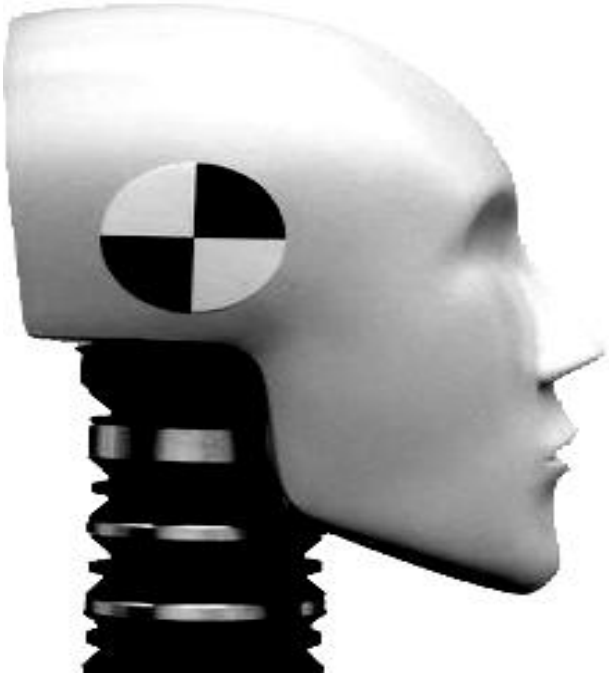
ЗНАМО ЛИ КО СВЕ УГРОЖАВА НАШУ ПРИВАТНОСТ?

Покрет за електронску приватност Србије



Скраћени преглед стручних студија

ПОЛИТИКА ONLINE

Проблем приватности грађана у Србији је комплексан и потпуно сагледив једино из свих стручних аспеката: етичких, социолошких, друштвених, теолошких, правних, информатичких, политичких... итд. У циљу решења проблема приватности треба се осврнути на вредна искуства најразвијених западних земаља где је питање приватности и заштите података озбиљно политичко питање.

www.privatnost-srbija.com

Знамо ли ко све угрожава нашу приватност?

Преглед и извештај о приватности и безбедности података грађана у Србији.

Аутори: Никола Марковић, Александар Ресановић, Драган Ћосић, Александар Арсенин, Александар Загорац, Стеван Лилић, Звонимир Ивановић, Горан Ј. Мандић, Милан Туба, Оливер Суботић, Војислав Родић, Ненад Маринковић, Бранислав Радивојша, Данило Тврдишић, Ненад Вукићевић, Александар Павић, Предраг Радовановић, Јован Валентин Истрати

Уредник: Александар Арсенин, председник Покрета за електронску приватност
Уредник Политиконог издања: Бранислав Радивојша, уредник Политике
Ексклузивно објављено: www.politika.rs/rubrike/Sta-da-se-radi/index.1.sr.html, и у дневним издањима Политике од 03.03 до 19.03.2011.

Садржај:

Мотивисати човека да се бори за приватност

Наслов овог текста је можда и најзвучнија порука са скупа.

Научни скуп на тему приватности грађана у информационом добу одржан је 17. фебруара у Београду у сали 513 Машинског факултета. **Приватност у Србији: привилегија, право или празнина** је назив скупа и питање на које су одговоре дали најеминентнији стручњаци из различитих области.

Циљ скупа је био да се "отвори" тема приватности у Србији и јасно прецизира проблем који је и по закључцима излагача комплексан и свеобухватан. У основним цртама можемо издвојити непостојање свести о приватности, неадекватност закона, недостатак прописа па и кршење постојећих правила - и правних и етичких. Све ово повећава повреду приватности са могућим озбиљним последицама и доводи грађане у велики ризик.

На скупу се коментарисало и о посебно осетљивим подацима као и о високо технолопком криминалу у будућности. Депои који садрже податке о инвалидности, здравственом стању, породичном статусу, евиденције разних пописа, спискова деце у школама, вртићима... итд. су осетљиве информације које свакодневно одајемо.

Неки од основних закључака су: проблему заштите приватности потребно је приступити као ослонцу ширег подухвата - борбе за очување слободе личности, нужно је подизати колективну и индивидуалну свест о значају очувања приватности и садржини тог личног нематеријалног добра, потребно је у рад покрета активније укључити и делатнике из области психологије, социологије, философије и других области ради формулисања што конструктивније и креативније друштвене критике, направити конкретну сарадњу између институција које имају везе са обрадом података о личности, обезбедити размену искустава и у локалним заједницама и у региону уопште, спроводити кампању кроз целокупну едукацију грађана, институција и руководиоца путем медија али и кроз директну сарадњу, обезбедити потребне препоруке и едукативна средства. Основна нит је да брига о приватности и безбедности података не сме да буде вођена

неким друштвеним нормама већ искључиво етичким стандардима који воде ка заштити грађана.

Скупу су учествовали: Александар Ресановић - заменик Повереника за информације од јавног значаја, през. Оливер Суботић - управник центра ЦЕПИС, проф. др. Драган Ћосић, г.Милан Туба... итд, а у публици су биле колеге из МУП-а, техничког и правног факултета (билтен скупа са представљеним учесницима се налази на адреси: http://www.privatnost-srbija.com/mediaCentar.htm).

Поред закључака, зборник радова са овог скупа ће бити квалитетна грађа за едукацију и креирање националне стратегије за очување приватности грађана.

Знамо ли ко све угрожава нашу приватност - Никола Марковић

Наши грађани олако остављају своје податке

Будућност информационог друштва зависи и од безбедности информација и заштите личних података

Грађани свакодневно, где год се кретали и шта год радили, остављају на десетине својих електронских трагова и то: док телефонирају, плаћају робу и услуге, комуницирају са државним органима и јавним службама, користе Интернети сл.

Успостављена је и електронска обрада скоро свих евиденција са личним подацима. Све више евиденција о грађанима се електронски повезује и интегрише како би се олакшало њихово ажурирање и увођење електронских сервиса за потребе становништва. Тиме се, међутим,повећава и опасност од њиховог неовлашћеног коришћења и зато су неопходне мере које би то онемогућиле.

Државни органи, банке, јавна и друга предузећа уводе електронску идентификацију својих клијената и тиме се постављају и нови захтеви за заштиту података о личности.

Расте и примена видео-надзора. Чување и право коришћења тих података није регулисано. Без дозволе субјекта снима се и преко Интернета преноси кретање грађана на улици и сл.

Све је већи број корисника социјалних мрежа (Фејсбук, Твитер и др.) на којима многи остављају своје личне податке. Треба имати у виду и то да у Србији 90 одстоод 1.700.000 корисника Интернетаима профил на Фејсбуку, где по својој вољи остављају многе личне податке.

У маркетиншке сврхе се користеинформације прикупљене од клијената приликом куповине или сурфовања по Интернету. На овај начин може се профилисати личност грађана.

Разне обавештајне службе, адвокатске канцеларије и друге институције пресрећу личне податке или прислушкују грађане, а у неким случајевима податке мењају и уништавају.

Све је више случајева крађе и злоупотребе идентитета који се касније користе при извршењу кривичних дела.

Примена GPS (Global Position System), поред информисања о локацији, може да се користи и за надзор над кретањемљуди.

Има и појава нелегалне продаје и уступањаевиденција са личним подацима.

Важећи закон о електронским комуникацијама дозвољава безбедносним службама надзор над електронским комуникацијама, и то без судског налога. Послодавци евидентирају поједине личне податке који превазилазе потребе кадровске евиденције и задиру у приватност запослених. У појединим компанијама надзиру се комуникације запосленихтоком радног времена. Телевизија снима, а медији пишу о хапшењу осумњичених, угрожавајући тиме њихову приватност и пре него што се утврди кривица.

У свету, а и у Србији, очекује се експанзија угрожавања личних података и зато треба организовати детаљна истраживањао томе и о мерама које се морају предузети.

Грађани код нас углавном олако остављају своје податке приликом куповине, дружења на социјалним мрежама и у разним другим приликама. Многи игноришу постојање опасности од злоупотреба личних података. Топоказуједа код многих од нас постоји мала заинтересованост за заштиту и низак ниво свести о угрожености личних података и приватности.

Како унапредити ту свест? Грађани би приликом давања личних података требало да буду обавештени о правном основу за прикупљање података, о праву на увид у прикупљене информације, о контроли коришћења и другим правима која произилазе из Закона о заштити података о личности.

Приликом добровољног давања података свако би требало да буде упозорен да се подаци могу и злоупотребити. Надлежни државни органи, медији и невладине организације треба да раде на афирмисању и популарисању заштите података о личности и на развоју свести о значају те заштите.

У информационом друштву, коме и наша земља стреми, основни ресурси су информације и знање који се прикупљају, обрађују, чувају и користе применом

савремених информационих технологија. Опстанак и будућност информационог друштва зависе и од безбедности информацијаи заштите личних података.

Председник Друштва за информатику Србије
Никола Марковић
објављено: 04.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Nasi-gradjani-olako-ostavljaju-svoje-podatke.sr.html

Знамо ли ко све угрожава нашу приватност – Александар Ресановић

Рокови прошли, прописа нема

Повереник је извршио надзор над радом 71 руковаоца подацима о личности –у 48 случајева по службеној дужности, у 23 по пријави грађана

Сваки савремени унутрашњи правни поредак мора да штити и приватност грађана. Подаци о личности представљају срж информационе приватности сваког појединца. Прописи којима се уређује обрада и заштита података о личности морају да одговарају реалним потребама и могућностима Србије, али и да су усаглашени са одговарајућим међународним стандардима, пре свега с Конвенцијом СЕ бр. 108. из 1981. и Директивом СЕ бр. 46. из 1995. године. Скоро све европске државе су својим законима на одговарајући начин уредиле ову област још од седамдесетих до деведесетих година прошлог века.

У нашој земљи први закон о заштити података о личности донет је 1998. године, на нивоу СР Југославије. Највећи проблем у вези са овим законом не лежи у чињеници да није био усаглашен с већим бројем тада већ успостављених европских стандарда него у

томе што се уопште није примењивао! И што је још горе, ово није једини закон из области људских права, који је Скупштина Србије усвојила, а који се није примењивао!

Нови закон о заштити података о личности Скупштина Србије је усвојила 2008. године. Овај релативно апстрактан закон је у сваком погледу свеобухватнији и у већој мери усаглашен са савременим европским стандардима него претходни, али има недостатака. Овај пропис је општи, матични закон у области заштите података о личности и садржи начела која би требало да буду разрађена, односно конкретизована великим бројем посебних, секторских закона. Иако је ово уставна обавеза, то се до сада углавном није десило, те само мали број секторских закона садржи одредбе које у потпуности уређују предметну материју. Супротно томе, највећи број секторских закона или уопште не садржи одредбе којима се уређује материја прикупљања, држања, обраде и коришћења података о личности, или садржи одредбе које ову материју уређују непотпуно, односно неодговарајуће.

Влада Србије није донела ни акт о начину архивирања и о мерама заштите нарочито осетљивих података, иако је законски рок за доношење овог акта истекао још у мају 2009, као ни Акциони план за спровођење Стратегије заштите података о личности, иако је рок за то истекао новембра 2010.

Основан је, ипак, независни државни орган – повереник за информације од јавног значаја и заштиту података о личности, који је током 2010. вршио своје законом установљене надлежности. Повереник је извршио надзор над радом 71 руковаоца подацима о личности, од чега у 48 случајева по службеној дужности, а у 23 по пријави грађана. У погледу структуре руковалаца над којима је извршио надзор, највећи је број органа локалне самоуправе (26), затим органа државне управе (22), па руковалаца у области производње, трговине и услуга (8), здравства (5) итд. Повреде закона које је повереник утврдио су: непостојање евиденција о збиркама података и њихово недостављање поверенику (26), прекомерна обрада (8), непримењивање организационих, техничких и кадровских мера заштите (8) итд. Због тога је повереник предузео следеће мере: издао је упозорење на неправилности у обради (29), поднео захтеве за покретање прекршајног поступка (20), поднео кривичне пријаве (18) итд. Такође, повереник је поступао по 45 жалби, поднео предлоге за оцену уставности три закона и др.

Може се закључити да Србија и даље не придаје потребан значај заштити података о личности. С једне стране, не чини одговарајуће напоре да ову област нормативно уреди, а с друге, поверенику не обезбеђује адекватну подршку. Једно време недостатак подршке се огледао у недовољним средствима за рад, затим у неодговарајућем простору, онда у проблематичним покушајима извршне, али и законодавне власти да у извесној мери релативизују овлашћења повереника и утичу на његову самосталност, чиме би могле да отупе оштрицу непристрасног деловања, па даље у непоступању или

неблаговременом поступању по актима повереника, укључујући ту и кривичне пријаве, захтеве за покретање прекршајног поступка, предлоге за оцену уставности и др.

Неспорно је да повереник врши послове заштите података о личности, али сви надлежни органи, организације, установе и др, требало би да се у оквиру свог делокруга рада баве заштитом података о личности кроз унапређивање прописа и њихову пуну примену, као и међусобну сарадњу и сарадњу са грађанима. Надлежни органи требало би да своје напоре усмере и на борбу против свих који не поштују закон и који злоупотребом савремених технолошких решења угрожавају или онемогућавају остваривање права на приватност.

**Заменик повереника за информације од јавног значаја*
Александар Ресановић
објављено: 05.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Rokovi-prosli-propisa-nema.sr.html

Знамо ли ко све угрожава нашу приватност - Драган Ћосић

Прате сваку интернет посету

Када се подаци повежу са личним информацијама које уноси корисник могуће је конструисати детаљан профил потрошача

Нема сумње да су користи од примене савремених информационо-комуникационих технологија многобројне, али постоје и извесне ,,нежељене последице" њихове растуће употребе. Једна од њих тиче се угрожавања приватности. Савремене технологије омогућиле су свеприсутну и перманентну присмотру, формирање огромних база података, невероватно брз пренос личних информација широм света... Правни прописи се споро прилагођавају веома динамичном развоју савремених информационо-

комуникационих технологија. Због тога се и воде широке расправе о реформи правног система како би се спречило нарушавање приватности.

Нагли пад цена и напредак у развоју опреме, у комбинацији са општедруштвеним циљевима као што су борба против криминала и тероризма, довели су до невероватно масовне употребе видео-надзора. Процењује се, наиме, да у савременој урбаној средини човек доживи и до триста снимања дневно од најмање тридесетак такозваних ЦЦТВ система. Велика Британија тренутно у томе предњачи. Само од 2004. до 2007. у овој држави је инсталирано око 4,3 милиона оваквих камера.

Овоме треба додати читав низ електронских система у којима се складиште информације чија злоупотреба може да доведе до нарушавања приватности. То су: електронски системи на граничним прелазима; електронски системи оператера мобилне и фиксне телефоније, који бележе податке о телефонским позивима и СМС-овима; електронски системи засновани на тзв. смарт картицама (све чешће, бесконтактне смарт картице) који се користе нпр. на рампама за наплату путарине или за контролу приликом уласка у поједине зграде; банкарски електронски системи који бележе и обрађују финансијске трансакције; електронски системи у здравству, образовању итд.

Комерцијализација јавних рачунарских мрежа довела је и до наглог пораста обима електронске трговине. Финансијске институције се све више ослањају на нове технологије, али њихова примена доноси и многе проблеме од којих је крађа идентитета један од веома актуелних. Крађом дигиталног идентитета могу да се баве: хакери, непоштени добављачи, бивши незадовољни упосленици итд.

Поред тога, на Интернету се може наћи обиље информација о познатим безбедносним пропустима. Простом употребом неког претраживача чак и просечан корисник рачунара може брзо да пронађе информације о томе како да ,,провали" у разне системе користећи уобичајене безбедносне пропусте. Нападачи могу и да ,,пробију" обезбеђење употребом такозваних аутоматских алата којима се ,,скенирају" мрежни системи: ако уоче ма какав пропуст у систему искористиће га да би неовлашћено приступили мрежи.

Компаније које се баве електронском трговином данас користе моћне технологије за прикупљање података које су у стању да евидентирају сваку посету одређеној интернет локацији, као и све акције потрошача на тој локацији. Када се овакви подаци повежу са личним информацијама које је корисник дужан да унесе приликом регистрације могуће је конструисати детаљан профил потрошача који ће садржати податке о производима који га интересују, о његовим навикама у куповини итд. Овоме треба додати да компаније које се баве електронском трговином у почетку углавном имају проблема са профитабилношћу па су заинтересоване за прикупљање информација о потенцијалним потрошачима. Дешава се да информације о потрошачима буду предмет продаје другим компанијама, а забележено је и то да компаније које су пред банкротством продају

информације о својим клијентима другим компанијама. Због природе Интернета као јавне рачунарске мреже потрошачи не могу знати које су информације о њима прикупљене и како ће те информације касније бити злоупотребљене. Управо је то један од разлога због којег многи потрошачи нису спремни на он-лајн трговину.

Компаније које се баве електронском трговином на Интернету схватиле су овај проблем, а у недостатку одговарајућег регулаторног окружења многе од њих су почеле јавно да публикују своју политику заштите приватности потрошача. Америчка Федерална комисија за трговину је, међутим, открила да се врло мали број компанија придржава властитих стандарда заштите приватности потрошача.

Досадашњи раст електронске трговине говори о томе да недовољна безбедност и приватност трансакција на Интернету за многе није проблем. Ипак, ради се и на заштити потрошача, заснованој на дигиталним потписима, дигиталним сертификатима итд. тако да се успон дигиталне економије тек очекује.

**Проф. др, Београдска висока школа струковних студија*
Драган Ћосић
објављено: 07.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Prate-svaku-internet-posetu.sr.html

Знамо ли ко све угрожава нашу приватност - Александар Арсенин

Са чипом или без чипа - будућност идентитета у информационом добу

Мотивисати човека да се бори за своју приватност је изазов

Електронске евиденције су све чешћа појава у урбаним просторима. Оне могу бити израз тежње да се формира једна аутоматизована структура која без сагласности грађана врши надзор над њиховим кретањем и доношењем разних одлука. С тим што је релативна чињеница када се каже ,,без сагласности", јер пристали смо на документа

која садрже чипове и технологије које нас идентификују у најразличитијим ситуацијама. Можда и невољно пристајемо на електронску идентификацију али приморани смо да поседујемо разна документа. Лична карта као примарни документ, са чипом или без чипа, данас је (још увек) резултат појединачне одлуке грађана, док су скоро сви секундарни документи ултимативно наметнути. То нас доводи у ситуацију да пристанемо на ,,чипове" или да одустанемо од пасоша, управљања аутомобилом и здравственог осигурања. На који начин обичном човеку ова скупа чипизација повећава квалитет живота? Чак и често спомињана привилегија ,,администрација без редова", слабо се примењује. Долазимо до закључка да од система електронских евиденција користи имају само власт и бирократски сервиси.

Практична будућност евиденција само је наизглед у једном обједињеном документу који обухвата све поменуте. Једини проблем је губитак слободе и стварање једног глобалног ,,електронског гулага" који на нас мотри током 24 сата. Прекомерна идентификација у свакодневном животу директан је атак на достојанство личности и право на приватност као основно људско право.

Подршка електронским документима су базе података о грађанима које ,,памте" наше дневне активности. За сада, на појединачном нивоу имамо евиденције пореских обвезника, здравствених осигураника, матичне књиге и разне друге мање или више осетљиве евиденције. Усаглашавањем активности тј. укрштањем разноразних докумената и база података отвара се могућност профилисања на основу најразличитијих критеријума – социјалних, здравствених, политичких..., а обједињени ,,папир" ће бити недостајућа веза за ,,освежавање" података на дневном нивоу. Такође, такав документ пружа могућност дискриминације по свим могућим критеријумима у потпуно аутоматском – роботском систему ван свих етичких и хуманих норми. С проблемом системске дискриминације и данас се суочавамо, а његова моћ ће се умножавати до неслућених граница.

С обзиром на могућност избора основног документа, личне карте, без чипа, закључујемо да иста могућност треба да постоји и у случају секундарних докумената, и за то нема препреке. Важећа директива ЕУ (2006/126/EEC) не намеће чип већ националним законодавствима препушта одлуку. У том правцу имамо и вредна искуства развијених земаља које одбацују биометријске концепте у документима као непожељне. Од 11. септембра 2001. до данас имамо и практичне студије које говоре супротно од антитерористичких стратегија које су у вези са масовном аутоматском идентификацијом и надзором.

Приватност грађана у савременом свету постаје питање слободе живљења. Навика да свој дигитални траг немарно остављамо за собом није ништа ново; многи ни не размишљају много о томе. Личне податке нам узимају свакодневно, фотокопирају наше личне карте, а често нас пописују и класификују уз нашу сагласност. Свест грађана о

личној приватности је на ниском нивоу, а одговорност институција које прикупљају и обрађују податке постоји у ретким случајевима, на шта и званичници упозоравају. Када сагледамо проблем можемо закључити следеће: мотивисати човека да се бори за своју приватност је изазов модерног друштва.

Огроман потенцијал је у медијима који могу публиковати ријалити забаву или вратити традиционалне вредности на сцену, о чему се говорило и на недавном научно скупу одржаном у организацији Покрета за електронску приватност.

Председник Покрета за електронску приватност
Александар Арсенин
објављено: 08.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Sa-cipom-ili-bez-cipa.sr.html

Знамо ли ко све угрожава нашу приватност - Александар Загорац

Добровољци угрожене приватности

Покушавају да увере јавност да се неопходне слободе могу очувати ако се жртвују оне које „нису неопходне”

Нимало занемарљив број људи у нашем друштву сматра да је одбрана личне приватности донкихотовски подухват.

Ипак, преко упрошћених закључака типа ,,они могу да нас прислушкују како хоће, какве везе има шта пише у закону, а ако од тога може да буде какве користи, да се путује без виза и слично, утолико боље...” не би требало олако прећи. Такви ставови, ма колико неутемељени, значајни су као показатељ поља на које би требало проширити наше деловање како бисмо постигли циљ: подизање нивоа свести о садржини нематеријалног личног добра које називамо приватношћу, као и разлозима, начинима и нужности њене све веће заштите у условима савременог технолошког развоја.

Глобални процеси прерастања индустријске у постиндустријску (потрошачко-информатичку) цивилизацију допринели су и стварању свести о личном идентитету савременог човека. Уколико не размотримо те процесе и не формулишемо ваљану стратегију излажемо се опасности да наши напори буду у најширој јавности доживљени као донекле елитистички, то јест они који са ,,стварним животом" немају превише додирних тачака. Размислимо још једном о ,,аргументу" који је приликом доношења Закона о заштити података пласиран у јавности као кључни: ,,Битно је да више не чекамо у редовима за визе, то ће нам олакшати живот".

Или, погледајмо шта се дешава у САД, у којој је из једне намерно нетачно протумачене реченице Бенџамина Френклина изведена незванична доктрина о подели људских слобода на оне које су неопходне (essential) и оне које то нису (non-essential). Тако су поборници идеје о ,,домаћој безбедности", као новом одбрамбеном концепту утемељеном на Патриотском закону, који је донет после терористичког напада 11. септембра, успели да увере јавно мњење да се неопходне слободе могу очувати само ако се жртвују оне које нису неопходне, а међу којима је и право на неповредивост садржине личне комуникације у најширем смислу.

Пример за то је и породица из Оклахоме која се добровољно подвргла имплантирању РФИД чипа под кожу, уз образложење да се тако осећају безбедније, јер их у случају терористичког напада полиција може врло лако пронаћи.

Указивање на чињеницу да политичко-технолошки притисци иду ка томе да претежан број људи добровољно пристане на жртвовање личне приватности, већ се може сматрати општим местом. Стратегија ,,штапа и шаргарепе" ту је јасно уочљива: са једне стране, нуде се бројне погодности, нпр. једноставнији прелазак из државе у државу, олакшано обављање новчаних трансакција електронским путем и слично, а са друге стране се интензивира страх од терористичких напада и других драстичних видова криминалног понашања, како би се становништво подстакло на добровољно подвргавање све агресивнијој контроли.

У Србији су поменуте тенденције још увек у повоју, но ипак су јасно препознатљиве: почев од идеје о увођењу јединственог електронског документа па до бежичне технологије за праћење лица која поседују такав документ и чињенице да допуштамо таквим и сличним наметањима готово несметан продор у сферу наше личне и колективне егзистенције.

*Потпредседник Покрета за електронску приватност
Александар Загорац
објављено: 09.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Dobrovoljci-ugrozene-privatnosti.sr.html

Знамо ли ко све угрожава нашу приватност - Стеван Лилић

Интернет доспео до петине

У 1988. години број корисника Интернета износио је један милион, а у 2009. - 1,5 милијарди или 21,9 одсто светске популације

Једна од ранијих дефиниција приватности формулисала се као „право да се буде остављен на миру". Савремене дефиниције приватности стављају нагласак на тзв. контролу информација. Конкретно, то значи да кључно питање постаје ко и како контролише Интернет. Цео свет имао је недавно прилику да види покушаје режима да спречи употребу мобилних телефона, видео-снимака и „социјалних интернет мрежа" (Гугл, Фејсбук, Јутјуб, Твитер) у протестима у Египту и другим земљама Блиског истока.

У развијеним земљама, ситуација тзв. релативне информационе изолованости појединца последњих година битно се променила. Ово је последица изузетног развоја компјутерске технологије уопште, а нарочито спектакуларног развоја технологије за тзв. електронско праћење и надзор понашања појединца. Статистика показује да је број корисника Интернета у 1988. години износио један милион, док је у 2009. забележено 1,5 милијарди корисника, што чини 21,9 одсто светске популације.

Србија је једна од ретких земаља која све до 2008. године није донела посебан закон који уређује заштиту података о личности. Додуше, постојао је савезни закон из 1998. године који је био усклађен са Конвенцијом Савета Европе о заштити лица у односу на аутоматску обраду личних података (1981), али није био усклађен са Директивом 95/46/ЕЗ Европског парламента и Савета о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података из 1995. године. Као правни следбеник некадашње СРЈ, и касније СЦГ, Србија се нашла у ситуацији да формално

има, али да фактички нема закон о заштити података о личности. Осим тога, када су преношене надлежности савезних органа на органе Србије није био одређен орган који би преузео надлежност за спровођење овог савезног закона, па се овај пропис у Србији није ни примењивао.

Устав Србије из 2006. године (чл. 42) гарантује заштиту података о личности. Да би се она могла ефикасно обезбедити било је неопходно донети нови закон, који би, у складу с важећим стандардима ЕУ, обезбедио ефикасну заштиту приватности. У међувремену, донети су закони који су у непосредној вези с подацима о личности (о личној карти, путним исправама и др.). Осим тога, и многи други закони у Србији уређују податке о личности (нпр. прописи из банкарског сектора, пензијско-инвалидског и здравственог осигурања, заштите здравља, безбедности, телекомуникација, образовања, радних односа, оглашавања и рекламирања, архивске грађе, тржишта хартија од вредности и др.). Коначно, постоје и веома важне области у којима још нису донети одговарајући прописи којима се уређује заштита података о личности (тзв. директни маркетинг, видео-надзор, употреба биометријских података у личним документима...).

Важан корак у заштити личних података у Србији учињен је усвајањем Закона о заштити података о личности у октобру 2008. Садашњи закон, међутим, није у потпуности усклађен с релевантним европским стандардима, посебно с Директивом 95/46/ЕЗ (о заштити физичких лица у погледу обраде личних података и слободног кретања тих података). У Извештају ЕУ о напредовању Србије за 2009. годину (§ 4.3.6) наводи се да је: „остварен одређени напредак по питању заштите података о личности. (...) Међутим, закон није у потпуности усклађен са стандардима ЕУ. Генерално, Србија је умерено напредовала у области заштите података о личности".

Постојећи законски оквир заштите података о личности треба да буде допуњен новим одредбама који ће обезбедити основне регулаторне смернице у „посебно осетљивим областима заштите личних података", као што су: национална безбедност, одбрана, кривично правосуђе; медицински подаци; медији, уметничко и књижевно изражавање; телекомуникације и Интернет; биометрија; видео-надзор; банкарство и финансијски подаци; политички избори; директни маркетинг; електронски документи и електронски потпис; агенције за физичко-техничку заштиту, овлашћења приватних детектива ...

*Професор универзитета, председник Удружења „Правници за демократију"
Стеван Лилић
објављено: 10.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Internet-dospeo-do-petine.sr.html

Знамо ли ко све угрожава нашу приватност - Владимир Урошевић; Звонимир Ивановић

Удар на платне картице

,,Пецање" изгледа овако: на електронску пошту корисника банке стиже порука да се преуређује база података и да прималац треба да унесе податке на ,,линк банке"

Главни циљ већине интернет страница електронских продавница је продаја производа и услуга. Ови интернет сајтови су углавном интерактивни. Контрола над њима се преузима на много начина како би се компромитовале базе података ради прибављања информација о клијентима. Најчешћи и најопаснији су напади тзв. SQL инјекцијама, када се у базу убацује неколико података или програмски код који истражује слабости у заштити саме базе, да би се оне затим несметано злоупотребиле ради крађе података о платним картицама.

Године 2008. једно предузеће са територије Србије које води успешну електронску продавницу на Интернету поднело је кривичну пријаву због основане сумње да је неидентификовани извршилац извршио кривично дело фалсификовања и злоупотребе платних картица (чл. 225 КЗ) и рачунарске преваре (чл. 301 КЗ). После провера је утврђено да је извршилац наведених кривичних дела прибавио електронске податке о платним картицама и идентитету њихових власника употребом ,,SQL инјекција" које је користио за нападе на слабо заштићене базе података на серверима електронских продавница – са подручја Аустралије. Поред података о бројевима платних картица, типу картице, имену и презимену корисника, извршилац кривичног дела је прибавио и друге информације (пребивалиште и електронска адреса власника, својство на основу

којег се име корисника налази у бази података електронске продавнице). Био је у могућности и да сазна укупан број платних картица чији се подаци налазе у самој ,,SQL бази" електронске продавнице.

Фишинг (Phishing) је такође један од честих видова прибављања поверљивих личних, финансијских и других података. Реч је о активностима којима неовлашћене особе коришћењем лажних електронских порука преко електронске поште и лажних интернет страница финансијских институција наводе кориснике Интернета на откривање поверљивих података као што су јединствени матични број, корисничко име и лозинка, ПИН број картице, број кредитне картице и слично. За овакве нападе користе се електронске поруке као што су: 1. лажна упозорења банака да ће доћи до гашења рачуна ако клијент не ажурира податке, 2. лажне поруке администратора у којима се траже кориснички подаци, нпр. лозинка, 3. поруке у којима се позива на безбедност и захтева од корисника откривање личних података ради отклањања откривеног безбедносног пропуста, 4. поруке којима се корисник обавештава да је ,,добио на лутрији", због чега треба да достави личне податке.

Да би се клијент ,,упецао" често се користе линкови који по називу личе на праве адресе банака, а заправо се налазе на сасвим другој адреси, док изглед интернет презентације у потпуности одговара правој интернет страници банке.

У принципу, ,,пецање" изгледа овако: на електронску пошту корисника одређене банке шаље се порука да се нпр. преуређује база података банке и да је потребно да прималац унесе своје податке на ,,линк банке". Линк је, наравно, лажан, тј. води на лажну страницу банке.

Опрез корисника услуга банака, кад је о ,,пецању" реч, данас је већа, па су и извршиоци кривичних дела приморани да употребе нове технике.

Током 2009. године неколико предузећа са територије Србије поднело је кривичне пријаве за кривична дела фалсификовање и злоупотреба платних картица (чл. 225 КЗ) и рачунарска превара (чл. 301 КЗ), против неидентификованих извршилаца. Утврђено је у једном случају да је извршилац преко Интернета прибавио податке о више десетина електронских адреса клијената Вестерн унион банке која је била постављена на сервер под његовом контролом, а он је затим слао ,,спам" поруке у којима је од корисника банке тражио да преко лажног линка посете наводне странице Вестерн унион банке ради ажурирања података. Тако су клијенти банке несвесно слали своје податке директно извршиоцу кривичног дела.

У Србији су регистровани и ,,фишинг" напади на кориснике услуга Интернета преко ,,спам" порука у којима су се извршиоци кривичних дела представљали као ,,интернет провајдери" и тражили податке ради ,,ажурирања базе података".

Оваквих и сличних случајева било је и у 2010. години, а све чешће жртве преваранта су и наши држављани који плаћају преко Интернета.

Проблематика о којој је овде реч веома је специфична, а неукост грађана може имати несагледиве последице по њихову приватност и имовину.

**Криминалистичко-полицијска академија

*Одељење МУП за борбу против високотехнолошког криминала

Звонимир Ивановић**
објављено: 11.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Udar-na-platne-kartice.sr.html

Знамо ли ко све угрожава нашу приватност – Горан Ј. Мандић

Нове мале справице за прислушкивање

Хардверски килогер може да снима све што је унесено преко тастатуре компјутера

Опрема за прислушкивање данас је релативно лако доступна. До ње се најлакше долази наручивањем и куповином преко Интернета. Прислушкивање се сад своди на то да у неком простору оставите неки предмет са скривеном електроником. И – имаћете и аудио и видео записе.

Мобилна телефонија се може користити у те сврхе. Поклони вам, рецимо, неко неку фигурицу, привезак и слично, а то може, у ствари, да буде ,,једносмерни" мобилни телефон који има у себи картицу. И када се успостави веза – чује се разговор у простору где се поклоњени предмет налази. Основни проблем код тих малих уређаја је извор

напајања. Они који немају константни извор напајања, у зависности од експлоатације, релативно брзо престају да функционишу. С тим што извор напајања може да буде и „трајни" извор: у сат је, рецимо, уграђен уређај за прислушкивање и тај уређај користи исту батерију као и сат.

Аудио-видео надзор је дозвољен у објектима у којима власник о томе, ознаком на улазу, обавештава посетиоце. Али и у тим ситуација важно је како се снимљени материјал касније користи, односно ко је од стране правног ентитета овлашћен за његово чување и прегледање. Ови снимци се могу уступити само овлашћеним лицима МУП-а уз легитиман налог у случају да могу да помогну у расветљавању неких кривичних дела. У свим другим случајевима власник не може да их користи нити објављује, осим уз сагласност онога ко је снимљен.

Међутим, ако је реч о туђем простору наравно да је снимање забрањено јер се нарушава интегритет простора и угрожава приватност.

Аудио-визуелно снимање физичка лица користе релативно ретко, за разлику од правних лица која на тај начин долазе до поузданих информација о конкуренцији. У те сврхе се користе и „поклоњени" мобилни телефони с програмом који омогућује да сви СМС-ови и сви разговори буду доступни и некоме ко је удаљен десетинама километара.

Сад се још више злоупотребљава компјутерска опрема. Користе се такозвани хардверски килогери, мали уређаји који се стављају између тастатуре и кућишта компјутера. Уређај ће бити ,,прикачен" ако неко ко то намерава само на тренутак буде сам у просторији и хардверски килогер који ће снимати све што је унесено преко тастатуре компјутера. Затим ће онај ко је тај килогер ,,прикачио" за две-три недеље доћи да га ,,откачи". Али сад је та справица препуна снимљеног материјала. До хардверског килогера је и код нас могуће доћи помоћу Интернета. Оправдање за легалну продају ових мини уређаја може бити заштита докумената у компјутеру у случају да цео систем потпуно ,,откаже".

Постоје и хардверски килогери који користе бежичну интернет-мрежу. Справица може да буде тако подешена да свака 24 сата шаље на унапред унесену интернет адресу све снимљене податке.

Тешко је говорити о томе колико су хардверски килогери код нас у употреби и колико се уопште злоупотребљавају разни уређаји за аудио-видео прислушкивање. Код хардверских килогера посебан проблем је и у томе што га заштитни програми не региструју, јер не користи ресурсе компјутера, осим напајања.

Кад је реч о прислушкивању којим се баве државне службе, претпоставља се да оне то увек раде легалним путем, на основу одговарајуће дозволе. Снимљени разговори политичара са простора бивше Југославије, које смо протеклих година слушали у

медијима, такође се подразумевају. Логично је било да су се разговори тада снимали по њиховим налозима, независно од тога да ли је микрофон био испред њих или није. Друго је питање ко и у ком контексту те снимке касније користи.

Наивно је, међутим, веровати у то да код нас ,,неке службе" прислушкују велики број грађана. Такав поступак је противзаконит а за то нема никаквих ни објективних, ни субјективних разлога. Поред тога реч је о сложеном „послу" који би захтевао релативно велике и људске и материјалне ресурсе и био би изузетно ризичан по легитимитет и углед служби.

Ипак, предострожности ради, због могућег прислушкивања, поклоне пословних партнера, у које је могуће уградити електронска средства за прислушкивање, не треба користити. Такође, не треба некоме омогућити да сам буде у вашем пословном простору. И треба спроводити проактивне мере заштите које умањују могућност угрожавања приватности. Оне су резултат политике безбедности која постоји на нивоу предузећа (установе), али и део су понашања сваког запосленог. То је сложен механизам који омогућава предузећу да заштити информације од значаја за пословање. Код нас се о томе, по правилу, слабо води рачуна па се дешавало да су они који су куповали предузећа знали много више о њима него они који су их продавали.

**Факултет безбедности БУ*
Горан Ј. Мандић
објављено: 12.03.2011
http://www.politika.rs/rubrike/Sta-da-se-radi/Nove-male-spravice-za-prisluskivanje.sr.html

Знамо ли ко све угрожава нашу приватност - Милан Туба

Одбрана и последњи дани

Хиљаде дигиталних камера са сваког крова и бандере су нешто сасвим друго

Док су људи имали векове за прилагођавање баруту и деценије за авионе, само неколико година за прилагођавање мобилним телефонима, Гуглу и дигиталним камерама оставља нас потпуно несвесним да смоугрожени, односно не само да нам је угрожена приватност већ и цела цивилизација какву познајемо.

Пре двадесетак година експериментисало се са електронским наруквицама којима се у сваком тренутку прецизно одређује локација носиоца. Као и обично, почело се „за опште добро" контролом мрских нам преступника (мала борба против тероризма), после се прелази на контролисање запослених у фирмама, на крају ће свако морати стално да носи такву наруквицу, огрлицу, шта нам већ пропишу. Тај орвеловски концепт је нажалост већ увелико превазиђен. Сви данас добровољно носе мобилни телефон, све више је цео живот организован око њега, а већина људи није свесна да су не само позиви, поруке па и разговори, већ и локација записани и сачувани заувек.

Гугл је постао део живота, њему се обраћамо када бирамо кафану, купујемо резервни део за ауто, тражимо адресу хотела или лекара, а сваки наш покрет по тастатури заувек остаје записан. Анализом места на Интернету која смо посетили, шта смо и колико дуго гледали, „они" знају о нама више него ми сами. Људи су донекле навикли на камере у продавницама, али хиљаде дигиталних камера са сваког крова и бандере су нешто сасвим друго.

Резултати оваквог система су стравични јер проблем није само у тој тоталној контроли, она је само средство, прави проблем је какав се антиљудски и антицивилизацијски социјални инжењеринг тиме намеће. Недавно је код нас медијски експониран случај, иначе јако уобичајен у тзв. демократским земљама, одузимања деце неким нашим људима у Америци на скоро годину дана због фотографија деце у кади.

Блажи пример сличне наопаке идеологије су наше зимске аутомобилске гуме (додуше строже код нас него код Словенаца, али ваљда су наше равнице опасније). Када прогутамо зимске, биће и пролетње и јесење, лако ће се наћи „стручњаци" који ће нас плашити опасним разликама између пролећних и јесењих киша од којих ћемо, не буду ли нас баш они мудро водили, сви изгинути. Тај болесни систем наопаке регулације свега и свачега, увлачења у сваку пору живота и непрекидног драконског кажњавања за измишљене преступе (ко прекорачи нацртану линију на стадиону ићи ће пет година у затвор) уништава смисао људског живота. Наметаче ненасиља сталним насиљем разоткрио је још чика Јова: „... Говорио патак о врлини мира и да нико никог не треба да дира, ... Слога, мир и љубав благослов је прави, зато нека нико никога не гњави. ... Један жабац мали поближе је стао, а патак га зграби, па га прогутао. Из овог се нешто и научит' даде: хуље лепо зборе, ал' нитковски раде."

У светлој будућности, снабдевени најмодернијим личним картама и поштанским сандучићима у свету, када дође пропис да носимо шерпу на глави, сви противници јединог пута биће већ на заслуженој робији и демократске двопартијске дискусије водиће се само о томе која је шерпа боља. Усрећитеља је било одувек, ново је што се нећете моћи сакрити и саботирати прогрес, бићете снимљени, пронађени и кажњени, а ако не платите одмах (ту казну или ТВ претплату онима који су вас недавно учили да не треба плаћати) премудра држава преко главатог господина, када вас је већ ослободила деце, породице, запослења и хлеба, ослободиће вас и стана. Ништа ново, Кочићева дијагноза још у пунијој мери важи: милина нека, ненасиље и људска права проширили су се и притисли да се више не може дисати. А тероризма и очајника све више…

**Професор универзитета*
Милан Туба
објављено: 14.03.2011
http://www.politika.rs/rubrike/Sta-da-se-radi/Odbrana-i-poslednji-dani.sr.html

Знамо ли ко све угрожава нашу приватност - Оливер Суботић

Мотивисати људе да се боре за своја права

Основна улога верских заједница када је реч о заштити приватности је посредног типа

Када је пре седам година Српска православна црква отворила јавну дебату у погледу биометријских система идентификације, а потом изашла и са сопственим виђењем те проблематике, многи су се упитали о чему је заправо реч и какве везе ова тема има са православним хришћанством. А ствар је била крајње једноставна: верници (али и многи атеисти) тражили су одговоре на питања којима се тада ниједна озбиљна друштвена институција није на одговарајући начин бавила. Данас, када постоји Покрет за електронску приватност и када све више универзитетских професора проучава поље приватности, потреба да било која верска заједница отвара сличне теме у јавности је неупоредиво мања. То је стога што су носеће структуре дискурса приватности у савременом друштву грађанске иницијативе и академска заједница. Они треба да објашњавају различите аспекте приватности, откривају механизме њеног нарушавања и да обавештавају (а по потреби и покрећу) ширу јавност. Да ли то онда значи да верске заједнице немају шта да допринесу у целој причи? Такав закључак би свакако био брзоплет.

Верске заједнице могу допринети афирмацији права на приватност на више начина. На првом месту, важно је да препознају то право као цивилизацијску тековину и да му дају отворену подршку. Други вид доприноса је на нивоу сопствене доктрине – Московска патријаршија је, примера ради, у допуњеној верзији своје социјалне концепције у одељку о грађанским правима недвосмислено упозорила на проблем масовног прикупљања и обраде података о личности. Трећи допринос који верске заједнице могу дати у вези је

са директним учешћем у јавној дебати када је то потребно, управо као што је то учинила СПЦ пре неколико година.

Но основна улога верских заједница када је реч о заштити приватности је посредног типа и односи се на карактер људи на чије формирање оне утичу, јер није проблем то како уочити механизме нарушавања приватности, већ како мотивисати људе да се боре за своја права. Српска православна црква је по броју припадника доминантна у Србији – уколико у наредним деценијама успе да формира вернике са чврстом вољом, подвижничким стилом живота и изграђеним осећајем за друштвену одговорност, то ће по природи ствари бити огромна брана свим антицивилизацијским токовима на овим просторима, а самим тим и препрека неконтролисаној пролиферацији технологија надзора. Дакле, кључ целе приче је у формирању критичке свести што већег броја људи у друштву.

Одличан пример како упорна иницијатива једне одважне личности може да уроди плодом је случај мајке Џој Робинсон ван Гилдер из градића Ервила у Илиноису која се 2005. године успротивила обавезном узимању биометријских отисака од њене деце у школи за услуге коришћења школске мензе. Она је покренула иницијативу за одбрану приватности своје и друге деце у школама. Резултат двогодишње борбе коју је иницирала и предводила ова храбра жена је било законско решење које је потписао гувернер Илиноиса лично, по коме родитељи морају бити питани за пристанак пре евентуалног узимања биометријских података од њихове деце.

На крају, треба приметити да приватност данас није нарушена из једног центра моћи – орвелијанска парадигма је одавно превазиђена. Реалност је мрежа хетерогених чворова надзора: државне службе, корпорације, приватни сектор и агенције за агрегирање података, а све уз подршку мас-медијског апарата. Одговор на такву парадигму у својој структури такође мора бити полицентричан и хетероген, при чему централна позиција припада грађанским иницијативама и академској заједници, док подршка верских заједница треба да буде примарно на нивоу формирања личности чврстог карактера.

Кључна борба се води на пољу свести, воље и критичког осећаја „обичних" грађана. Исход те борбе одлучиће победника.

*Управник Центра за проучавање и употребу савремених технологија Архиепископије београдско-карловачке
Оливер Суботић
објављено: 15.03.2011.

Знамо ли ко све угрожава нашу приватност - Војислав Родић

Шта све може Интернет!

Домови који нису имали присуство на Интернету нису били разматрани

„Хоћеш ли ми писати?", „Наравно да хоћу, сваки дан".

Овакви разговори су се често чули на сурчинском аеродрому почетком деведесетих, када смо испраћали бољи део наше будућности, који ће највећи (и најпродуктивнији) део живота провести у иностранству. Прва разгледница би стигла са аеродрома у Цириху или Франкфурту. Онда би уследила прва писма о томе како је у „новом крају", у почетку једном недељно, па месечно, па једном у три месеца, па у шест месеци....

Свакодневне обавезе су остављале све мање времена за писма онима који су остали код куће. Празнину у срцу је било тешко надоместити, а сећања су бледела са неумитним протоком времена.

А онда су се половином деведесетих појавили први интернет провајдери и покидане везе су се обновиле са потпуно новим квалитетом комуникације. Могли смо по повољној цени да размењујемо поруке које су испоручиване тренутно. И то не само текстуалне поруке, већ и фотографије. Како се годинама повећавао домаћи садржај на Интернету, тако је расло и интересовање наше дијаспоре за све аспекте нашег присуства на Интернету – почев од сајтова информативних кућа па до комерцијалне понуде производа и услуга.

При том не мислимо на физички „извоз", већ на чињеницу да су „наши у белом свету" своје одлуке о трошењу новца у Србији све више базирали на директном увиду у понуду преко домаћих веб-локација. У 2009. години (и поред светске кризе) укупне дознаке наше дијаспоре износиле су 5,5 милијарди долара, што је тада било 15 одсто бруто друштвеног производа Србије и више од 50 одсто српског извоза!

Захваљујући управо Интернету, многи локални понуђачи производа и услуга су, задовољавајући потребе домаћих потрошача, остваривали извоз, а да често тога ни сами нису свесни. Син који из Аустралије долази у Србију да би за мајку пронашао одговарајући смештај у дому за старије особе, пре доласка прегледао је преко 25 сајтова разних домова, направио ужи избор и по доласку за два дана обишао пет који су задовољавали критеријуме. Домови који нису имали присуство на Интернету нису били разматрани.

Један други син живи већ 35 година у Америци и жели да преко Интернета плаћа рачуне за своју мајку која живи у Србији и да је поштеди стајања у реду или одласка у пошту (банку). Али ниједно комунално предузеће (ЕДБ, Инфостан, Телеком, кабловски провајдер) не прима уплате преко Интернета. Решење је опет пронађено управо на Интернету. Мајка је овластила сина на динарски рачун у локалној банци и он преко Интернета из Њујорка плаћа рачуне комуналних услуга са рачуна у банци у Србији. Али како да зна колико да плати, када рачуни стижу у поштанско сандуче његове мајке у Србији? Сва поменута предузећа омогућавају увид у ажурне копије рачуна на Интернету, тако да можете да видите све ваше рачуне и пре него што их поштар донесе на вашу адресу.

Уз прилагођавање финансијских прописа огромне уштеде (финансијске и еколошке) могле би да се остваре само у томе што се рачуни не би штампали и дистрибуирали оним потрошачима који би се изјаснили да за потребе њихових рачуна више не морају да се секу шуме. А када би комунална предузећа омогућила уплате банкарским и кредитним картицама преко Интернета, то би био додатни ,,извоз услуга", првенствено нашој дијаспори.

Проблеми сигурности интернет корисника, као и заштите њихове приватности су од врхунског значаја у виртуелном свету, у коме и искусни корисници, једним брзоплетим „ кликом" могу да дођу у врло неугодне ситуације.

Предности коришћења интернет сервиса су исувише велике да би их се одрекли због ових претњи. Технологија је неутрална – ни добра ни лоша, од нашег начина коришћења зависи какав ће бити друштвени ефекат употребе напредних интернет сервиса.

објављено: 16.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Sta-sve-moze-Internet.sr.html

Из славине или на бунару

Замислите данас да покушавате да комуницирате са пословним партнерима само преко телефона, факса и курирске службе

Пре пола године вест дана била је да је Делта ерлајнз прва авио-компанија у свету која је почела да продаје карте преко Фејсбука. Мање је познато да код нас можете преко Фејсбука да резервишете смештај у једном хотелу код Ивањице, а претходно се детаљно упознате са свим садржајима који су доступни у хотелу и изузетној природној околини и на Фејсбук зиду „поразговарате" са директором маркетинга.

У америчким школама су се управо на друштвеним мрежама (Фејсбук) појавили нови облици ђачког мобинга, по много чему неупоредиво тежи од оног на који смо се већ (нажалост) навикли. Разлика је у томе што се од виртуелног мобинга не може побећи – ако се ученик упише у другу школу (са жељом за нови почетак), у новом одељењу ће га одмах препознати по профилу на друштвеној мрежи који га прати много комплетније и свеобухватније него некадашње „карактеристике" од којих смо ,,стрепели" пре 40-50 година.

Пре него што олако „забраните" коришћење друштвених мрежа (што је и технички неизводљиво) размислите о томе да иста технологија може да се употреби на сасвим другачији начин. Учитељица разредне наставе у основној школи у Панчеву користи Фејсбук странице да многе педагошке активности повеже и са децом и са њиховим родитељима. На њеном друштвеном профилу су обавештења о: распореду часова, променама смене, родитељским састанцима, систематским прегледима, такмичењима и резултатима такмичења, позоришним и биоскопским представама, важним стварима које треба да се понесу у школу и слично.

Када је земљотрес погодио Краљево (3. новембра, у два сата ујутро), корисници Твитер друштвене мреже су прве информације о томе имали од других твитераша после седам минута, много пре него што су обавештење добили од било ког јавног медијског сервиса. Једна банка је преко своје Фејсбук странице организовала одлазак добровољаца на викенд-рашчишћавање рушевина у Краљеву, а „Лајк" је служио да се пријавите за одлазак (банка је плаћала превоз).

Можемо ли да замислимо да се лишимо Интернета? Они старији, којима се Интернет појавио у зрелом животном добу, вероватно и могу много лакше од млађих, који не знају да је постојало и време у коме широкопојасни Интернет није био део уобичајене стамбене инфраструктуре. Као што ни аутор ових редова не може уверљиво да замисли да се вода не добија из славине, већ да се по њу мора ићи у двориште на бунар, што је била реалност многих из претходне генерације. Тако би без Интернета опет слали писма нашим исељеницима, рачуне би плаћали само у пошти и банци (па какав год да је напољу кијамет), родитељи би се виђали са учитељицом на родитељским састанцима и у дану отворених врата, авио-карте бисмо куповали само у пословницама и туристичким агенцијама...

Наш привреда, која је део глобалне привредне инфраструктуре, не само да не би била конкурентна већ би била скоро потпуно онемогућена у функционисању. Замислите данас да покушавате да комуницирате са пословним партнерима само преко телефона, факса и курирске службе? Пре него што бисте поштом (факсом) и примили захтев за понудом, ваш потенцијални купац би своју набавку извршио код неког другог. Док бисте ви ујутро чекали да вам курир донесе извод из банке у коме је извештај о томе шта се јуче дешавало на вашем рачуну, ваша конкуренција би у реалном времену вршила робно-новчане трансакције.

Опасности, које нам реално прете у виртуелном свету, нису ни у чему преувеличане, у том погледу будућност је много црња него што сада можемо и да претпоставимо. Све то није разлог да се одустане од коришћења свих интернет сервиса (чији број непрестано расте) него управо мотивација да се сталном обуком оспособљавамо за безбедно коришћење Интернета, јер је то услов нашег економског опстанка.

Ипак, повремено прошетајте парком вашег кућног љубимца у off-line режиму...

Директор И Нет доо
Војислав Родић
објављено: 17.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Iz-slavine-ili-na-bunaru.sr.html

Знамо ли ко све угрожава нашу приватност - Ненад Маринковић

Истина или претеривање

Да ли неко зна за било које откриће које нема своју двоструку намену

Приватност појединца, заштита података, поверљиви досијеи у архивама државних установа и приватних предузећа појмови су које је лако изрећи и позвати се на њих наводећи низ случајева када су неке информације злоупотребљене, а грађанима нанета штета.

Нажалост, ретко ћемо чути да постојање истих података, њихова повезаност итд. многима од нас доноси корист. Да ли је корист од тога мања или већа од штета о којима се са тако пуно енергије пише?

Не треба бити економски стручњак да бисмо претпоставили колико уштеда у раду разних установа, а и прихода предузећима доносе разне базе података; колико се скраћује време чекања за решавање појединих захтева, колико се лакше стиже до власничких листова; колико се, захваљујући Интернету, роба брже продаје...

Да ли, на пример, можете претпоставити колико времена је потребно да бисте у Србији купили боцу вина из Аргентине? Данас за само неколико десетина минута или за сат-два можете наручити, платити картицом, добити потврду банке о успешно обављеној трансакцији. Преостаје само да у наредних неколико дана вино стигне у Србију по смешно ниској цени. Међутим, на тој путањи постоје многе тачке које су повезане с давањем личних података банци, интернет провајдеру, продавцу робе, МУП-у и ко зна још коме. Да ли се одрећи вина или давања података? Велики број грађана Србије вероватно би се одрекао аргентинског вина јер су и наша одлична, али није тако у многим другим ситуацијама.

Рецимо, узимање кредита код банака, било у виду новчаних готовинских кредита, било у виду кредитних платних картица. Колико корисника банкарских кредита је дало своје податке: матични број, адресу, просечна месечна примања, место становања, број чланова породице. Да ли је неко тужио пословне банке због прикупљања оволике количине информација и угрожавања приватности? Број издатих платних картица мери се милионима чак и у сиромашним и релативно малим земљама као што је Србија, а број радника пословних банака који могу да располажу овим подацима све је већи и већи.

Недавно је на једној интернет страници објављен снимак камере МУП-а за видео надзор саобраћаја на аутопуту који приказује сцене са паркинга поред београдске ,,Арене". Да су на том снимку којим случајем били неки од оних који позајмљују аутомобиле широм Београда, технологија даљинског осматрања града била би слављена. Овако су сниматељи забележени као ,,воајери", а снимак је послужио као аргумент више за смањење употребе видео-надзора.

Темом приватности бавили су се и многи уметници, сетимо се само ,,Балканског шпијуна", ,,Професионалца", филма ,,Прислушкивање", којима смо се или слатко смејали или због њих туговали.

Све ово, као и многе друге чињенице наводе нас на закључак да се технологије временом мењају, али увек је било и биће интересовања за дешавања у комшијском дворишту.

Сведоци смо и игара речи коришћених у маркетиншким кампањама, напомена написаних ситним словима по угловима огласа, скривених трошкова кредитирања, дугачких ситно куцаних неразумљивих уговора које потписујемо у банкама, брзог потврђивања да смо упознати са одредбама лиценцних уговора за софтвере које инсталирамо на нашим рачунарима. Таквих и сличних замки било је одувек, и само они који су имали довољно информација и знања успевали су да их избегну.

Исто тако знамо да су се појединци увек скривали у маси и бежали од креирања препознатљивог идентитета како би избегли личну одговорност.

Зато гласам за популаризацију и ширење коришћења знања и информација.

За оне који су забринути да ли неко неовлашћено снима наше разговоре, наше кретање, наше поруке, не морају да брину. То се ради у целом свету, код нас постоје инсталирана решења која су пренета из других држава. Али да ли неко зна за било које откриће које нема своју двоструку намену? Да ли знате неко комерцијално врхунско решење које није последица развоја војне индустрије и комерцијализације решења замењеног у војној индустрији неким новим, бољим решењем?

Зато олакшајмо себи свакодневни живот, као и животе пријатеља, комшија и рођака, разлога за бригу и без тога има довољно.

Дипл. инж. електротехнике
Ненад Маринковић
објављено: 18.03.2011.
http://www.politika.rs/rubrike/Sta-da-se-radi/Istina-ili-preterivanje.sr.html

Знамо ли ко све угрожава нашу приватност – Бранислав Радивојша

Мало објекти, више субјекти

Звучи помало ,,лудистички" када се каже да је модерна електронска опрема одговорна за угрожавање наше приватности

Да нема телевизије не би било ни ,,Великог брата", ,,Фарме" и ,,Двора". Другим речима, без телевизије милиони гледалаца не би могли свакодневно да посматрају шта раде неке познате личности, како изгледају разголићене, како се понашају за столом, како у кухињи итд. Али, опет, није телевизија ,,папарацо": не омогућава нам она да неовлашћено завиримо у приватност тих познатих људи. Они су нам сами то дозволили својим пристанком да учествују у емисијама у којима се њихова приватност излаже погледима најширег гледалишта.

Слична разлика је неопходна и кад говоримо о томе ко данас угрожава приватност нас обичних грађана. Под утицајем домета нових технологија, Интернета, видео-уређаја, камера, нових минијатурних прислушних апарата, могло би се помислити да су те справе, попут телевизије код ,,Великог брата", одговорне за то што је наша приватност све више и готово несметано изложена погледима других; што су многи подаци о нама доступни разним банкарским и другим службеницима; што мало боље обучени хакери могу да открију број нашег банковног рачуна и што нас свако, ако му је то потребно, може снимати и прислушкивати.

Фасцинација техником нас, међутим, не сме удаљити од истине која гласи да су, као и увек, разне справе само помоћно средство нечијих намера. Па и када је реч о намерама криминалаца, педофила и сличних.

Зато звучи помало ,,лудистички" када се каже да је модерна електронска опрема одговорна за угрожавање наше приватности. То истицање значаја опреме и технике може, додуше, да буде на месту када се наведе податак да је у Великој Британији од 2004. до 2007. године инсталирано 4,3 милиона камера за видео-надзор. На основу тога се може претпоставити да у тој земљи нема места које није покривено неким објективом који вас посматра у улози ,,Великог брата". Али камере су инсталирале локалне-државне власти или управе компанија, одлуке су њихове, а високософистицирана технологија томе само служи.

Зато је бесмислено питање да ли ту нову технологију треба користити. Јер у многим аспектима она поједностављује разне процедуре и скраћује време које смо непотребно трошили, рецимо, за добијање разних докумената или у потрази за неким производом или услугом. Нове технологије помажу и у заштити од разних терористичких, криминалних и сличних намера.

Обичном човеку, међутим, смета то што је употреба те технологије све масовнија и што се ствара утисак да постајемо њени објекти: сви нас чују, сви нас гледају, малтене свако може да дође до неких наших података.

Али овај проблем с доминацијом технологије се сад понавља и у јапанској катастофи. Јер сад се може помислити да Јапанцима владају нуклеарке. Они су их саградили, а ових дана су у њиховој милости и немилости. У односу на људе, техника је, међутим, и у овом случају невина. Она се понаша онако како су то њени творци смислили, укључујући ту и последице које тим дејствима настају. Ако су неке од тих последица за човека веома неповољне, нису за то одговорне нуклеарке, као што ни за нашу угрожену приватност не можемо кривити камере, бежичну телефонију и Интернет.

Бранислав Радивојша
објављено: 19.03.2011
http://www.politika.rs/rubrike/Sta-da-se-radi/Malo-objekti-vise-subjekti.sr.html

Знамо ли ко све угрожава нашу приватност - Данило Тврдишић

Ријалити Србија на раскршћу

Ми живимо у времену и цивилизацији у којој је приватност до те мере угрожена да је велико питање да ли ће приватност за коју годину уопште постојати као категорија коју данас познајемо. Ако узмемо у обзир да је приватност синоним за слободу, онда долазимо до застрашујуће чињенице да слобода у савременом друштву полако нестаје. Шта се десило са друштвима у којима се слобода изгубила? Завршни чин процеса нестанка слободе је неки гулаг као у време Стаљина или неки концентрациони логор као у време хитлервог трећег рајха.

Угрожавање приватности се данас одвија у неколико основних правца:

Злоупотреба савремених технолгија (биометрија, укрштање база електронских података, дигитални новац, чипови са процесором, РФИД технологија и уређаји за одређивање тачне локације, сателитско праћење, камере на јавним местима, ласерска технологија, интернет, мобилни телефони...). Да би се у пракси остварила поменута злоупотреба савремених технологија прилагођава се законска регулатива у правцу свеобухватне контроле и надзора. Прилагођавање законске регулативе у Србији реализовало се кроз доношење неколико системских закона који за резултат имају угрожавање приватности (Закон о електронским комуникацијама, закон о електронској личној карти, РАТЕЛОВ закон о надзору интернета, закон о Војно Безбедносној Агенцији итд).У односу на овај сет закона донешен је само један закон који штити приватност, закон о заштити слободе личности који уз то потпуно непримењив на наше услове.

Али има нешто опасније од злоупотребе нових технологија и законске регулативе када је у питању угрожавање приватности. У питању је афирмисање једне нове идеологије до сада непознате у историји људске цивилизације. Реч је о идеологији неслободе. Шта је то идеологија неслободе? У питању је утицај и порука на свест и савест човечанства с почетка трећег миленијума да са слободом може да се тргује, односно да је слобода на продају . На пример сведоци смо праве поплаве ријалити емисија типа „Двор“, „Фарма“, „Велики Брат“, „Парови“, „Сарвајвор“ и сл. Варају се они који мисле да су поменути

ријалитији само ревије простаклука и медијске проституције. Они то јесу, али су и много више и опасније од тога. Ријалитији представљају нови пројектовани модни тренд, афирмирмативан нови јавни морал и културни образац који представља друштво 24 часовног надзора. Порука гласи: ако могу јавне личности да буду под 24 часовним надзором и жртвују своју слободу, зашто би то био проблем обичним „смртницима“?

Поред тога врло често се чује питање од стране необавештене јавности: што би мени био проблем да будем надзиран ако ја немам ништа да кријем јер нисам криминалац? Замислимо једно такво питање у времену када су милиони невиних људи одведени пут концентрационих логора у време хитлеровог трећег рајха или у време Стаљинових гулага. Или неко можда може да тврди да ми можемо и треба да верујемо данашњим владајућим елитама које нпр. сада већ отворено говоре да је смањење светског становништва решење за проблеме цивилизације у којој живимо. Ко би смео да повери своју приватност и слободу људима који уводе Кодекс Алиментариус, односно скуп прописа којима се на мала врата уводе у ланац људске исхране генетски модификовани производи чији утицај на људско здравље је у најмању руку штетан и до краја неиспитан? Дакле, ми не само да имамо шта да кријемо од те и такве владајуће елите, а то наша слобода, већ је то и услов да је као такву задржимо. Значај иницијатива какав је и овај научни скуп који је организован од стране Покрета за приватност и Двери покрета за живот Србије у едукацији ширих слојева становништва је огроман јер се само на такав начин шира јавност може квалитетније упознати са опасностима које произилазе из угрожене приватности.

Данило Тврдишић, Двери

Знамо ли ко све угрожава нашу приватност - Ненад Вукићевић

Профилисање личности

Замислите да постоји психолог, задужен да вас прати, и на основу скупљених података да прави профил ваше личности, или тим стручњака који 24 часа на дан обављају такав задатак. Не би вам било све једно. Сада замислите да сваког грађанина надзире један такав тим. Мислите да је немогуће, наравно, из више очигледних разлога.

Међутим, ако заменимо психологе за рачунаре, препустимо анализу алгоритмима, и таква замисао – провођена неуморним, аморалним системима који би обрађивали све што изговоримо, купимо, чинимо и размишљамо – постаје сасвим могућа.

Заправо, већ годинама се развија технологија обраде личности. На пример, водеће интернет корпорације врше анализу активности посетиоца како би кориговали рекламне кампање. Банке профилишу клијенте када рачунају њихов кредитни рејтинг. Потенцијали таквог профилисања су ограничени само количином расположивих података, која се повећава из дана у дан.

Аутоматизовано профилисање личности је у многоме омогућено пролиферацијом технологија које скупљају огромне количине података о нама. Сваки пут када употребимо кредитну картицу, мобилни телефон или Интернет, наше активности се бележе у некој бази података.

Појединачно, те базе података не представљају огромну претњу по приватност, посебно ако се подаци чувају и обрађују по закону. Проблем настаје када се подаци укрштају. Информације које саме по себи не откривају ништа посебно, збирно откривају прецизну слику наших живота. У том процесу обједињавања система често губимо контролу над нашим подацима, самим тим и над приватношћу.

На Интернету је посебно изражен феномен укрштања услуга и централизације података, предвођен неколицином компанија које стварају својеврсни информацијски монопол. Ове компаније су се толико уплеле у све поре виртуелног друштва да је скоро немогуће бити на Интернету а не користити неке од њихових, често невидљивих, услуга.

Узмимо у обзир најпознатији сајт: Гугл. Осим што бележи сваку претрагу извршену на њиховом претраживачу, Гугл прати кориснике који њихов сајт никада нису ни посетили. Преко веб сервиса попут реклама (интегрисаних на стотинама хиљада сајтова) или Гугл Аналитикс-а (статистичком сервису који се налази на половини од милион најпопуларнијих сајтова) Гугл добија податке о кретању интернет популације. Укрштањем података које скупљају на тај начин, са подацима својих система за наплату, имејл, геолокацију, оцењивање сајтова и сл, Гугл је у могућности да анализира виртуелни живот интернет корисника.

Упоредно, Фејсбук, најпопуларнија социјална мрежа са скоро 700 милиона корисника, настоји да сазна шта волимо, како се осећамо и с ким се дружимо. Гугл, Фејсбук и још неколико приватних компанија са седиштем у САД фактички успостављају надзор над корисницима интернета, без њихове сагласности.

Нажалост, процеси обједињавања дигиталних услуга се одвијају и ван виртуелног света, без озбиљног разматрања последица по приватност и слободе грађана. Питања приватности и слобода су посебно битна када разматрамо коришћење разнородних података за профилисање личности, због опасности да се такви системи могу користити за надзор и манипулацију.

На пример, медији се често критикују да подупиру власт и велике корпорације. Међутим, ако су овакви медији, без „интерактивног“ елемента, имали толики утицај над становништвом, поставља се питање могућности обичног грађанина да се одупре усмереној, психолошком профилу кројеној, пропаганди коју би системи аутоматизованог профилисања омогућили. Пропаганда, креирана са сазнањима о најинтимнијим слабостима, жељама и страховима појединца, би била далеко софистицираније од данашње. Истраживања показују да су прилагођене рекламне кампање, на основу

профилисања урађеним на постојећим системима, и до 2.68 пута ефектније од класичних.

Технологије које би омогућиле корпорацијама и владама да у реалном времену прате грађане, да на основу огромних количина приватних података профилишу њихову личност, и да евентуално те информаиције (зло)употребе у пропагандне сврхе представаљају огромну претњу, не само за приватност, него слободе грађана.

Ненад Вукићевић

Знамо ли ко све угрожава нашу приватност - Александар Павић

11.9.2001: почетак глобалног рата против личности

Напад на Светски трговински центар у Њујорку од 11.9. 2001. означио је прекретницу, почетак краја сна о непрекидном, глобалном „ширењу слободе“ које се чинило незаустављивим у времену после пада Берлинског зида. Управо је тај догађај постао повод за примену све агресивнијих мера (укључујући и војну агресију) широм света – у име „борбе против тероризма“ и за „безбедност“ – које су на добром путу да учине свет из Орвелове „1984“ стварним.

Напад од 11.9.2001. изнедрио је тзв. Патриотски акт, закон који је знатно проширио могућности америчке државе да не само надзире већ и шпијунира грађане (и своје и стране), тј. њихове комуникације и здравствене, финансијске и друге податке (укључујући и књиге позајмљене из библиотеке); проширене су мере безбедности и умножене надзорне камере по јавним местима, и уведени агресивни поступци претресања путника у авионском саобраћају (до садашњих скенера који људе визуелно „скидају до голе коже“); полицијске снаге су милитаризоване, а ограничења на вршење ненајављених претрага приватног поседа знатно смањена; отворен је пут држави да хапси или киднапује „потенцијалне терористе“ и затим их држи у неограниченом притвору, без права на спољну комуникацију или адвоката, у логорима широм света.

Још горе, „Патриотски акт“ је послужио као глобална матрица, узор (или изговор) за владе широм света, па и у Србији.

Његово усвајање у Конгресу САД је максимално збрзано. Прве верзије су убачене у процедуру већ неколико дана после 11.9. рађајући сумње да је све већ било спремно и да се само „чекао“ погодан тренутак. Више конгресмена се жалило да нису имали прилику да га чак ни прочитају:

„Ово је најмање демократски процес расправе о питањима од фундаменталног значаја за демократију који сам икада видео,“ рекао је посланик Барни Френк. „Предлог закона тајно сроченог од стране неколико људи, који није прошао никакву расправу у комитетима, представљен нам је без права на амандман.“ Према посланику Рону Полу, закон „дефинитивно није био доступан посланицима пре гласања“.

Начин доношења и садржај „Патриотског акта“ били би можда мање спорни да се сама званична верзија 11.9. није показала у тој мери сумњивом да се захтеви за нову истрагу и даље умножавају. Више професионалних група у САД са хиљадама угледних чланова – Пилоти, Архитекти, Инжењери, Политички лидери, Авио-механичари, Официри, итд. „...за истину о 11.9.“ захтева ново расветљавање, а многи и директно оптужују своју владу за умешаност. Нова грађанска иницијатива је у јесен 2010. лансирана у самом Њујорку, тражећи истину о тајанственом рушењу треће зграде Светског трговинског центра, високе 47 спратова, која је „сама пала“ неких 7 сати после „кула-близнакиња“, за само 7 секунди (указујући на постављени експлозив), а да никакав авион у њу није ударио. Указује се, између осталог, и на извештавање ЦНН и ББЦ, који су „објавили“ рушење поменуте зграде 70, односно 23 минута унапред – новинарка ББЦ је о томе „извештавала“ док је иста зграда штрчала у кадру иза ње. У јануару 2011. је нову „фрку“ изазвао Ричард Фок, стручњак Већа за људска права УН, написавши да постоје очигледна прикривања у „званичној верзији“ 11.9. а да поготово узнемирава „сабласна тишина мејнстрим медија“ у свему томе. Занимљиво је да је Фоково иступање наишло на оштре и негативне реакције не само америчког амбасадора у УН већ и Бан Ки-Муна. Такође је занимљиво да Кес Санстин, Обамин администратор за информације, предлаже „инфилтрирање“ интернет група чије „теорије завере“ доводе у питање „званичну верзију“ 11.9. – и не само њу.

Глобално угрожавање личних слобода и приватности није само ствар „незадрживог развоја технологије“, јер вове технологије нуде не само могућност тоталног надзора већ и могућност да се он и ограничи. Ко год инсистира на аспекту контроле људи а не на контроли технологије – нема чисте намере. Чињеница да превагу у владајућим структурама широм света односе ови први говори нам да на сцени није глобални рат против „тероризма“, већ пре рат против саме људске слободе, чији је исход од животне важности за све нас.

Александар Павић

Знамо ли ко све угрожава нашу приватност - Предраг Радовановић

Заштита података у електронском банкарству

Електронско банкарство најсажетије можемо дефинисати као испоруку банкарских „производа“ и услуга преко електронских канала дистрибуције. Електронске трансакције најпре су постале реалност у сегменту банкарства „на велико“ (wholesale banking) а крајем осамдесетих и почетком деведесетих година прошлога века водеће банке понудиле су овакве системе и у сегменту банкарства „на мало“ (retail banking). Банке су, у почетку, самостално развијале софтвер намењен електронском банкарству. Поред тога што је клијент морао да инсталира овакав софтвер на свом персоналном рачунару, недостаци овог приступа огледали су се и у томе што је такав софтвер био наклоњен информационом систему банке, а не кориснику. Софтвер је био компликован за употребу и, што је још горе, није био компатибилан са софтвером других банака. Ако би клијент одлучио да промени банку, морао је да се одрекне читаве евиденције коју је до тада водио у софтверу претходне банке. Неки од водећих произвођача софтвера уочили су овај проблем и убрзо понудили стандардизоване софтверске пакете за управљање личним финансијама који су, између осталог, омогућавали коришћење услуга кућног банкарства. Банке мале и средње величине, које нису имале довољно средстава да самостално развијају софтвер намењен кућном банкарству, напокон су могле понудити услуге кућног банкарства употребом стандардизованог софтвера. Овакви системи, које најчешће називамо системима кућног или PC банкарства, имали су компаративну предност из аспекта безбедности: за повезивање са информационим системом банке користиле су се приватне, резервисане линије које су гарантовале високи степен безбедности.

Животни циклус кућног банкарства нагло је прекинут развојем Интернета. Развој приватних мрежа, које су чиниле инфраструктуру кућног банкарства, био је веома скуп. Због тога су банке, уместо да самостално развијају приватне мреже, убрзо почеле да користе инфраструктуру јавних рачунарских мрежа, практично без икаквих трошкова. Употреба јавних рачунарских мрежа, пре свега Интернета, има бројне компаративне предности над приватним мрежама. Пре свега, трошкови употребе оваквих мрежа су значајно нижи. Поред тога, Интернет има глобални домет, па је могуће пружати услуге

клијентима на ширем географском подручју, па чак и изван националних граница. Потенцијал за привлачење нових клијената преко Интернета је вишеструко већи у односу на приватне мреже. Коначно, развијени су тзв. web e–banking системи за чију употребу није потребно инсталирати никакав додатни софтвер. Овакви системи омогућили су коришћење услуга електронског банкарства преко Интернета са било ког стоног или преносног рачунара, мобилног телефона или другог сличног мобилног уређаја који садржи стандардни софтвер за претраживање Интернета (web browser) и има могућност повезивања са Интернетом.

Упркос наведеним предностима, основни недостатак јавних, у односу на приватне рачунарске мреже, је недовољна безбедност трансакција. Интернет је јавна, отворена мрежа којој свако може приступити. Злонамерни појединци и организоване криминалне групе могу да „пресретну“ и злоупотребе податке који се прослеђују преко Интернета, па чак и да украду нечији дигитални идентитет. Мада је број оваквих злоупотреба мали у односу на укупан број трансакција, медији су им често приступали сензационалистички, па код клијената у електронском банкарству преко Интернета постоји страх када треба да проследе своје осетљиве финансијске информације преко Интернета.

Имајући у виду да управо та перцепција клијената о безбедности трансакција преко Интернета представља једну од најзначајнијих баријера за даљу експанзију електронског банкарства и електронског пословања уопште, ангажован је велики број стручњака на решавању овог проблема.

Да би се спречила злоупотреба података у јавним рачунарским мрежама, прибегава се њиховом шифровању (енкрипцији). Шифровање се користи да би се поверљиве информације сакриле од онога коме нису намењене. Обрнути процес назива се дешифровањем (декрипцијом). Наука која се бави шифровањем података и њиховом трансформацијом у облик којем је немогуће приступити без познавања тајног кључа назива се криптографијом. Конвенционална криптографија, која се још назива и енкрипцијом са тајним (симетричним) кључем, користи један исти кључ за шифровање и дешифровање. Предности конвенционалне енкрипције су у томе што је веома брза и погодна за податке који се одлажу или архивирају. Оваква енкрипција, међутим, није погодна за податке које треба некоме проследити, због тога што је уз шифроване податке потребно приложити и тајни кључ, који је неопходан за њихово дешифровање.

Данас се за ускладиштење поверљивих података или њихов пренос преко неосигураних мрежа (какав је Интернет) највише користи криптографија уз помоћ јавног кључа. Ово је асиметрични модел криптографије који користи пар кључева: за шифровање се користи јавни кључ, док се за дешифровање користи приватни или тајни кључ. Јавни кључ се може, без проблема, послати било коме, будући да је рачунски неизводљиво открити тајни кључ на основу јавног кључа. Свакако највећи допринос криптографије уз помоћ јавног кључа огледа се у томе што она омогућава употребу дигиталних потписа и дигиталних цертификата. Дигитални потписи омогућавају примаоцу информација да провери аутентичност њиховог порекла као и да се увери у то да су информације пренете у нетакнутој, неизмењеној форми. Дигитални потписи базирани на јавном кључу, дакле, омогућавају аутентикацију и интегритет података. Дигитални потписи, такође, гарантују непорецивост, што значи да онемогућавају пошиљаоца поруке да тврди како он није послао поруку. Ова карактеристика је од скоро исте важности за криптографију као и приватност.

Дигитални цертификати садрже информације које су придружене нечијем јавном кључу и помажу другима да провере да ли је кључ оригиналан и валидан. Дигитални цертификат, дакле, садржи јавни кључ, информације о идентитету корисника и један или

више дигиталних потписа. Све шира употреба криптографије уз помоћ јавног кључа захтева формирање инфраструктуре јавних кључева, која ће допринети успостављању поверења међу корисницима. У ту сврху се формирају центри за цертификацију или цертификациона тела, чија се улога састоји у провери валидности цертификата и потписивању валидних цертификата. Наравно, формирање инфраструктуре јавних кључева немогуће је без претходног усвајања сета закона (пре свега, Закона о дигиталном потпису и Закона о електронској трговини) којим се дефинише одговарајући правни оквир.

Приступ системима електронског банкарства може се извршити на више различитих начина, што зависи од конкретне банке, али и од врсте услуга које клијент жели да користи. Обично се за приступ основним услугама, као што је нпр. увид у стање на рачуну, користи број партије и лични идентифи кациони број (PIN). За коришћење напреднијих услуга, као што је нпр. трансфер средстава на унапред утврђене рачуне или обављање мењачких послова, потребно је пријавити се на систем употребом корисничког имена и лозинке. За обављање осталих напредних услуга, као што је нпр. трансфер средстава на друге рачуне, корисник се мора пријавити на систем употребом различитих преносивих медија (на којима се налазе потребни дигитални цертификати за безбедан приступ апликацији) и личног идентификационог броја. Зависно од банке, као медији се могу користити мини компакт дискови (мини–CD), смарт картица или USB диск. Поједине банке захтевају употребу различитих лозинки — једне за приступ систему, а друге за одобрење плаћања — чиме се могућност злоупотребе значајно смањује. Неке пак банке захтевају да се код појединих трансакција у сврху идентифи кације користи посебан наменски хардверски уређај за генерисање једнократних лозинки („токен“). Овај начин се у пракси показао и као најпоузданији и најфлексибилнији, јер генератор лозинки може да се користи за приступ услугама електронског банкарства са било ког рачунара, а могућност да функционише независно од рачунара омогућава и његову употребу за приступ систему електронског банкарства преко других канала, као што су говорни аутомати, инфо–киосци, електронска пошта, SMS сервис, WAP сервис, факс и др.

Поједине банке увеле су и могућност плаћања OTAPOS системом. На овај начин може се платити сваки рачун, са било ког рачунара. Систем функционише тако што се налог за плаћање „потписује“ шестоцифреним кодом који се добија путем SMS поруке. OTAPOS систем је прилично безбедан начин за ауторизацију плаћања јер се шифра коју клијент добија SMS поруком користи само једном. Овим системом се мобилни телефон, у суштини, претвара у „генератор“ једнократних лозинки.

Недавно је уведен и мобилни платни сервис који омогућава да се на стандардној SIM картици (која се може користити у било ком мобилном телефону) меморише дигитални цертификат који гарантује сигурност и заштиту трансакција. Када на мобилни телефон пристигне рачун за плаћање, клијент треба да упише лични идентифи кациони број за ауторизацију плаћања, након чега добија поруку о извршеном плаћању. Плаћање је једноставно, а посебна погодност је што се не мора уписивати број рачуна, износ, позив на број и сл. На овај начин се мобилни телефон трансформише у безбедан трансакциони уређај.

Предраг Радовановић

Знамо ли ко све угрожава нашу приватност - Јован Валентин Истрати

Камера скривена у души

Све смо ближи једни другима, а све усамљенији, све даље од душа других људи.

Читао сам ових дана на Интернету о разноврсности средстава за аудио и видео запис који постоје данас, разноврсности која је налик на халуцинацију.

Микрокамере, скривене у реверу сакоа, у оловци за писање, наочарама, телефону – све имају задатак да запишу и открију сакривене и, наравно, интересантне детаље твог личног живота. Сада се сваки догађај истог трена снима на мобилни телефон или камеру која је постављена негде. Сва места на земљи се лако виде.

Уз помоћ програма „Google Earth“ можеш видети све, чак и шешир старице на Ајфеловој кули. Можеш се виртуелно прошетати својом улицом, гледати је са сателита, можеш пратити из минута у минут како расте мали птић на некој бостонској крошњи.

Све се снима, све је откривено, рекли би ми. Сваки детаљ, колико год безначајан, треба и мора да буде постављен пред очи гомиле која је жедна сензације. Пре свега се на медијске звезде обрушава лавина погледа, у њихов приватни живот упадају, прате их свуда.

Међутим и обични људи, који ничим нису посебно за њих занимљиви, могу постати мета радозналих мас-медија – због важности своје професије например. Уопште, не можеш се сакрити ни у мишју рупу од урокљивих очију Великог брата. Свевидећем Богу на чудовишан и ненормалан начин подражавају у новом потрошачком друштву. Безуспешно се са Свевидећим Творцем такмиче нове структуре праћења, безбедности, итд.

У Царству Божијем ће све тајно бити објављено и осуђено пред свима, „на крововима“ говори Свето Писмо. На тај начин, тајне људске душе ће постати откривене за милијарде анђела и сву нашу сабрану људе – и биће разлог васељенског плача и бесконачног ридања.

Архиве служби безбедности ће бити показане, чак и уништене да би се показала чисто и одједном, без икаквих грешака у тумачењу, апсолутна истина о сваком људском бићу. Све ће бити објављено, измерено праведним и љубећим судом Божијим и постати основа или за вечно блаженство или обрнуто, за вечну осуду. Најезда система посматрања – електронског, компјутерског, медијског, политичког и тако даље – јесте пророштво о томе да се време истине, која ће се громко објавити, са кровова света, приближава.

Постајемо све ближи једни другима, живимо у преиспуњеном глобалном селу, али се осећамо све усамљенији, све даље од душа других људи. Живимо на растојању звучног сигнала до Америке, али на растојању целе вечности до неба. Или, боље рећи, тела се не приближавају, постају све већа под притиском материје, а душе све ситније, зато нам се чине тако далекима.

Шта нам остаје да чинимо? Записују нас, прислушкују, виде, коментаришу све више и више електронских очију, иза којих се крију непознате (добре или лоше) замисли. О нама је све познато. „Јер постасмо призор (theatron) и анђелима и људима“. (1 Кор. 4:9). Играмо на гигантској сцени, која је до апсурда осветљена хиљадама пројектора, а никада не видимо гледаоце, који су сакривени иза заштитних екрана и којих је све више и више.

Једино добро и истинито што треба да чинимо је да живимо по Истини, по Христу. Да се не би стидели ни једног нашег дела (то јест да чинимо само добро). Живети као да – а тако и јесте – живимо под непрестаним и љубећим погледом Божијим. Камера, скривена у души је шатор Духа Светога у коме света љубав

Христа Женика слави празник и доноси бесмртност.

Мисли о покајању, саосећању и праштању не могу бити снимљене ни најсавршенијим апаратом. Дакле, терор скривених објектива је снажан само тамо где има шта да се крије. Код човека доброг, милостивог и верујућег живот иде природним путем, без скривених детаља, у границама нормалности и здравог смисла. И ко ког да га гледа, чак у личном, домаћем животу не може видети ништа до живота, испуњеног Богом и оваплоћене молитве – живе и делатне љубави.

Свештеник Јован Валентин Истрати
Превод: Станоје Станковић
http://www.pravoslavie.ru

О ауторима:

Никола Марковић
Председник Друштва за информатику Србије
www.dis.org.rs

Г. **Никола Марковић** и друштво за информатику на чијем је челу свих ових година је значајно допринело развоју информационих технологија у Србији. Брига о стандардима, школству, законима... су теме којима се друштво за информатику Србије бави.

Александар Ресановић
Заменик повереника за информације од јавног значаја и заштиту података о личности
www.poverenik.org.rs

Александар Ресановић је помоћник Повереника за информације од јавног значаја и приватност. Заједно са г. Родољубом Шабићем, велики је борац за слободу живљења. Једна од битних ствари која је изашла из канцеларије Повереника је уређење правила о евиденцијама грађана.

Проф. др Инж. **Драган Ћосић**
Београдска пословна школа - висока школа струковних студија
Савез за примену микрорачунара Србије
www.polarotor.tv

Професор Београдске пословне школе др. инж. **Драган Ћосић** је и уредник чувене, сада већ и историјске емисије о технологијама Поларотор. Проф. Ћосић је такође и оснивач друштва за примену микрорачунара Србије.

Александар Арсенин
Председник покрета за електронску приватност
Консултант за безбедност електронских система
www.internetservis.co.rs

Александар Арсенин се преко десет година бави превенцијом електронског криминала на пољу дечије педофилије и порнографије на интернету. Радом у Покрету за приватност указује на слабе тачке електронских система у технологије које угрожавају слободу.

Александар Загорац

Стални сарадник ЦЕПИС-а
Подпредседник Покрета за електронску приватност Србије
www.privatnost-srbija.com

Г. **Александар Загорац**, правник иначе стручни сарадник Центра за проучавање технологија СПЦ-а. Г. Загорац је изврстан аналитичар, његове препоруке и решења су крајње практична и применљива. Један од битних радова је и критички осврт закона о заштити података о личности рађен 2008. године.

Стеван Лилић

Професор универзитета, председник Удружења „Правници за демократију
www. slilic.com

Објавио преко 300 библиографских јединица, универзитетских уџбеника, монографија, чланака и есеја на тему управног и уставног права, људских права, заштите приватности, јавне управе и правне информатике.

Звонимир Ивановић

Криминалистичко-полицијска академија
Одељење МУП за борбу против високотехнолошког криминала
www. mup.gov.rs

Горан Ј. Мандић

Факултет за безбедност - Универзитет у Београду
www.fb.bg.ac.rs

Асистент на Системима обезбеђења и заштите у Корпоративној безбедности. Учествовао у обликовању наставног плана и изводи наставу на специјалистичким студијама безбедносног менаџмента.

Милан Туба

Факултет за компјутерске науке - Мегатренд

Директор је Више школе за компјутерске науке у оквиру приватног Мегатренд универзитета у Београду. Ту је координатор програма ECDL (European Computer Driving Licence). Пионир је у области приватности

и један од првих стручњака који је реаговао и говорио о овој теми још пре 17 година.
http://sr.wikipedia.org/sr/Милан_Туба

през. Оливер Суботић
Центар за проучавање и употребу савремених технологија
Архиепископије београдско-карловачке
Аутор је једине домаће студије о биометријским системима. През. Оливер је дугогодишњи борац за правилну и разумну употребу модерних технологија у свакодневном животу.
www.cepis-spc.com
www.covekitehnologija.com

Војислав Родић
Директор И Нет доо
www.inet.rs

Ненад Маринковић
Дипл. инж. електротехнике

Бранислав Радивојша
Уредник Политике
www.politika.rs

Данило Тврдишић
Покрет за живот Србије
www.dverisrpske.com
Иницијатор одбора за приватност Двери српске. Његов рад приказује шири смисао и различите инструменте контроле људи који су постали свакодневница.

Ненад Вукићевић
Уредник сајта Српски националисти
Стручњак са вредним искуством по питањима слободе говора и заштите личних података.

Предраг Радовановић
Редовни професор, Виша пословна школа у Лесковцу

Александар Павић
Оснивач НВО "За живот без жига", колумниста Фонда стратешке културе (Русија) и члан уредништва сајта www.vidovdan.org
www.zazivot.org.rs
Један од пионира борбе за слободу живљења. Велики допринос је дао 2005. године у кампањи која је за резултат омогућила слободу избора - ЛК са биометријским подацима или без.

Јован Валентин Истрати
Свештеник
www.pravoslavie.ru

Поводом Научно скупа одржаног 17.02.2011. године у Београду

Приватност у Србији са погледом на регион

Проблем приватности грађана у Србији али и у ширем региону добио је "додатну вредност" честим повредама идентитета у последњих годину дана. Готово да нема државе која је избегла проблем високотехнлошког криминала од ситних крађа електронског новца, крађе идентитета па и до проблема на националном нивоу. Земље "ExYU", земље из окружења и земље припаднице Европске уније су подједнако третиране од стране електронског криминала без нарочите разлике.

Заједничко за све поменуте државе је недостатак контроле и недовољна пажња институција задужених за безбедност података. Административна правила у већини случајева захтевају писани документ и папирну архиву без обзира на постојање електронског потписа чије би масовно увођење свакако повећало степен заштите на свим нивоима. Слаба карика у ланцу заштите се налази у класичним депоима јер поред добрих технолошких и информатичких стандарда који обезбеђују интегритет података, папирне архиве остају необезбеђене[1]. Ту наилазимо на сасвим класичан проблем физичко-техничке заштите и проблем непоштовања протокола о приступу класичним архивама. У информатичким базама података су поменуте ситуације уређене на највишем нивоу (уколико је систем рађен по

[1] У Србији имамо проблем, што је показано и инспекцијским надзором Повереника (презентованом на Научном скупу 17.02.2011.), да поред најсавременијих информатичких система имамо класичне архиве у необезбеђеним орманима по ходницима институција. То су копије или оригинали који имају важност.Тако долазимо до закључка да имплементирани информациони системи не служе заштити података већ њиховој обради. Чест је случај да се папирне архиве чувају на потпуно незаштићеним местима.

безбедносним стандардима). Поменуто је да је свест о важности затите података је на ниском нивоу, тај проблем се превазилази информатичким моделима где институција не мора водити рачуна о физичкој заштити већ се све решава у самом "срцу" рачунарског система.

Паралелно са поменутим, постоји невероватно низак степен заштите рачунарских мрежа. Статистички надзор спроведен на добровољној бази током 2010. године на узорку од 100 правних лица (неки од њих садрже веома осетљиве приватне податке корисника), говори да је у само 6 случајева постојала адекватна информатичка заштита која може гарантовати висок степен заштите података. У 19 случајева је заштита била на ниском нивоу и спецификација инсталиране опреме није била адекватна потребама институције тако да је постојао огроман ризик од крађе података и оштећења система. У 54 случаја, заштита није постојала. Остатак у овој статистици се односи на сиситеме који су препуштени случају на најбизарнији начин. Поменућу да изузетно поверљиве податке о грађанима можемо наћи у школама, у архивама политичких странака, у разним институцијама за бригу о људима (то су евиденције особа са ниским социјалним статусом, особа са инвалидитетом, особа са здравственим проблемима итд, а њихове податке третирају често разне НВО које прикупљају узорак на нивоу ширег подручја на којем раде). Физичка заштита бежичних мрежа се у 75% случајева може превазићи, а то је узроковано опет ниском свешћу о заштити и штедњи на инсталираној информатичкој опреми. Интересантан је још један податак да је у 85% случајева заштиту рачунарских система радило нестручно лице, углавном неко из окружења - информатичар или особа која "зна о томе". У тим случајевима не постоји пројекат, анализа ризика, слабих тачака... итд. већ се заштита обезбеди по неким универзалним методама и непровереним веровањима "стручног лица".

За државе у региону које се налазе у ЕУ можемо рећи да се делимично придржавају препорука али то не обезбеђује потребан безбедносни квалитет. Корисне податке о томе можемо видети из извештаја које је PrivacyInternational[2] објавио за регион. Србије нема у том извештају али уколико погледамо резултате земаља које технички и правно имају боље мере предострожности, а које су на самом дну лествице стичемо довољан утисак о нивоу заштите података у Србији. Ово је

[2] PrivacyInternational је један од партнера Покрета за електронску приватност Србије

добар показатељ да правила ЕУ нису функционална сем у случајевима савршеног друштвеног и државног уређења. Да оправдам ову реченицу, напоменућу и случај Немачке која и сама има престижну организацију за приватност[3], а која је током 2010. године увела низ препорука и измена протокола за приступ и заштиту података (не само информатичких већ и правних). Ове препоруке су у неким битним тачкама дијаметрално супротне препорукама ЕУ.

Поред недостатка свести о потреби заштите података, заједнички фактор је недостатак новца. Било да су у питању развијене земље или државе са слабим економским статусом, проблем приватности је банализован на првом кораку. Недостатак финансијских средстава условљава мањак информатичке опреме или инсталацију алтернативне неадекватне методе заштите, непостојање физичке заштите архива и опет, употребу алтернативних магацина[4] и свакако условљава непостојање обучених службеника.

Одржан научни скуп је указао на неколико основних проблема заштите података, а следи корак који треба да донесе практичне моделе који ће бити усаглашени са социјалним, техничким, правним, економским и етичким начелима у Србији. Тако локализован модел решења може уз највиши степен уштеде финансијских средстава за резултат пружити безбедност грађана у информационом добу.

[3] FoeBud

[4] Овај проблем у појединим институцијама иде дотле да не постоје средства за куповину ормана или замену бравица за закључавање на постојећим орманима са архивама грађана.

Покрет за електронску приватност Србије

председник
Александар Арсенин

подпредседник
Александар Загорац

kontakt@privatnost-srbija.com

www.privatnost-srbija.com