или увредљиве поруке, компромитујуће фотографије, ширење гласина, злоупотреба мејлаа нападнуте особе и слично.

Резултати бројних истраживања на тему насиља на интернету показују да они који су укључени у насиље преко Интернета, најчешће имају истовремено две улоге: жртве и злостављача. Преовладава мишљење да је насиље последица недовољно развијених социјалних вештина и вештина решавања сукоба, према чему они који доживљавају насиље то решавају на начин да узврате насиљем (Bulat & Ajduković, 2012).

Психичко злостављање у реалном свету је подједнако распоређено на све категорије и све старосне групе становништва. Почиње од првих школских дана и наставља се у радним колективима. Сајбер злостављање је првенствено сконцентрисано на млађу популацију која се рађа и одраста са новим технологијама. Тешко је доћи до податка колико је раширена ова врста злостављања код омладине јер се пријављује, како се процењује, мање од половине инцидената.

Жртве не говоре о злостављању јер се осећају понижено, беспомоћно и често не желе да се „покажу“ у таквом светлу. Не ретко је у питању и

страх од злостављача. Жртве злостављања често постају социјално изоловане и у страху су да ће их вршњаци одбацити (Robers et al. 2013).

Последице континуираног злостављања врло брзо мењају карактер жртве и доводе до поремећаја понашања, потпуно промењене личности која агресивност не усмерава само према другима, већ и према самој себи. Јавља се склоност према самоповређивању, чак и према суициду. Из агресивног стања, жртва прелази у стање потпуне пасивности и изолације. До тада уравнотежена личност почиње да посеже за супститути-ма попут дувана, алкохола или лекова за смирење. Неретко показује и склоност ка булимији и анорексији, а подложна је и сексуалним поремећајима (Балтезаревић, 2013: 33).

Интернет је поред свих изузетно позитивних карактеристика, нажалост, попримио и карактеристику „сајбер бојног поља”. Зашто насиље преко Интернета? Тражење одговора се креће у правцу да анонимност олакшава непристојно понашање, да се насиље врши да би се осветили оном ко је њих малтретирао и слично. То није прави одговор. Насиље на интернету треба посматрати у много ширем контексту. Не можемо да вршимо сегментацију насиља на онлајн свет и реалан свет. Ако има насиља на интернету, ради се само о варијацијама у методама које користе злостављачи зависно од тога да ли злостављање спроводе у онлајн или офлајн простору.

1.3. Да ли колачићи имају горак укус?

Шта је интернет колачић? То је мали део података који се шаљу са страница током претраживања одређеног сајта, а затим чувају на сајту који служи за претрагу интернетских садржаја (internet explorer, firefox, chrome, safari, итд). Колачићи памте корисничке податке приликом попуњавања регистрационих упитника. Легитимни сајтови их користе као посебне понуде корисницима, као и да би пратили резултате њиховог рекламирања. У сваком случају, ради се о „добрим колачићима”.

Међутим, „колачићи за праћење”, или „упорни колачићи” се обично користе од стране оглашивача да прате шта корисник ради на Интернету за дужи временски период. Све те информације се упућују назад на сервер компаније. Ову врсту колачића користе рекламне куће како би искористиле историју прегледања која се налази на рачунару, формирају датотеку свега што је власник рачунара купио путем интернета, свих страница које је посетио и добијене податке прослеђују осталим компанијама које се баве рекламирањем. Наравно, без знања власника података.

Срећом, колачићи нису везани са вирусима или злонамерним садржајем. Они су једноставно само уређај за праћење (Clemens, 2015)

Колачићине могу да украду личне информације. Сервер може преко колачића да идентификује посетиоца, односно да га повеже са одређеном ИП адресом, да памти име рачунара и да идентификује који оперативни систем се користи. Међутим, увек постоји опасност од крађе колачића.

То може да се уради преко неког скрипт језика (JavaScript или JScript). Укратко, скрипт сакупља колачиће из приватног рачунара и шаље их на адресу заинтересованог сервера. Колачићи сами по себи нису штетни, али увек постоји могућност злоупотребе (Бонч-Брујевић, 2009).

Супер колачићи који се не могу избрисати помоћу „antispyware” програма. Они стално „надзиру” власнике рачунара јер одолевају напорима власника компјутера да их уклоне. Савремене информационо-комуникацијске технологије поред свих добрих особина које имају, нажалост, представљају и моћно шпијунско средство. Подаци на интернету су угрожени и увек постоји могућност злоупотребе „остављених” података. Сајтови на интернету прате своје посетиоце. Неки сајтови прате не само посете учињене на њиховом сајту, већ и посете свим осталим сајтовима.²

Заштита приватности корисника интернета на тлу Европе регулисана је одредбама Директиве ЕУ 2002/58 о приватности у области електронских комуникација која је усвојена 2002. године, а допуњена 2009. године. Члан 5. Директиве ЕУ 2009/136 која је део Регулаторног оквира за електронске комуникације, између осталог, предвиђа да су државе чланице дужне да обезбеде да „похрањивање података или успостављање приступа већ похрањеним подацима у терминалној опреми корисника или претплатника, буде дозвољено само под условом да је конкретни корисник или претплатник дао свој пристанак, након што је свеобухватно и разумљиво, у складу са Директивом ЕУ 95/46, између осталог, обавештен о сврси поступка обраде.” (Стојковић, 2015)

Слика 2: Интернет колачићи¹

¹ <https://exceptionless.com/server-browser-cookie-error/>. Посећено 09.09.2015.

² „Инцидент” са Едвардом Снуоден-ом потврдио је сумње да су америчке обавештајне службе на основу закона осигурале директан приступ фирмама Microsoft, Yahoo, Google, Facebook, Skype, YouTube, PalTalk, AOL и Apple. Фејсбук шпијунира своје кориснике (више од 700 милиона) чак и кад више нису на овој друштвеној мрежи. Facebook је инсталирао колачиће у браузеру који могу да прате посете сваком другом сајту, а не само Facebook-у. И са Google-ом је исто. Чим отворите gmail налог, adsense, google analytics, google почиње да прати све ваше упите.

Овај члан се директно односи на колачиће који се инсталирају у рачунаре корисника. С обзиром на постојање дилеме да ли се заиста путем колачића прикупљају само неопходни подаци или је у питању много шири захват, наведени европски документи указују на то да политика „приватности” које прокламују друштвене мреже не задовољавају дефинисане правне стандарде заштите података о личности.

1.4. Скенирање фототрафија

*Дух је пуштен из боце, нема повратка.
(Alessandro Acquisiti)*

Истраживачи са Карнеги Мелон Универзитета објединили су скенирање слика, „*cloud computing*” и јавне профиле са социјалних мрежа како би покушали да идентификују људе у стварном свету. Резултати које су добили су веома узнемирујући, јер су за неке особе успели чак да добију њихов број социјалног осигурања (Rashid, 2011).

Развијање технологије у смеру препознавања лица корисника друштвених мрежа, драстично се одражава на нарушавање приватности онлајн посетилаца. Трагање за идентитетом на основу фотографија могу да користе владе оних земаља које су заинтересоване за контролу масе. Ове апликације се могу користити на сликама гужве са протеста и демонстрација, стварајући нови облик контроле грађана. Америчка влада финансира истраживачке пројекте у јавном сектору, а што се тиче приватног сектора *Google* и *Facebook* увелико развијају ову технологију. Често се срећу и мишљења да ова технологија, чим се довољно развије, треба да постане доступна јавности. Могућност да примена технологије за препознавање лица постане ефикасна и доступна свима маскира се синтагмом „демократичан надзор”. Колико демократије има у задирању у туђу приватност и личне податке, без

сагласности особе чије се фотографије скенирају, је друго питање?

Слика 3: Скенирање људског лица са циљем прибављања личних података (Dormehl, 2014)

Без обзира на игру по ивици закона о заштити података о личности, који није стран ниједној развијеној, савременој држави, *Facebook* наставља истраживања у овој области и развија „*Deep Face*” технологију којом се отварају питања о моћи данашњих алата за препознавање лица и шта то значи за будућност (Simonite, T. 2014)?

Facebook тврди да има добре намере са развијањем „Deep Face” програма и да ће корисници моћи да виде фотографије на којима се појављују и уколико буду желели моћи ће да траже да се њихови ликови „замуте” и да не буду препознатљиви.

Без обзира на природу намера, да ли је она добра или лоша, чињеница је да је ова технологија врло интригантна. Програм је у стању да идентификује особе са било које слике до које дође на мрежи, а то значи да после тога улази у зону приватности и „чита” све личне податке.

Ова врста технологије носи са собом различите врсте ризика, поготово ако подаци дођу у руке хакера и других злонамерно оријентисаних лица. Украдени подаци могу да буду злоупотребљени за крађу идентитета, злоупотребу података о личности или за виртуелно узнемиравање.

2. Регулаторне дилеме

Присутно је мишљење да се интернет не може регулисати али не због тога што закони нису релевантни, већ због тога што право појединих држава нема могућност да регулише глобалну мрежу. „Сајбер право је по својој природи глобално а ми још увек нисмо добри у овој области” (Higgins, & Azhar, 1996: 9).

Сама употреба термина „глобално управљање” и „глобална права” стварају заблуду јер су национална права појединих држава као и мање формализовани механизми контроле везани за националне владе и представљају основни облик контроле интернет приступа, активности и функционалности.

Велики број земаља је у последњој деценији почео да уводи контролу над технологијом доношењем националних закона у циљу регулисања појединих сегмената интернета у оквиру својих домаћих граница, сматрајући да ова област припада њиховој правној надлежности.

Националне владе често раде у координацији са приватним ИТ компанијама ради заштите информација и вршења контроле у сајбер простору и на тај начин демантују да је интернет изван прописа који су донети у „реалном” свету (Palfrey, 2010).

Дигитални подаци који се отпремају посредством интернета одавно су превазишли проток само веб текста. Путем интернета се све више дистрибуирају велике количине података корисника, врше финансијске трансакције и мобилне комуникације. Да би се заштитила ова врста пословања неопходна је национална регулација. До сада су идентификована три различита модела регулације који су дефинисани по већ постојећим регулаторним приступима. Тако имамо командно-контролни или државни модел, у

коме држава утврђује правила, контролише њихово спровођење и кажњава оне који та правила крше; саморегулаторни модел, у коме је примарно да приватни сектор самостално утврђује правила и спроводи их колективно без икакве јавне интервенције; трећи модел је кооперативни модел који се карактерише тиме да дефинисање правила, имплементација и праћење примене, се раде у кооперацији између јавних и приватних актера, али је иницијатива и надзор у рукама државе (Frydman et al., 2012).

Национално регулисање интернета генерално добро функционише када је регулисана активност добро дефинисана у постојећим законима и сви актери који су идентификовани као прекршиоци конкретне регулативе се налазе на територији одређене државе.

Неподобан садржај на интернету, на пример, може да буде процесуиран по одредбама Кривичног закона које се односе на увреду, превару и сл. Судски поступак у коме се докаже постојање неког кривичног дела повлачи за собом грађанску или кривичну одговорност. Међутим, национална регулатива интернета је неефикасна када је спорни садржај настао ван државне границе (Solum, 2009: 75).

Регулација интернета на међународном нивоу указује на компликовану и проблематичну примену различитих националних прописа, због укључености великог броја различитих држава, различитих нивоа економског и технолошког развоја и различитих оцена о томе да ли је садржај такав да угрожава јавни интерес и да ли због тога заслужује интервенцију државе.

Међународна регулатива у овој области постоји кроз резолуције УН, конвенције и уговоре. Међународна регулатива интернета пре свега обухвата електронску трговину и електронске потписе, интелектуалну својину и област дечије порнографије (Еко, 2001).

Глобална регулаторна тела, укључујући Светски самит о информационом друштву (VSIS) и Радну групу за управљање интернетом (VGIG), су такође укључена у функционална интернет питања, али је њихова улога маргинализована.

Контрола интернета има своју двоструку природу. Она може бити пожељна и позитивна када омогући спречавање криминогеног понашања (праћење ланца трговине људима) или негативна (пресретање порука између опозиционих активиста).

Национална регулатива интернета варира од државе до државе и резултат је дивергентних политичких циљева и режима. Постоје области где готово све државе имају истоветан приступ регулацији. Такав пример је забрана дечије порнографије и пресретање комуникације између терористичких група. Међутим, поједине земље користе контролу интернета за блокирање сајтова за заштиту људских права и надзор над комуникацијом цивилног сектора.

За глобални приступ регулацији интернета посебан проблем је то што поједини садржаји на интернету могу да се посматрају, у појединим земљама, као нелегитимни и да се контрола сматра оправданом, док у другим земљама такви садржаји су прихватљиво понашање и контрола нема оправдања.

У 2011. години коалиција ауторитарних режима предложила је Генералној Скупштини УН резолуцију о увођењу глобалне информационе безбедности под називом „Кодекс понашања” у настојању да резолуцијом осигура да је надлежност над контролом интернета ради заштите јавних интереса суверено право држава.

Резолуција није донета, али је оваква иницијатива алармирала светску јавност, која је у овом покушају препознала покушај да се омогући цензура и неоправдано контролисање интернета.

Евентуална правна регулатива таквог усмерења може да доведе до страха од државне репресије и до прекомерне аутоцензуре онлајн комуникатора. Државни органи уобичајено користе филтрирање садржаја као прву генерацију техничке контроле кад се садржај сматра непожељним из друштвених, политичких и безбедносних разлога. Филтрирање се често примењује када је физичка контрола над одређеним сајтом ван домашаја надлежних органа. Ову методу ауторитарни режими користе за надзор у циљу праћења и контроле дисидената, шпијунирају новинаре и њихове изворе. Eriksson & Giacomello (2009) описују филтрирање као неопходно за безбедност дигиталне комуникације и заштиту података, али и као инструмент за одбрану од пиратерије и кршења ауторских права.

Тако долазимо до констатације да пресретање мејла, читање приватних порука са социјалних мрежа, приступ и претраживање евиденција корисника, представљају форму већ постојеће контроле, која може да се окарактерише као оправдана или не у зависности од тога да ли је контрола урађена са одговарајућим разлогом у оквиру добро дефинисаног правног оквира или није.

Велика Британија је омогућила приступ приватним рачунарима само уз налог овлашћеног лица, кад постоји сумња да корисник интернета чини озбиљан преступ. У том случају се приступа „даљинском претраживању” рачунара. Иако овакав закон игнорише право на анонимност и приватност, Британски пример следе са мањим варијацијама и друге државе унутар ЕУ. Што се тиче САД подаци показују да Национална служба безбедности може да надзире 75% корисника интернета (TANJUG, 2013).

Регулација интернета има несумњиво своје добре стране јер може да спречи сајбер криминал, посебно када су у питању преваре, дечија порнографија, трафикинг, трговина дрогом. Међутим, ко контролише кон-

тролоре интернета? Свака врста контроле онлајн садржаја је задирање у приватност и насилно нарушавање анонимности корисника.

Упуштање у ову проблематику намеће две, не тако лако решиве дилеме. Једна је пред корисницима интернета и садржана је у питању: како спојити задовољство интернета и страх, односно одбрану од нарушене безбедности? Друга дилема је изазов за савремене државе: како решити криминал на интернету а не угрозити сферу приватности корисника интернета? Ако се крене у потрагу за неким виртуелним идентитетом, за који постоји основана сумња да представља претњу за угрожавање безбедности корисника интернета, истрага није могућа без праћења физичког ентитета. Односно, потрага прелази из виртуелног у реални свет. Осим тога, државе се суочавају и са проблемом јурисдикције: интернет страница је на пр. постављена у једној држави, а оштећен корисник је у надлежности друге државе; сајбер криминалци могу да буду група оформљена од стране различитих држављана, а сама територија извршења кривичног дела је отворен проблем за законодавство које је применљиво на офлајн свет (Балтезаревић & Балтезаревић, 2015: 154).

Чињеница јесте да је неопходан системски одговор државе, повезивање и јачање сарадње међу свим секторима друштва и то од индивидуалног до државног нивоа. Како је криминал на интернету врста криминала који не познаје границе, неопходна је, такође и чвршћа, континуирана међународна сарадња у овој области. Међутим, да би државни органи могли адекватно да реагују, а да не наруше одредбе предвиђене чланом 10. Европске конвенције о људским правима, којим се сваком лицу гарантује право на слободу изражавања (слободу мишљења, саопштавања и давања информација и идеја), свако ограничење овог права мора да буде садржано у законској легислативи и државни органи морају да буду уверени да за такво ограничење постоји оправдан интерес.³

Пре свега требало би одговорити на три основна питања: да ли и шта се регулише, на који начин и, треће, ко ће спровести регулацију, а ко ће бити регулисан (Lievens et al., 2011: 8).

³ Одредбом чл. 10. Европске конвенције за заштиту људских права и основних слобода прописано је да свако има право на слободу изражавања. Ово право укључује слободу поседовања сопственог мишљења, примања и саопштавања информација и идеја без мешања јавне власти и без обзира на границе. Овај члан не спречава државе да захтевају дозволе за рад телевизијских, радио и биоскопских предузећа (став 1). Пошто коришћење ових слобода повлачи за собом дужности и одговорности, оно се може подвргнути формалностима, условима, ограничењима или казнама прописаним законом и неопходним у демократском друштву у интересу националне безбедности, територијалног интегритета или јавне безбедности, ради спречавања нереда или криминала, заштите здравља или морала, заштите угледа или права других, спречавања откривања обавештења добијених у поверењу, или ради очувања ауторитета и непристрасности судства (став 2). <http://www.informator.rs/sloboda-izrazavanja-primena-clana-10.-evropske-konvencije-za-zastitu-ljudskih-prava-i-osnovnih-sloboda-u-sudskoj-praksi.html>.

Закључак

Сваки приступ интернету, осим слободе и одсуства цензуре, истовремено је и хакерска замка која чека комуникацију сајбер саговорника у којој ће се разоткрити профил комуникатора. Тако се личност виртуелног посетиоца потпуно огољује и искусни хакери лако долазе разних података који би требало да буду у сфери заштићене приватности.

Циљ регулације нових медија треба да буде усмерен према постављању чврстих темеља на којима ће моћи да се изграде методе за одбрану људског достојанства и приватности у оквиру сајбер простора. Међутим, свако ограничавање слободе изражавања и информисања на интернету мора имати легитимно оправдање у демократским оквирима, у супротном иза покушаја регулације у интересу корисника може да се сакрије цензура.

Количина садржаја, као и број корисника интернета константно расте. Истовремено се стално креирају нове методе погодне за злоупотребу интернета. Због тога слобода на интернету не може да буде неограничена и неопходни су ефикасни механизми заштите права појединаца у сајбер простору, а да се истовремено не угрожава слобода изражавања.

Државе покушавају различитим регулаторним документима да омогуће контролисање друштвених мрежа. Одбрана од прекомерне регулације интернета треба да се креће у правцу широко постављене саморегулације уз учешће цивилног друштва, компанија и других релевантних актера.

Литература:

- [1] Балтезаревић, В. (2013): *Туђи људи*; Београд: Просвета.
- [2] Baltezarevic V. & Baltezarevic R. (2015): *Medijsko pozorište*; Београд: Alma Mater Европаеа.
- [3] Bulat, L. R. & Ajduković, M. (2012): „Obiteljske i psihosocijalne odrednice vršnjačkog nasilja među mladima”, *Psihologijske teme*, 21(1), 167-194.
- [4] Eko, L. (2001): „Many spiders, one worldwide web: Towards a typology of Internet regulation”, *Communication Law & Policy*, 6(3), 445-484.
- [5] Eriksson, J., & Giacomello, G. (2009): „Who controls the Internet? Beyond the obstinacy or obsolescence of the State”, *International Studies Review*, 11(1), 205-230.
- [6] Каличанин, П. и Петровић, Д. (2011): *Приручник о сџресу*; Београд: Институт за ментално здравље.
- [7] Lievens, E; Valcke, P. and Jan Valgaeren, P. (2011): *State of the art on regulatory trends in media*; Brussels: EMSOC. p. 8.
- [8] Palfrey, J. (2010): „Four phases of Internet regulation”, *Social Research: An International Quarterly*, 77(3), 981-996.
- [9] Robers, S; Kemp, J. & Truman, J. (2013): *Indicators of School Crime and Safety: 2012* (NCES 2013-036/NCJ 241446). National Center for Education Statistics, U.S. Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice. Washington, DC.
- [10] Rheingold, H. (1994): *A Slice of Life in My Virtual Community*. In L. M. Harasim (Ed.), *Global Networks: Computers and International Communication* (pp. 57-80). Cambridge: MIT Press.
- [11] Samoriski, J. (2002): *Issues in Cyberspace – Communication, Technology, Law and Society on the Internet Frontier*; Boston: Allyn and Bacon
- [12] Saračević, T. (2000) „Information jungle on the Web: Finding and evaluating information sources”, The Fifth International Conference *Information Technology and Journalism*, Inter-University Center, Dubrovnik, May 22-26.
- [13] Solum, B. (2009): „Models of Internet Governance”. In Bygrave, L. A. & Bing, J. (Eds.). *Internet Governance: Infrastructure and Institutions* (pp. 48-91). Oxford University Press.
- [14] Frydman, B; Hennebel, L. & Lewkowicz, G. (2012): „Coregulation and the rule of law”. In Brousseau, E; Marzouki, M. & Méadel, C. (Eds.) *Governance, regulation and powers on the Internet* (pp. 133-150). Cambridge: Cambridge University Press.
- [15] Higgins, A. & Azhar, A. (1996): „China begins to erect second Great Wall in Cyberspace”. The Guardian. Infotrac Newsstand.
- [16] Chandrika, V. (2014): „Ethical hacking: types of ethical hackers”, *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, Volume 11 Issue 1 November 2014.

Вебографија:

- [1] Бонч-Брујевић Милица (2009): *Бакини колачићи*.
- [2] Доступно на: <http://www.sk.rs/2009/02/skin05.html>
- [3] Весић, И. (2005). Интернет између децентрализованости и фрагментације, приватности и идентификације. <http://www.sk.co.rs/2011/09/skin05.html>
- [4] Dormehl, L. (2014): *Facial recognition: is the technology taking away your identity?*, Доступно на: <http://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues>
- [5] Kahn, J. (2014). Study says most „black hat” hackers don't believe what they do is wrong. Доступно на <http://www.techspot.com/news/57742-study-says-most-black-hat-hackers-dont-believe-what-they-do-is-wrong.html>
- [6] Rashid, Fahmida Y. (2011): *Facial-Recognition Tools, Facebook Photos Threaten End to Anonymity: Study*. Доступно на: <http://www.eweek.com/c/a/Security/Facial-Recognition-Tools-Facebook-Photos-Threaten-End-to-Anonymity-Study-565285>.
- [7] Simonite, T. (2014): *Facebook Creates Software That Matches Faces Almost as Well as You Do*. Доступно на: <http://www.technologyreview.com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/>
- [8] Стојковић, М. (2015): *Фејсбук и праћење корисника путем додатака за друштвене мреже*. Доступно на: <http://pravoikt.org/fejsbuk-i-pracenje-korisnika-putem-dodataka-za-drustvene-mreze/>
- [9] TANJUG, (2013): *NSA nadzire 75 % interneta u SAD*. Доступно на: https://www.butobu.rs/business_news.php?idnews=2955&catnavig1=IT&src=1
- [10] Cetin, Yaman & Peker (2011). *Cross-Gender Equivalence of Cyber Bullying and Victimization Participatory Educational Research (PER)* Vol. 2(2), pp. 59-69, August, 2015. Available online at Clemens, M. (2015). *Cookies are bad for your health and your computer!* Доступно на: <http://dormnet.blogspot.rs/2015/02/cookies-are-bad-for-your-health-and.html>
- [11] <http://www.partedres.com>
- [12] <https://exceptionless.com/server-browser-cookie-error/>.
Посећено 09.09.2015.
- [13] <http://www.informator.rs/sloboda-izrazavanja-primena-clana-10.-evropske-konvencije-za-zastitu-ljudskih-prava-i-osnovnih-sloboda-u-sudskoj-praksi.html>. Посећено 11.09.2015.

Associate Professor Vesna Baltezarević, PhD

Faculty of Culture and Media

„John Naisbitt” University

Belgrade

Radoslav Baltazarević, PhD

FREEDOM ON THE INTERNET AND ITS CONSEQUENCES

Summary: *The Internet is undoubtedly one of the most provocative sociological and psychological phenomena. It is said that Internet links all those fallen communicators who cannot cope in the real world. However, socializing and surfing online space does not pass without leaving a trace. Each user provides information about themselves, sometimes as a condition to be able to access the required application, when consciously accedes to it, sometimes exchanging information with other members of the network, unaware that the network "remembers everything", that data remains deposited even when its removed profile. Increasingly, we are faced with data theft and identity by criminal hacker groups. These works generally go unpunished because the internet as „free” network, often beyond legal control. Cyber security is a challenge that will have to be resolved regulatory as soon as possible. It leads to a dualism in solving these problems. The problem arises because of the possibility that the resolution of security issues on the one hand, undermine the protection of privacy on the Internet on the other.*

Key words: INTERNET, COMMUNICATORS, DATA, HACKERS, SECURITY.