ЗБОРНИК РАДОВА ПРАВНОГ ФАКУЛТЕТА У НИШУ
XLVI/2005

Др Видоје Спасић

НЕКИ АСПЕКТИ ПРИВАТНОСТИ У САЈБЕРСПЕЈСУ

UDK 004.738.5:179

Рецензент: проф. др Зоран Миладиновић

Сажетак

Питање приватности одувек је изазивало пажњу у различитим научним областима. Проблем је мултидисциплинаран и захтева обраду и посматрање са различитих аспеката. Са појавом дигиталне технологије проблем приватаности све више добија на својој актуелности и значају. У раду су обрађени неки аспекти приватности у сајберспејсу (виртуелном простору): правни, технички и психолошки.

Кључне речи: приватност, internet, сајберспејс.

Др Видоје Спасић[1]

НЕКИ АСПЕКТИ ПРИВАТНОСТИ У САЈБЕРСПЕЈСУ

1. УВОДНЕ НАПОМЕНЕ

Сајберспејс (кибернетски простор) осим што нам пружа многе погодности, садржи бројне латентне опасности. Најзначајније области у којима се, нарочито, огледају потенцијално негативни утицаји дигиталних технологија представљају сајбер криминал, интелектуална својина и област приватности.

Кључне области у којима долази до електронског сакупљања личних података и до могућности њихове злоупотребе су електронско пословање (укључујући и електронско плаћање), медицинско поступање и коришћење различитих врста internet сервиса. Тако, нпр, при електронском пословању сакупљају се велике количине информација о потрошачима, посебно путем "click-stream monitoring-a". Поред тога, појединци откривају информације о себи на internet-у, било активно, односно добровољно или пасивно, односно несвесно. Пасивним откривањем одају се подаци које појединац, иначе, не би желео да открије о себи, најчешће употребом тзв."cookies" фајлова, који могу да открију информације о " click-stream "-у, односно који корисник, када и колико је користио одређени сајт, које друге сајтове посећује, па чак и информације о садржају корисниковог хард драјва.

Електронска комуникација подразумева размену информација између два корисника или корисника и сервера. Она има два основна вида: видљива и невидљива размена.

Видљив процес размене података врши се уз знање корисника и одвија се путем тзв. "ћаскања", односно "четовања" (chat rooms discussion), news-groups, e-mail-a, директоријума (тзв. именика или регистра) и електронског

[1] Асистент Правног факултета у Нишу.

пословања (укључујући и електронска плаћања, мада се она могу, у извесним случајевима, обављати и путем невидљиве комуникације).

Невидљиво поступање одвија се без знања корисника и врши се преко података за повезивање loge file (тзв. лог фајлова), "trafic data" (података о саобраћају) и "cookies" (тзв. "колачића").

Под приватношћу подразумевамо скуп информација нераскидиво везаних за појединца које дају печат његовој индивидуалности, а које су правно заштићене од неовлашћеног приступа, као и од повреде сваког другог лица (а тичу се имена, слике, брачног или породичног живота, навика, хобија или другог личног интересовања појединца). У најширем смислу, приватност значи много ствари многим људима и различите ствари у различитим контекстима.

Када појединац сурфује Web-ом, он очекује потпуну анонимност, чак и већу него у физичком свету. Уколико он није намерно открио податке о себи и свом идентитету, он верује да нико не зна ко је он или шта ради. Али, internet оставља детаљан траг података о сваком кораку који појединац направи на Web-у. Трансакциони подаци, "click stream" подаци или "mouse-dropings" подаци могу да дају профил нечијег онлајн живота.

Многе технологије исписане директно на корисниковом хардверу омогућавају Web сајтовима да тајно прикупљају информације о његовим онлајн активностима и сачувају их за каснију употребу.

У физичком свету појединци могу да плаћају робу и услуге великим бројем платежних средстава (готовина, кредит, платне картице итд). Избор платежног механизма представља латентан атак на приватност. Количина личних информација која се добија и сакупља креће се од практично никакве у готовинској трансакцији, до откривања идентитета, врсте робе или услуге, имена продавца, датума кредитне трансакције, и сл. код електронског плаћања. Сходно томе, листа лица која имају приступ личним подацима много је већа. У суштини, готовина пружа највећу могућу заштиту приватности приликом финансијских трансакција у офлајн свету. Њој је тешко ући у траг, јер се не захтева додатно доказивање аутентичности које често доводи до прикупљања информација о идентитету.

У онлајн свету, дигитални еквивалент готовини још није нашао широку примену. Већина онлајн куповина обавља се кредитном картицом, која открива

лични идентитет и олакшава прикупљање података о куповини. Недостатак еквивалента готовини у онлајн свету, као и његова редукована употреба у физичком свету прете да озбиљно угрозе личну приватност у финансијским трансакцијама.

Исто тако, када појединци повере информације доктору, трговцу или банци, они очекују од њих да са њиховим информацијама поступају професионално и користе их само у сврхе пружања жељене услуге. Међутим, постоје бројни примери да компаније, али и владине организације користе поверене личне информације својих клијената у сврхе које далеко премашују намере и жеље клијената.[2]

Када неко пошаље e-mail поруку, он очекује да ће је прочитати једино особа којој је та порука и намењена. Нажалост, и ово очекивање је у опасности. У поређењу са писмом, e-mail порука путује по релативно непредвидљивом и неконтролисаном окружењу. Док путује мрежом, e-mail-ом манипулишу многи независни субјекти. И док порука може без тешкоћа путовати од једног народа до другог, уставна заштита приватности престаје на граници. Осим тога, за разлику од телефонских или поштанских система, internet нема централизована места контроле.

Слично претходном, опасност од неовлашћеог прикупљања и злоупотребе личних податак постоји и код коришћења других internet сервиса (четовање, претраживање и сл).

Осим наведеног, данас је вероватније да се наши дневници, медицински досијеи, приватни разговори и поверљива документа нађу у виртуелном простору, него на неком сигурном физичком месту. То има драстичне последице по нашу приватност. Док се наше личне информације крећу све даље и даље сајбер простором, постојећи закон пружа све мању и мању заштиту.

Такође, постоји слаба заштита приватности када је реч о личним документима и досијеима. Традиционално су се дневници чували под креветом, у

[2] Према најновијим информацијама, Федералне власти у САД дозволиле електронске здравствене картоне. Чип величине зрна пиринча уграђује се изнад лакта и ради на основу радио-таласа. Он емитује шифру (код) са 16 бројева коју доктор декодира путем скенера како би утврдио идентитет пацијента и његове медицинске податке (историју ранијих болести, алергије, тип крвне групе). Ти подаци ће бити смештени у посебној бази података.

задњој фиоци ормана или у радном столу. Са најездом кућних компјутера лични дневници су премештени у хардвер. Грађани су брзо искористили предности компјутера за обраду и преписивање својих важних докумената и мисли. На исти начин и слике из фото албума прешле су на CD-ROM.

Данас компјутерска мрежа пружа појединцима могућност да изнајме простор ван својих кућа и тамо чувају личне досијее и личне странице са Web-а. Али, чување ових личних мисли и успомена на удаљеном серверу елиминише многе могућности заштите приватности, које су постојале док су чуване на традиционалан начин у кући.

2.ВРСТЕ ПРИВАТНОСТИ

Генерално, постоје четири врсте приватности:[3]
- *физичка приватност* – која се дефинише као слобода неке особе од сензорног мешања неког другог, која се постиже захваљујући томе што су други спречени да физички опазе ту особу;
- *менална приватност* - слобода од психолошког мешања неког другог, а постиже се преко спречавања других да приступе и утичу на психу те особе;
- *приватност одлучивања* - као слобода од мешања неког другог у одлуке које доноси особа а које се тичу ње и њене ближе околине;
- *информациона приватност* – која се са гледишта појединца дефинише као слобода од недозвољеног сазнавања података о њему.

Основна питања информационе приватности, којом ћемо се бавити, јесу које информације о себи особа треба да преда другима, које информације треба да задржи за себе и који услови треба да се поставе. Две су основне опасности по информациону приватност:
- *напредак информационе технологије,* и њени повећани капацитети за надгледање, комуникацију, израчунавање, складиштење и враћање ускладиштених информација;
- *повећање вредности информације у доношењу одлука*. Менаџери све више траже информације, чак и када њихово набављање захтева кршење приватности.

[3] Према неким подацима постоји преко 8.000 различитих система који садрже податке о грађанима на основу којих се они могу користити у различите сврхе.

У информационом друштву грађанин треба да поседује барем три основне ствари:
- интелектуалне вештине да прими информацију.[4]
- право да приступи технологијама које чувају, преносе и обрађују информације.[5]
- право да приступи самој информацији.[6]

2.1. Основне особености човека у сајберспејсу

Нема сумње да се виртуелни свет доста разликује од стварног. Дигитализовање људи, односа и појава потпуно је променило начине на који људи могу комуницирати. Укратко ћемо анализирати како се људи понашају ради утврђивања неких психолошких карактеристика које су карактеристичне за понашање људи у "cyberspace-у". У различитим условима јавља се и различита комбинација ових карактеристика, која резултује различитим психолошким квалитетом окружења које одређује како људи доживљавају себе и друге.

Основне психолошке карактеристике човека у "cyberspace"-у су:
- смањење сензације;
- повећање перцепције за текст;
- флексибилност идентитета;
- измена перцепције;
- уједначавање статуса;
- несхватање простора и удаљености;
- привремена флексибилност;
- друштвена вишеструкост;
- свест о могућности архивирања свега;
- поремећаји медија.

Што се тиче смањења сензације, она је условљена технолошким могућностима. Мултимедијални "chat" је засада доступан малом броју корисника

[4] То укључује читање, писање, разумевање и израчунавање. Задатак да развије ове вештине код људи припао је модерном образовању;
[5] То су библиотеке, радио и телевизијске станице, телефони, рачунари и све више интернет. Ово постаје проблем социјалне економије;
[6] И ово је такође проблем социјалне економије, али он укључује и питања интелектуалне својине.

мреже. Највећи део корисника комуницира путем куцања текста. Чак и када се превазиђу ова ограничења, људи дуго неће моћи да остваре стварну физичку интеракцију (јер, технологија ће јако тешко моћи да пренесе загрљај, руковање или пољубац). Ограничена сензорна искуства имају своје предности и мане, и представљају једну од основних карактеристика "cyberspace"-а.

У вези са ограничењима комуникације путем писаног текста, њу никада не треба потценити као моћну форму изражавања и комуникације. E-mail, "chat" и сервиси инстантних порука попут "ICQ" поред лакоће коришћења и штедње онлајн ресурса имају и друге предности над мултимедијалним сервисима комуникације.

Што се тиче флексибилности идентитета, важан фактор је недостатак комуникације лицем у лице (face to face). Комуницирајући само путем куцања текста, отвара се опција у којој појединац може да бира хоће ли бити оно што јесте, приказати само делове свога идентитета, претворити се у неку фиктивну особу, или остати потпуно анониман. У мултимедијалним окружењима, пружа се и могућност изражавања путем визуелног костима, или мултимедијлног "avatar-а".[7] Анонимност која произилази из овога може постати и веома опасна. Људи могу или да некоректно поступају са другима, или да потпуно отворено разговарају о темама о којима не би смели да разговарају лице у лице са другим људима.

Измена перцепције је стање које произилази из дуготрајног мировања и посматрања монитора. Перцепција нормалног света постаје непотребна и она се значајно смањује. Док читају поруке или "chat"-ују са другима неки људи доживе осећај сличан спајању интелекта. У замишљеним мултимедијалним световима, где учесници пролазе кроз зидове, стварају објекте по својој жељи и остварују интеракцију са другим учесницима, то осећање се претвара у измењено стање свести, које подсећа на сан. Оно може чак узроковати и неку форму зависности од компјутера и "cyberspace"-а.

У највећем броју случајева свако на internet-у има једнака права да се изрази. Она не зависе од друштвеног статуса, пола, имовинског стања, расе, старости... Такво стање се све чешће назива "демократија мреже".

[7] Аватари, или виртуелне индивидуе, су становници "cyberspace"-а. Аватар је стабилан идентитет који је креирао неки корисник "cyberspace"-а. Простор који је познат под именом "cyberspace" у ствари чини проток информација и то двојако: *размена инфомација преко софтверског кода, или размена информација међу аватарима.*

Географска удаљеност помало спутава комуникацију у "cyberspace"-у. Човек из Србије без тешкоћа комуницира са неким из Мексика преко сервера у Аустралији. Безначајност географске удаљености олакшава људима који имају јединствене тежње да се међусобно споје. У својој ближој околини, такви људи често не могу да пронађу себи сличне. То може бити веома позитивно, рецимо у случају када се људи који имају јединствене проблеме нађу и међусобно помажу, али може бити и негативно јер омогућава да се нађу и комуницирају људи који имају неке асоцијалне тенденције које могу бити опасне по њихову околину.

Ако узмемо критеријум време, у принципу постоје две врсте комуникације.

Прва је *синхрона комуникација*, код које је потребно да људи комуницирају у исто време, на пример "chat", а друга је *асинхрона комуникација*, која не захтева интеракцију људи, који су укључени у комуникцаију у исто време.

Но и у синхроном и у асинхроном начину комуникације, постоји одређени временски размак. Он може трајати од неколико секунди, до неколико дана или недеља. Тај временски размак омогућује људима да размисле и смисле прави одговор. Неискуснији корисници "cyberspace"-а могу имати тешкоће око тога да схвате да тај размак мора да постоји, јер они често очекују одговор одмах. Такође, по питању времена, оно у "cyberspace"-у тече у неку руку брзо (уколико сте на неком форуму или било ком "on-line" друштву пар месеци, већ Вас сматрају за старог члана.

На internet-у се релативно лако можемо комуницирати са више људи истовремено. Лакоћа којом упознајемо велики број људи, још је повећана развојем претраживача и глобализацијом мреже. Питање зашто упознајемо једну врсту људи, одавно је познато психолозима. Приликом бирања пријатеља, ми користимо не само свесне, већ и подсвесне разлоге. Готово све "онлајн" активности могу се снимити на неком носачу података. За разлику од спољног света, корисник internet-а може имати стални записник о својој комуникацији. Такви документи могу бити веома корисним.

Упркос целокупном развоју internet-а, постоје моменти када техника не може да нам послужи у испуњењу наших жеља. Постоје тренуци када се конекције прекину или једноставно постоје сметње у каналима комуникације.[8]

[8] Некада рачунар не враћа ништа, чак ни поруку о грешци. Тада се осећамо беспомоћно, зависно од технике или љути због њене несавршености (уколико знамо прави разлог квара).

Један од познатих ефеката који има "cyberspace" је дезинхибиција, непостојање забрана. Познато је да људи у "cyberspace"-у говоре и чине ствари које не би иначе радили или говорили. Људи се опусте, изражавају се отвореније и слободније. Тај ефекат, међутим, може бити, мач са две оштрице. Људи се могу отворити и говорити о ономе што их мучи, или пак бити груби, некоректни, па чак и понижавати или претити.

Ову дезинхибицију изазива неколико фактора, а то су:
- *ти незнаш ко сам ја (анонимност);*
- *ти ме не видиш (невидљвост);*
- *одложене реакције (асинхронизација);*
- *то је све у мојој глави (солипсистичка интројекција);*
- *неутрализација статуса;*
- *ефекат интеракције.*

Приликом крстарења internet-ом, већина људи нема податке о нама. Систем оператори, или неки напреднији корисници могу на основу e-mail адресе сазнати нешто о нама, али већина људи зна само оно што им кажемо. Охрабрени анонимношћу многи људи раде оно што у спољном свету никада не би радили. Тако на површину често избијају потиснуте емоције и тежње и та појава се у психологији назива дисоцијација.

Већина "онлајн" окружења не дозвољава корисницима да се међусобно виде. Док крстаре internet-ом и посећују сајтове, места за конверзацију, људи уопште не морају да знају да сте уопште присутни. Они који могу знати да смо присутни, не могу стварно да нас виде или чују. Чак и ако је наш електронски идентитет видљив, прилика да физички будемо невидљиви још појачава ефекат дезинхибиције. Нема потребе бринути се како изгледате или звучите док куцате неку поруку. У свакодневној комуникацији, људи некад покушавају да избегну да се међусобно гледају у очи, јер то отежава да кажу нешто што им тешко пада.

Феномен асинхроности може се размотрити и са психолошке тачке гледишта. То што не морамо одмах да се суочимо са нечијом реакцијом, такође може да појача ефекат дезинхибиције. Неки људи схватају то као својеврстан начин да побегну од онога што су казали, јер су они то само "послали" и сигурни су неко време док одговор не стигне.

Док читамо поруку, ми често осећамо да нас прожима особа која нам ју је послала. Некада замишљамо њен глас и чини нам се да га чујемо како нам чита редове. Не морамо чак ни знати како тој особи глас звучи у стварности, већ га можемо замислити на основу онога што знамо о њој. У ствари, свесно или несвесно, ми можемо замислити и изглед особе са којом комуницирамо као и то како се она понаша у спољном свету.

Наш "онлајн" пријатељ тада постаје карактер нашег унутрашњег света, којега делимично обликују наше жеље, емоције, потребе потиснуте или видљиве, а делимично оно како се та особа представља пред нама. Уколико нас та особа подсети нечим на неку особу коју познајемо, ми можемо да јој придружимо и њен лик. Како тај замишљени карактер све више постаје стваран у нашој машти, ми можемо почети да замишљамо (можда не свесно) како је цела комуникација између нас и те особе само наша имагинација.

У својој машти, људи слободно говоре оно што би хтели, али немају храбрости да то учине. У случају "онлајн" окружења, реалност и машта се могу приближити преко горе разматраног феномена. Једна од честих појава је да људи замисле сопствени глас како им чита туђу поруку. То није непознато психолозима, који ту појаву објашњавају тиме да особа стиче утисак да разговара са самом собом. Наши "онлајн" пријатељи, који како смо видели могу представљати и нас саме, могу често у нашој машти то и постати, и тада у разговору са самим собом откривамо ствари које другима не бисмо никада рекли.

Такође, разматрана је и чињеница да је статус особе неважан у "онлајн" окружењу (људи не знају да ли сте директор, политичар, студент или домаћица која комуницира преко кућног рачунара). Чак и ако људи знају нешто о вашем "офлајн" статусу, он има мало утицаја на ваш "онлајн"статус. Људи тада показују тенденцију да према онима који би могли представљати "офлајн" ауторитете буду грубљи и да их више критикују, па чак и малтретирају, надокнађујући оно што не смеју да чине у стварном окружењу.

Наравно, ови фактори нису кључни на понашање људи. Понашање највише зависи од међусобне интеракције и расположења које влада у том делу "cyberspace"-а. Ефекат "онлајн" дезинхибиције може имати велики утицај на понашање појединца, али може и једва приметно утицати на њега. Понашање такође зависи и од типа личности у "cyberspace"-у.

2.2. Типови личности у "cyberspace"-у

Постоји више исцрпних теоријских система који нам могу показати како се бројни типови личности понашају у "cyberspace"-у. Бројна схватања стоје на гледишту да "cyberspace" посматрају као продужетак унутрашњег психичког света. То је психолошки гледано, простор који може да стимулише процесе пројекције, може изменити сензорно искуство и чак створити стање слично сну. Психоаналитичка теорија је веома корисна код разумевање унутрашњег психичког света и бројних димензија свести које су карактеристичне за особу која се налази у сајберспејсу.

Теорија психоанализе садржи веома богат, описан модел типова личности који је резултат сто година истраживања и клиничке праксе. Nancy Mc Williams у својој књизи "Психоаналитичке дијагнозе" нуди обједињени преглед бројних психоаналитичких концепата који се тичу типова девијантних личности. За сваки од њих, ааутор анализира ефекте карактеристика, темперамента, одбрамбених и процеса прилагођавања као и односа међу објектима.

Типови личности који се могу навести су:
- *психопатски (асоцијални);*
- *нарцисоидни;*
- *шизоидни;*
- *параноидни;*
- *депресивно/манични (импулсивни);*
- *мазохистичко/садистички;*
- *опсесивно/компулсивни;*
- *хистерични;*
- *асоцијативни тип.*

Веома продуктивно поље истраживања се односи на начин како се различити типови личности понашају "онлајн", како субјективно доживљавају и реагују на различите психолошке карактеристике "cyberspace"-а, како доживљавају друге особе и како "cyberspace" утиче на њих и патолошки и благотворно.

3. "COOKIES" ("КОЛАЧИЋИ")

Наводећи тзв. невидљиву комуникацију на мрежи, истакли смо да се она, углавном, обавља у форми података за повезивање или "loge file", "trafic data", као његова поткатегорија и "cookies" (тзв. "колачићи").

Сваки пут када клијент посети неки сајт, односно сервер, он оставља неку врсту посетнице која открива његов екстензивни профил: његов ID, IP адресу, мејл адресу, који тип компјутера има, који сајт је задњи посетио и које је радње предузимао, податке о његовом читачу, односно претраживачу, време приступа, време задржавања, и друге детаље. Подаци овакве врсте аутоматски се сакупљају од стране сервис-провајдера и чувају на његовом серверу, у посебној датотеци која се зове "log file". Детаљнији подаци овакве природе називају се "trafic data." Наравно, сакупљање и евентуална касниј употреба свих ових података (осим ако се то ради по налогу државног органа, нарочито приликом извршења појединих кривичних дела), итекако може нарушити клијентову приватност. Дакле, иако изгледа да би "сурфовање" internet-ом требало бити анонимно, као читање новина, оно то, ипак, није.

Један од најзначајнијих примера повреде личних података, односно, нарушавања приватности појединца представљају тзв. "колачићи" ("cookies"). "Cookie" је мали фајл створен на клијентовом хард диску, од стране сервера коме је овај приступио. То је механизам којим сервер (помоћу CGI скрипте) може код клијента креирати неку информацију и касније је опет користити. То се у правилу догађа када сервер враћа HTTP објект клијенту. Било који будући HTTP захтев од стране клијента, укључиће и информације спремљене у "колачићу". Међутим, такав механизам омогућује нове типове апликација. Изворно, Netscape их је креирао, како би омогућио повратак на претходни екран, а данас их у Netscape-у зову Persistent Client-Side State Information. Нико са сигурношћу не зна по чему су "колачићи" добили своје необично име.

Најпопуларнији internet читачи, Netscape Navigator и Internet Explorer омогућавају WWW серверима да шаљу и примају информације о клијентовим посетама путем "колачића". Када неки сервер жели послати "колачић" клијенту, отвори се тзв. Dialog box, а он има избор прихватити га или не. Ипак, увек постоји имплицитна "претња" да сервер неће радити најисправније уколико клијент не прихвати његов "колачић". Срећом за већину

претраживача (Search Engines) то не важи. Но, уколико клијент иде у онлајн трговину, без прихватања "колачића", то највероватније неће успети. На располагању су и софистицираније алати за хватање у коштац с "колачићима".[9]

У великом броју случајева овај ће бити искоришћен да забележи и сачува клијентово корисничко име (user ID) и лозинку (password), како би се следећи пут убрзао приступ. Међутим, "колачићи"се могу користити и за истраживање тржишта у којем клијенти већином недобровољно учествују, што нарушава њихову приватност. Наиме, како се "колачићи" могу користити и за праћење информација од једног до другог WWW сајта, то постаје врло корисно у апликацијама као што су каталошка куповања. Корисник бира артикле с најразличитијих WWW сајтова, а "колачић" бележи потребне податке. То би у пракси омогућило разгранавање виртуалних трговина стварањем јединствене понуде низа мањих компанија.

Данас, није уопште необично да клијент добије поруку да неко жели спремити "колачић" на његов диск, а да уопште није ни посетио тај WWW сервер. Такође, већ је увелико заживела пракса да клијента усред рада на рачунару прекидају рекламним порукама баш као што се рекламама прекидају ТВ емисије. Ипак, без обзира на речено, уколико клијент не жели "колачиће", техничке могућности му дозвољавају да може предузети мере ка њиховом елиминисању. Као прво, може их избрисати, наравно након што изађе из својих претраживача, односно читача.[10] Брисање неће имати никакве последице, осим што ће WWW сервери, који на клијентовом диску неће пронаћи своје "колачиће", приликом следеће посете одмах "испећи" нове. Уколико клијент жели видети који му то сервери шаљу "колачиће", постоје техничке могућности да то и утврди.

Без обзира на изречено, данас већ толико сервера масовно користи "колачиће" да упозорења о њима више немају никакву сврху. Али, срећом постоје и техничке могућности клијент установи ко му шаље "колачиће".Наша све већа зависност од internet-а умањује шансе да сачувамо приватност. Данас већина Web презентација смешта тзв. "колачиће" на клијентов хард диск како би, у зависности од његових интересовања, испоручивале одговарајуће

[9] То су нпр. Cookie.cutter од PGP-а и CookieMaster ZDNet-а и други.

[10] Корисници Netscape Navigator-а наћи ће их под именом cookies.txt у Netscape folder-у. Корисници Internet explorer-а наћи ће "колачиће" у folder-у Cookies унутар Windovs folder-а

информације. Засад, најсигурнији начин заштитите приватности јесте да клијент подеси читач тако да не прима "колачиће" и да обрише постојеће "колачиће" с хард диска. Међутим, уколико клијент одбаци "колачиће", постоји реална опасност да неће моћи да приступи жељеним сајтовима, односно Web презентацијама.

4. ЛЕГИСЛАТИВА

У чл. 12, Универзалне Декларације о људским правима, од 10. децембра 1949. године, каже се: "Нико не сме патити због самовољног уплитања у његов приватан живот, породицу, дом или кореспонденцију, или због вређања његове части и угледа."

Такође, у чл. 8, Европске Конвенције о заштити људских права и основних слобода, од 04. 11. 1950. године, установљено је овлашћење на поштовање приватности и породичног живота, дома и кореспонденције.

У Француској, Актом N° 70-643, од 17. јула 1970. године, уведен је чл. 9 у Грађански законик, чији први параграф истиче да свако има право на поштовање своје приватности.

У Немачкој је на снази Савезни Закон о мултимедијима, од 1. августа 1997. године, у чијем чл. 2 се регулише заштита података. У том смислу, установљена је обавеза за пружаоце услуга да понуде својим корисницима могућност анонимног приступа и плаћања (или псеудонимно), кад год је то разумно и технички могуће.

На нивоу ЕУ донета је Директива 95/46, од 24. октобра 1995. године, о заштити и слободном кретању личних података (Official Journal L 281, 23/11/1995. p. 0031-0050) као и Директива 97/66, о поступању и заштити података личног карактера у сектору комуникације, од 15. децембра 1997. године (Official Journal N° L 024, 30/01 1998, p. 0001-0008). Најзад, 12. јула 2002. године, донета је Директива поступању са личним подацима и заштити приватности у области електронске комуникације (Директива о приватном животу и електронским комуникацијама, бр. 2002/58, 12. 07. 2002, Official Journal N° L 201, од 31/07/2002. p. 0037-047). Ова Директива намеће обавезу хармонизације у циљу обезбеђивања адекватног нивоа заштите фундаменталних права и слобода, нарочито права на приватност, у поступању са

личним подацима у електронској комуникацији и слободног кретања таквих података и средстава и сервиса електронских комуникација у оквиру ЕУ. У том смислу, провајдери јавно приступачних електронских комуникационих сервиса морају предузети све техничке и организационе мере ради обезбеђивања сигурности својих сервиса (чл. 4).

Државе чланице дужне су, такође, да у националним законодавствима, а посредством наведених јавних сервиса, обезбеде поверљивост комуникација у односу на тзв. "trafic data" (податке о саобраћају или промету на мрежи, који укључују све појединости везане за приступ и коришћење мреже, као што су усер (корисник), компјутер са кога се приступа, време и трајање приступа, назив приступљеним сајтовима, радње предузете на њима, читање или "скидање" одређених фајлова и тд.). Овакви подаци морају остати тајни и бити недоступни трећим лицима, осим на захтев државних органа при спровођењу одређених поступака. (чл. 5). Такође, подаци везани за претплатника или другог корисника на мрежи, морају бити уништени или бити држани анонимно и могу се употребити само за строго прецизирану сврху (нпр. за специфицирање наплате од стране овлашћеног провајдер сервиса, а која обухвата мерење и наплату времена коришћења мреже, од стране овлашћеног провајдер-сервиса, или за утврђивање неовлашћеног приступа и коришћења мреже, односно одређених сајтова) (чл. 6 и 7).

У случајевима када се за коришћење мреже захтева откривање идентитета корисника, сервис-провајдер је дужан спречити његово откривање трећим лицима (чл. 8).

У чл. 12, Директиве, регулисани су тзв. директоријуми или именици (регистри). У том смислу, чланице треба да обезбеде да претплатник буде бесплатно и пре укључивања у директоријум информисан о сврси штампаног или електронског директоријума претплатника, који је на располагању јавности или је добијен преко директоријума захтеваног сервиса, у којима лични подаци могу бити инкорпорисани, тако да свака њихова будућа употреба може бити базирана на тражењу уграђених функција у електронској верзији директоријума (чл.12).

У Повељи о људским и мањинским правима и грађанским слободама (од 28. фебруара 2003. године, која је саставни део Уставне повеље Заједнице Србија и Црна Гора), у чл. 24 регулисано је право на поштовање приватног и породичног живота. У том смислу, свако има право на поштовање приватног

и породичног живота. Такође, тајност писама и других средстава комуникација је неповредива. Одступања су дозвољена само у законом предвиђеним случајевима, на основу одлуке суда, и то на одређено време и ако је то неопходно ради вођења кривичног поступка или одбране земље.

Заштита података о личности је загарантована. Њихово сакупљање, држање и употреба уређују се законом. Такође, забрањена је и кажњива свака употреба података ван сврхе за коју су намењени. Најзад, свако лице има параво, у складу са законом, да буде обавештено о прикупљеним подацима о својој личности.

Национални кривични закони санкционишу повреде права на приватни живот. Тако су, на пример, кривична дела неовлашћено фотографисање, објављивање туђег списа, портрета, фотографије, филма или фонограма личног карактера, неовлашћено прислушкивање и тонско снимање, неовлашћено сакупљање података и др. Кривични законик РС, из 2005. године[11], прописао је више кривичних дела која се односе на повреду приватности појединца (чл. 141-146).

Закон о здравственој заштити РС, из 2005. године[12], у чл. 30 пружа право на приватност и поверљивост информација.

Закони који омогућавају властима да шпијунирају кориснике internet-a све чешћи су и у демократским земљама. Амерички конгрес усвојио је такав Закон (Patriot Act), у октобру 2001. године, а Француска месец дана касније (Закон о свакодневној безбедности и Закон о дигиталној економији).

У Француској су internet провајдери проглашени одговорним за садржај који се објављује на сајтовима и обавезни су да у кратком временском року блокирају приступ таквим информацијама.

Немачка је једна од земаља пионира у изградњи онога што је internet данас. Она припада групи од двадесет земаља које су потпуно, интернет речником речено, "конектоване". Власти су озбиљније почеле да се боре против расизма, као и порнографије присутне на мрежи, а који угрожавају приватност или слободу изражавања. Оно што покушаје оваквих борби спутава је немачка

[11] "Сл. Гласник РС" бр. 85/05, од 29.09.2005. године.
[12] "Сл. Гласник РС" бр. 107/05, од 28.11.2005. године.

бирократија, тј. компликованост односа између федералних и локалних, односно покрајинских власти.

5. КАКО СЕ ЗАШТИТИТИ?

Постојећи законски оквир није предвидео свеобухватну и прожимајућу улогу коју ће информациона технологија имати у нашем свакодневном животу. Законски оквир за заштиту личних података у средствима електронске комуникације, иако изграђен на уставним и законским принципима заштите, одсликава техничке и социјалне "пропусте", одређених периода историје.

Такође, проблем представљају и одређене карактеристике интернета (отворе-ност мреже, нецентрализован систем контроле и сл). С друге стране, стварање одговарајуће заштите приватности у сфери електронике одувек је представљало велики напор. То захтева велику свест, не само о променама у технологији, већ такође и о променама у начину коришења технологије од стране грађана и о томе како се те промене крећу у границама постојећег закона.

Постоји више подручја на која морамо да усмеримо наше активности како би смо побољшали заштиту наше приватности. У том смислу треба, пре свега, предузети следеће кораке у заштити личних података, сакупљених онлајн:
- задржати конзистентан ниво заштите приватности комуникација и инфор-мација без обзира на то где се чувају (било аналогним или дигиталним начином, офлајн или онлајн, свеједно);
- спровести легалну заштиту прикупљених трансакционих података (како би исти били коришћени само за сврхе за које су намењени);
- подстаћи технологије које ограничавају прикупљање података који идентификују појединца (када се то чини без његове сагласности);
- увести правила и применити технологије које у току комерцијалних инте-ракција дају појединцима контролу над личним информацијама (нарочито употребом криптографских метода).

5. ЗАКЉУЧАК

Нема сумње да су подаци који спадају у домен приватности појединца у сајберспејсу стављени пред велику и озбиљну опасност. Различити начини деловања на мрежи (видљиви и невидљиви), доводе до сталне и све веће

размене података, који садрже знатне елементе приватности и који могу бити употребљени, па и злоупотребљени на различите начине.

Оно што произилази из правних прописа, али и из основних правила етичког кодекса и елементарних постулата културе, јесте чињеница да прикупљање података личног карактера, чак и ако се и врши мимо знање клијента, не сме бити злоупотребљено или употребљено у друге сврхе, осим оне за коју је примарно намењено.

Упркос реченом, данас, нема никакве сумње да је приватност у дигиталном свету веома крхка. Другим речима, информациона приватност је редак комодитет у сајбер простору. То је неминовна реалност коју сви путници по сајбер простору треба да знају и у одређеној мери прихвате, како их не би дочекала и изненадила другачија стварност.

Ипак, да би се, колико-толико обезбедила заштита личних података у дигиталном окружењу и тако сачувала приватност појединца, потребно је предузети озбиљне и свеобухватне мере, које ће обухватити комбинацију средстава - законских, политичких, технолошких (снажне мере криптографије), саморегулативних (деонтолошки или етички кодекси и сл).

С обзиром на развој и коришћење савремене информационе технологије, постоје два виђења будућности човечанства. Једно је остварење утопије, а друго је потпуна дистопија. Бројни писци су предвидели у својим делима настајање болесног друштва које зависи потпуно од технике и не обезбеђује својим члановима никакво остварење људскости. Људи би постали киборзи, продужавајући свој живот механичким помагалима али не би имали идеју зашто би продужавали свој живот. Моћ би се налазила у рукама малог броја људи који би контролисали масу тако да ова постаје све мање свесна било чега што није сасвим неопходно. Бројна дела, од Орвелове "1984", преко Гибсоновог "Неуромансера" и Харисоновог "Бил, херој галаксије" нуде слику доминације технике и пропадања људскости.

Друго виђење је карактеристично по томе да предвиђа коришћење технике за остваривање људских тежњи. Слободни од присилног рада људи би своје капацитете могли да окрену ка сопственом усавршавању и повећању добробити целог човечанства.

И једно и друго виђење зависе од начина на који предвиђају да ће људи користити рачунаре. У сваком случају, потребно је остварити једну глобалну организацију која би на принципима информационе етике изградила етички кодекс, а који би поштовали сви информатичари. Постоји тенденција да једног дана готово цело човечанство буде на неки начин уско повезано са информационо-комуникационом техником, да сви једном будемо "информатичари".

У будућности нам тако усмерено понашање можда и помогне да остваримо најсмелије снова своје врсте. Сан о бесмртности може се остварити пребацивањем наших знања и осећаја, наше "суштине" у електронску форму, можда укључивањем свих таквих наших "cyber" душа у једну заједничку мрежу. Ко зна шта се може догодити када би се сви људски умови спојили у један? Постоје бројне теорије које иду од мистике до кибернетике. Можда би то био почетак једне нове ере, као што су давно ћелије почеле да се удружују и граде организме. Можда би се тада умови, као некада ћелије, специјализовали за одређене задатке и заједно сачинили ентитет који би се налазио на вишем нивоу од свесног човека? А можда би принцип сарадње био потпуно другачији. Можда је то природан наставак који следи из удруживања људи у заједнице, које ће упоређене са таквим "супер ентитетом" можда изгледати несавршено и готово бизарно.

У сваком случају, морамо схватити снагу информационо-комуникационе технике и чињеницу да наша будућност највише зависи од начина на који ћемо је користити. Ходамо уском стазом, често сувише близу амбиса, али нада, ипак, постоји. У сваком случају, одлука је само у нашим рукама.

Vidoje Spasić, LLD
Teaching Assistant

SOME ASPECTS OF PRIVACY IN CYBERSPACE

Summary

The privacy issue has always been the focal point of attention in different scientific areas. The problem is multidisciplinary and should therefore be treated and observed from different points of view. The emergence of digital technology has rendered the privacy problem increasingly current and significant. In this paper, the author discusses some aspects of privacy in cyberspace (virtual environment), dealing with its legal, technical and psychological aspects.
Depending on the types of different services offered to users, there are two new forms of threat: the information collected on individuals through "visible" processing, or data collection without individuals knowing anything about it ("invisible processing").
Various items of user-information are collected on-line in uncoded form. This involves either habits observed in chat rooms or newsgroups, e-mail or directories, and e-commerce (including electronic payment). "Invisible processing" includes connection data or "log file", "traffic data" and "cookies."
Protection of personal data in the cyberspace is one of the serious burning issues that must be resolved. Information privacy is a scarce commodity in cyberspace. The technical infrastructure of cyberspace makes it remarkably easy and cheap to collect substantial amounts of information identifiable to particular individuals.
Privacy on the internet and in the cyberspace is in a fragile state. However, there is new hope for its resuscitation. Providing a web protecting the privacy of data and communication requires a unique combination of legal, policy, technical, and self-regulatory tools.

Key words: privacy, internet, cyberspace.