KOMPJUTERSKA KRAĐA IDENTITETA I NAČINI ZAŠTITE

dr Milan Radosavljević*
mr Maja Anđelković**
mr Dragana Radosavljević***

Sažetak: *Informatičko doba je donelo mnogo zadovoljstva i poboljšalo brojne performanse života i rada. Informatička tehnologija je olakšala život i rad, ali je omogućila i brže i pouzdanije komuniciranje i bavljenje biznisom, na nacionalnom i međunarodnom tržištu. Internet je ukinuo tradicionalni značaj lokacije i tradicionalno tržište preneo na telekomunikacione mreže. Međutim, informacione tehnologije su donele i mnoge probleme u biznisu i životu uopšte. Krađa identiteta putem kompjutera je postala savremeni oblik kriminala, pre svega u informatički razvijenim zemljama sveta. Zakonitost koja je postojala u ranijim tehnologijama se i ovde nastavlja, samo je njen intenzitet jači, kao i implikacije. Dakle, svaka tehnologija se manje više stvara radi olakšanja života i rada čoveka, ali se može upotrebiti i u neželjenom smeru, pa i zloupotrebiti. Rad ima za cilj da skrene pažnju na problem kompjuterskog kriminala, posebno na krađe identiteta kao sofisticiranog oblika kriminala, koji je prisutan u razvijenim zemljama, a koji nije dobio šire razmere u zemljama razvoja i tranzicije, kako bi se na vreme preduzele odgovarajuće mere na nacionalnom, korporativnom ili mikro nivoima. razmere.*

Ključne reči: *On line kriminal, privatnog, krađa identiteta, zaštita*

Abstract: *The Information Age has brought many pleasures and improved numerous life and working performances. Information technology has made life and work easier, but also it has enabled faster and more reliable communication and business operations both in the national and international market. The Internet eliminated the traditional significance of the location and transferred the traditional market to the telecommunication networks. However, IT has brought many other problems in life and business. Identity theft by computerized technology is a modern criminal act, especially in the most developed countries. The rules existed in earlier technologies can be seen here as well, but its intensity and implications are much stronger. Therefore, every technology is more or less created for making life and work easier for a human being although it may be misused or even abused. The aim of this paper is to emphasize the problem of computer criminal, especially the identity theft as a sophisticated criminal act which is present in the most developed countries, but which has not spread in a larger extent in the developing countries so some measures in the national, corporation and micro level can be undertaken beforehand.*

Key words: *Online crime, private, identity theft, protection*

Problem digitalnog gepa

Digitalna podela je jedna od glavnih moralnih izazova sa kojom se savremeno globalno društvo suočava. Dakako, ona polarizuje svet na onaj deo koji informatičku tehnologiju koristi u poslovne i privatne svrhe i onaj koji često i ne poznaje značenje reči internet.

Ovo posebno dolazi do izražaja u uslovima snažne povezanosti informatičke pismenosti i poslovne efikasnosti. Jasno je da informatičko obrazovanje ima snažnu moć, verovatno veću nego što su to

* dr Milan Radosavljević, profesor,Visoka poslovna škola strukovnih studija u Novom Sadu
** mr Maja Anđelković, asistent, FORKUP, Privredna akademija, Novi Sad
*** mr Dragana Radosavljević, asistent, FORKUP, Privredna akademija, Novi Sad

svojevremeno imali para, nafta ili atomska energija. Na primer, pristup zemlji u agrarnom društvu je predstavljao uslov velike moći, zbog čega je svako nastojao da poseduje što veće površine obradive zemlje. „Ali u informatičkom društvu, moć je u znanju", ističe John Kenneth Galbraith, Američki ekonomista specijalizovan za nove nastale trendove u SAD ekonomiji. „Danas vidimo novu podelu u strukturi klasa – sve je podeljeno na one koje poseduju informaciju i na one koje moraju da funkcionišu neznanjem. Ova nova klasa ima svoju moć, ne od imanja i pare, već od znanja".[1]

Dobra vest je da se digitalna podela u Americi smanjuje, ali i dalje postoje veliki izazovi koji moraju da se prođu. Pogotovo ljudi u ruralnim sredinama, stariji, hendikepirani i manjine, znatno zaostaju za javnim pristupom za Internetom i informatičkim obrazovanjem. Ovo je svojevrsna zakonitost u mnogim zemljama.

Loša vest je da izvan Sjedinjenih Država, postoji još uvek veliki gep koji se sve više širi, posebno u zemljama u razvoju gde informatička infrastruktura i obrazovani informatički stručnjaci nedostaju. Ovim se limitira i moć onih koji imaju razvijenu informatičku infrastrukturu, jer je poznato da što je veći broj povezanih računara u mrežu, da se povećava moć mreže. Manji broj kompjutera u mreži, znači manji broj komunikacija i manje mogućnosti za širenje informacija. Očigledno, digitalna podela je veliko moralno posrnuće savremenog sveta, koje ostavlja ozbiljne implikacije na globalnom nivou, pa i u razvijenim tržišnim zemljama sveta.

Prethodni moralni problem proširuje se i na druga etička pitanja posebno kad je u pitanju privatnost informacije. Ovaj problem nije bio aktuelan u nastanku kompjutera i prvobitnih informatičkih tehnologija, jer je dominantan cilj bio otkriti informaciju. Fenomen privatnosti informacije je dobio na značaju poboljšanjem tehničkih mogućnosti za prikupljanjem, selekcijom i analizom podataka, a posebno transformacijom istih u informacije, odnosno znanje kao verifikovanu i proverenu informaciju čije se postavke ne mogu dovesti u pitanje. Informatička etika se koristi da opiše probleme i standarde upravljanja i korišćenja informacionih sistema. Godine 1986. Richard O. Manson napisao je klasično delo o problemima koji su ključni u ovoj oblasti, a to je: privatnost informacija, preciznost, vlasništvo, i pristupi informacija. Ovi problemi su aktuelni i u savremenim uslovima i postaju vodeći u većini moralnih rasprava.

Korporativna informatička odgovornost i zaštita privatnosti

Brojni poslovni skandali koji su se desili u prethodne dve decenije prošlog veka, ostavljaju ozbiljne dileme i traže odgovor na pitanje, kako napraviti moralnu i društveno odgovornu kompaniju koja bi bila konkurentnija u odnosu na nemoralne i neodgovorne kompanije. Konkretno, radi se o dilemi da li je u informatičkom društvu korisno biti moralan, odnosno da li moralnost i odgovornost stvara određene prednosti u poslovnom biznisu. Problem je složen, utoliko pre što ne postoje jasne korelacije između moralnog i odgovornog poslovanja i korporativne uspešnosti. Ipak, stereotipi govore da se u biznisu mora biti moralan, jer tvrditi suprotno bilo bi neprihvatljivo sa stanovišta konzumenata proizvoda ili usluga. Zbog navedenog, mnoge nacionalne zajednice i organizacije korporativnog tipa ipak nastoje da budu etičke i odgovorne, dokazujući da se etično poslovanje na dugi rok isplati.

Prema stavu CEO Deloitte & Touche, Harold Tinklera, etičko upravljanje kompanijom zasniva se na kulturi, kontroli i odgovornosti. Drugim rečima, moralne i odgovorne kompanije se stvaraju, što je i prirodno, jer se pokazuje da ništa ne nastaje iz ničega, već za sve postoje izvori i koreni. Iako su sva tri elementa etičkog upravljanja kompanijom bitni, ipak najvažniji faktor je kultura, odnosno organizaciono ponašanje zaposlenih.[2] Organizaciono, odnosno poslovno ponašanje menadžmenta i zaposlenih često predstavlja vrednu stavku u aktivi kompanije koja se neopravdano zapostavlja.

[1] Relativno dobro predstavljanje ljudske civilizacije dao je A. Tofler u svom delu „Treći talas", Otokar Keršovani, Rijeka, 1992. On razlikuje prvi ili agrarni talas, drugi ili industrijski i treći talas pod nazivom informatički, koji ima svoj najviši nivo, a to je doba znanja.

[2] www.deloitte.com (dtt) press_release, 14.10.2004.

Moralno i odgovorno ponašanje i lični primeri upravljačko rukovodilačke strukture u kompaniji su najbolji načini za stvaranje poželjne organizacione kulture. Praksa pokazuje, da bez obzira na dominaciju informatičke tehnologije u korporativnom poslovanju, zaposleni slušaju šta im menadžeri govore, ali se ponašaju najčešće na način kako se ponašaju i menadžeri. Da bi se izgradila, a potom održala određena organizaciona kultura, kompanije koriste različite mehanizme i institucije. Neke uspešne kompanije su se odlučile da otvore radno mesto moralnog menadžera, koji je često zamenik CEO za moralno delovanje i vaspitanje. Ova praksa je preuzeta iz vojnih organizacija zemalja real socijalizma koja je svoju osnovu imala u ideološkoj postavci širenja ideje o real socijalizmu i samoupravljanju kao najhumanijem društvenom sistemu. Ovi sistemi su pokazali da bez zadovoljavajuće moralne i društveno odgovorne komponente u organizaciji ne vredi mnogo ni tehnički progres.

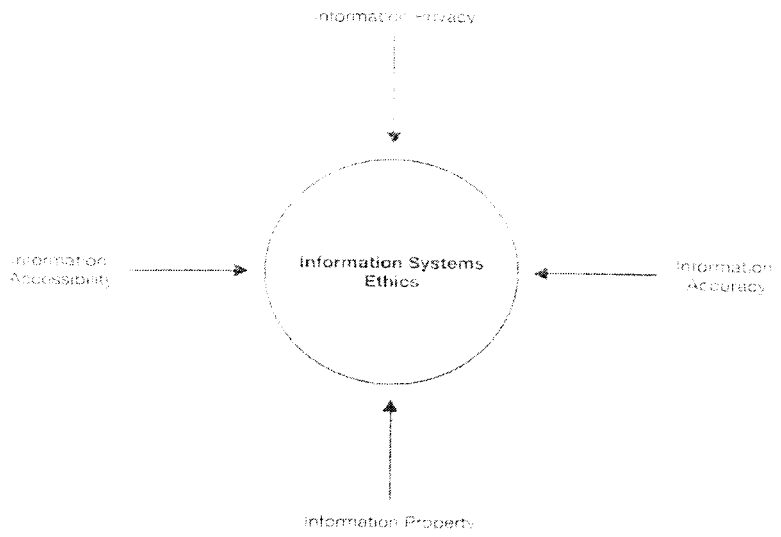
Korporativna pitanja i problemi predmet su regulisanja od strane države, kroz odgovarajuće sistemske zakone. Tako je u „2002, posle podnošenje tužbe za prevaru, odnosno friziranje finansijskih izveštaja i sakrivanja više od četiri miliona dolara troškova, globalna telekomunikaciona kompanija *MCI Worldcom* morala da pokrene postupak stečaja, ali sa zakašnjenjem od godinu dana. Kompanija je u trenutku skrivanja troškova, radi smanjenja osnovice za poreske obračune, ostvarila finansijski efekat na način koji je protivan zakonskim odredbama, ali i protiv etičkih načela koja su joj teže pala, nego čak i vraćanje iznosa od četiri miliona dolara u troškove. Kompanija je nakon otkrivene afere i nemoralnog poteza, uložila dosta energije da obnovi svoj moralni kredibilitet, jer se pokazalo da niko ne želi da posluje sa nemoralnom kompanijom. U cilju povratka povoljne moralne atmosfere i pridobijanja akcionara, kompanija se odlučila da zaposli menadžera za moral i odgovornost Nancy Higgins koja je u isto vreme dobila visok rang u menadžerskoj hijerarhiji, odnosno mesto izvršnog potpredsednika morala. Odmah po imenovanju, novi potpredsednik je napravio plan moralnog treninga za više od 55.000 zaposlenih, uvodeći oficijelni moralni kod, i moralni hotlajn da bi stvorili moralnu i društveno odgovornu kulturu unutar organizacije."[3]

Tako je kompanija *MCI Woldcom* stavila do znanja zaposlenima, ali što je mnogo važnije i poslovnim partnerima, da je moralnost u obavljanju poslova nova korporativna vrednost koju menadžment želi da izgradi, ali i da implementira u sve elemente menadžment procesa. Ovo je u isto vreme bio i strateški potez za brzu konsolidaciju ove kompanije, koji je trebao da manifestuje i novu filozofiju poslovanja, a u cilju pridobijanja poverenja i lojalnosti kupaca, odnosno potrošača.

Paralelno sa navedenim, korporativni menadžment mora da vodi računa i o drugim etičkim vrednostima ili elementima morala. Uvođenjem informatičke tehnologije, potreba za moralom nije prestala, već se pojavljuje u sve većoj ozbiljnosti i u novoj formi, utoliko pre što se određeni propusti i greške u korporativnim organizacijama prebacuju na kompjutere. Iako je na problem etičkih vrednosti još pre dvadeset godina ukazao Richard O. Mason, ovaj problem posebno je dobio na značaju početkom trećeg milenijuma. U informatičkoj eri posebno se insistira na onim elementima koje je dao Mason, odnosno na: privatnosti informacije, preciznosti, vlasništvu i pristupačnosti informacije, što se relativno dobro može videti na sledećem prikazu:[4]

[3] Izvor: Anonimus, "Deloitte Cheif Ethics Officer Tinkler Outlines three critical elements to creating a foundation for an Ethicaly-Managed company: Culture, control, consequencies are the core requirments to ethical security", Deloitte Press Release (March 16, 2004), http://www.deloitte.com/dtt/press_release/0,2309,sid%253D2281%2526cid%253D41724,00html, Anonimus, "MCI names cheif ethic officer", Itworld.com (October 14, 2003). http://www.itworld.com/career/1909/031014mciethics/pfindex.html Anonimus, "WorldCom class action Opt out deadline has been extended", Parker & Waichman http://www.worldcomstockfraud.com.

[4] Prikaz preuzet od: R. Mason: "Four Ethical issues for the Information Age, MIS Quarterly 16 pp. 424.



Slika 1. Masonov prikaz elemenata etike u informacionim sistemima

Ova četiri elementa etičkih informacionih sistema nisu autonomna. Drugim rečima, oni ne deluju samostalno, već jedan na drugi utiču i često se nalaze u uzročno posledičnim vezama i odnosima.

Privatnost u informatičkom društvu

Privatnost je pravo da čovek bude u miru kad to želi, da ima kontrolu nad svojom privatnošću i da ne bude pod prismotrom, odnosno posmatran bez njegovog pristanka. To je pravo da pojedinac bude slobodan od nepoželjnih upada u njegov privatni život. Privatnost ima više dimenzija od kojih su dve najvažnije i to: psihološka i pravna.

Psihološki aspekt polazi od toga da je to potreba za ličnim prostorom. Svaki pojedinac u većoj ili manjoj meri, ima potrebu da se oseća kao da kontroliše svoju najvredniju imovinu ili vrednost. Lična informacija pripada toj listi vrednosti.

Pravno uzevši, privatnost je potrebna za samozaštitu. Ako ključ od kuće sakrijete na posebno mesto u dvorištu, želite da ta informacija ostane lična. Ova informacija može biti zloupotrebljena i naneti vam bol. Postoje specifične oblasti privatnosti kao što su: individualno špijuniranje jedni drugih, korporativna evidencija podataka o radnicima, poslovna evidencija podataka o korisnicima, vladina evidencija ličnih podataka za građanstvo i pitanje privatnosti u internacionalnoj trgovini.

Iako je u demokratskim zemljama nivo sloboda doživeo zavidan nivo, zahvaljujući informatičkoj tehnologiji i neodgovornosti, privatnost je u brojnim slučajevima ugrožena. Dakako, mnogi su svesni da je informatička era razbila fenomen tajni, jer se svaka poruka koju emituje pojedinac ili organizacija preko Interneta skladišti na više mesta. Dakle, iz navedenog se može konstatovati da je mejl potpuno nesiguran instrument komuniciranja. Sadržina mejla je dostupna, kao da sadržaj šaljemo razglednicom. I ne samo to, svaki mejl koji se pošalje ima tri ili četiri kopije koje se čuvaju na različitim kompjuterima i to: na kompjuteru pošiljaoca, kompjuteru servera pošiljaoca, na kompjuteru servera primaoca i na kompjuteru primaoca.[5]

[5] Preuzeto od: H. Stephen i drugih, *Management information Systems – for the information age*, McGraw-Hill, Irwin Boston, 2007., p. 362.

Pokazuje se da danas više nije problem otkriti informaciju, već je očuvati i adekvatno koristiti. Često dolaze mejl poruke sa pozdravima po imenu, nuđenje robe ili usluge, čestitanje rođendana ili važnog jubileja u ličnom i porodičnom životu, do intimnijih stvari, itd. Mnogi zaključuju da se o vlasniku mejla skoro sve zna i da oni koji šalju poruke i pozdrave, manje više imaju formiran stav o pojedincu po pitanju njegovih želja ili robe koju bi najverovatnije želeo da nabavi.

Dakle, svaki dan *inbox* je prepunjen porukama gde se nude proizvodi ili usluge, ponude različitog tipa. Čovek ponekad poveruje da su u informatičkoj eri, sve oči sveta uprte u njega, da su sve informacije koje šalje otvorene i da su privatnost i intimnost dovedeni u pitanje. U pitanju je veliki broj privatnih informacija, kao što su: socijalni sigurnosni broj, broj kreditnih kartica, zdravstveno stanje, imovno stanje, pa čak i istorija familije, porodično stanje. U velikom broju slučajeva, ove informacije možemo videti na Internetu, što je dokaz da je ugrožena privatnost, kao jedna od vrednosti kojoj teže demokratska društva.

Dakako, negativna informacija o pojedincu često ostaje duže vreme na Internetu, kao veliki teret za svakog pojedinca. Ovo je u direktnoj suprotnosti sa organizacionim postavkama, gde je najveći broj korporativnih organizacija regulisao da se kazne i određene sankcije posle određenog vremena brišu iz personalnih dosijea pojedinaca i na taj način se „skidao" teret prošlosti za pojedince ili grupe.

Privatnost i krađa identiteta

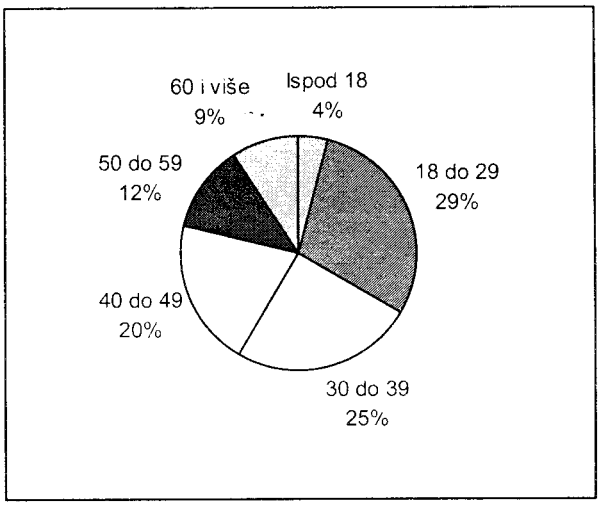
Informatika je uticala na povećanje „informacionog zločina", kao suprotnost moralnom i društveno odgovornom ponašanju kompanija i njihovog menadžmenta. On se manifestuje u različitim formama, ali je u proteklim godinama na intenzitetu posebno dobio problem krađe identiteta. Pod tim pojmom treba podrazumevati krađu broja druge osobe, kao što je lični broj, broj kreditne kartice, stanje na poslovnim računima i druge informacije sa ciljem pribavljanja materijalne ili nematerijalne koristi. U nekim slučajevima, zahvaljujući krađi platne ili kreditne kartice, lopovi direktno podignu novac sa računa žrtve. Pošto mnoge državne i privatne organizacije drže informacije o pojedincima na pristupačnim bazama podataka, postoji mnoštvo prilika za lopove da dođu do vrednih informacija. Vraćati svoj identitet i svoj kreditni rejting može biti frustrirajuće i često zahteva mnogo vremena i napora. Mnogi dožive brojne nerve slomove, a neretko žrtvu dovodi i do oboljenja sa smrtnim ishodima.[6]

Prema istraživanju objavljenom od strane Javelin Strategy and Research, oko devet miliona odraslih u Sjedinjenim Državama bili su žrtve krađe identiteta u periodu od oktobra 2003. do septembra 2004. godine. Biro za uspešniji biznis (*Better Business Bureau*) procenjuje da je prosečni gubitak po ovom osnovu oko 1.000 dolara po osobi, da se ne spominju sati provedeni u ispravljanju kreditnih kartica i predaje zahteva za novim identifikacionim dokumentima, kao što su brojevi socijalnog osiguranja i vozačke dozvole. Federalna trgovinska komisija kaže da trošak krađe identiteta za firme i klijente iznosi čak 60 biliona dolara godišnje.

Krađa identiteta je falsifikovanje nečijeg identiteta za svrhu prevare. Prevara je često zbog finansijske dobiti, i ukradeni identitet se koristi za prijavu i korišćenje kreditnih kartica u ime žrtve ili za prijavljivanje za kredit. Ali takođe može biti jednostavno za prikrivanje identiteta, posebno ako se lopov krije od organa vlasti ili vrši neku prevaru. Na sledećem prikazu data je struktura žrtava po godinama starosti:[7]

[6] O navedenom se može više videti u: D. Radosavljević: „Etika i kompjuterski kriminal", Naučni skup Radmil, Beograd, 2008.

[7] Podaci uzeti iz Izveštaja koji je sačinila FTC-a za 2004.



Slika 2. Starosna struktura žrtava krađe identiteta u SAD
oktobar 2003. – septembar 2004. godine

Iz prethodnog prikaza je vidljivo da je od ukupnog broja prijavljenih lica za krađu identiteta oko 95% njih dalo podatke o godinama starosti, dok to nije učinilo oko 5% žrtava krađe (jer su mlađi od 18 godina). Od ukupnog broja prijavljenih više od polovine pripadaju starosnom dobu od 18 do 39 godini. Uzeto pojedinačno, vidljivo je da najveći broj žrtava krađe identiteta ima populacija starosnog doba od 30 – 39 godina, a da ih slede populacije starosnog doba od 18 – 29, i od 40 – 49. godina. Dakle, kao žrtve krađe identitet se javlja populacija u svim starosnim dobima. Razlika je samo u intenzitetu.

Prethodne podatke potvrđuju i druga istraživanja. Prema podacima IFCC ove federalne organizacije, tipična žrtva prevare je muškarac, u kasnim tridesetim godinama, koji živi u nekim od najnaseljenijih država Amerike. Oni ističu da svakako ovaj profil je najčešće žrtva, ali žrtve su postojale i u drugim profilima, kako polne, tako i starosne i socijalne strukture. Dakle, nesumnjivo je da je Internet postao značajan instrument za svakog čoveka, ali on je postao i bitan za kriminalce i prevarante u sticanju koristi.[8]

Nije jasno zbog čega je relativno visok krađe identiteta u populaciji starosnog doba od 30 – 39 godina, kad se zna da je ona relativno iskusna i po tom osnovu bi trebalo da bude i opreznija u stvaranju šansi da nastane krađa identiteta. U pitanju je verovatno uticaj i drugih faktora.

U nastavku slede primeri krađe identiteta, i posledice koje su se pokazale, nakon što je žrtva otkrila da je bila predmet krađe:

- Osamdesetdvogodišnja žena iz *Fort Worth*, Teksas, otkrila je da je njen identitet bio ukraden kada je žena koja je koristila njeno ime doživela sudar. Ona je 18 meseci, dobijala obaveštenja o tužbi i prekoračenju medicinskih računa koji su u stvari bili namenjeni nekom drugom. Bilo joj je potrebno sedam godina da povrati poverenje, pošto je kradljivac identiteta naplatio preko 100.000 dolara na njenih 12 proneverom stečenih kreditnih kartica.
- Čedrdesetdvogodišnji penzionisani vojni kapetan iz Roki Hila, Konektiket, saznao je da je kradljivac identiteta potrošio 260.000 dolara kupujući proizvode i usluge koja uključuju dva kamiona, „harley davidson" motor i periodično deljenu vikendicu u Južnoj Karolini. Žrtva je otkrila svoj problem, tek kada je njegova penzija obustavljena kako bi se isplatili ogromni dugovi.

[8] Izvor: Anonimus, "IFCC 2002 Internet Fraud Report January 1, 2002 – December 31, 2002", http://www.ifccfbi.gov./strategy/2002_IFCCReport.pdf, P. Thibodeau, "Ninty arrested for internet fraud in FBI sweep", Computerworld (May 23, 2001). http://www.computerworld.com

- U Njujorku, članovi džeparoškog kruga falsifikovali su vozačke dozvole njihovih žrtvi za nekoliko sati od krađe ženskih tašni. Džeparoši znaju ako se ukrade nečija tašna, plen obično neće biti veći od 200 dolara, verovatno mnogo manji. Sa druge strane, ako ukrade identitet osobe, može zaraditi prosečno između 4.000 i 10.000 dolara.
- Jedna kriminalna banda je uzela osam miliona dolara vredne hipoteke na žrtvine kuće. Ispostavilo se da je izvor svih instanci krađe identiteta došao od dilera automobilima.
- Do danas najveću krađu identiteta u istoriji Sjedinjenih Država prekinula je policija 2002. kada su otkrili da su tri čoveka skinuli kreditne kartice koristeći ukradene lozinke i prodali ih kriminalcima na ulici po pojedinačnoj ceni od 60 dolara. Na ovaj način ukradeno je nekoliko desetina miliona dolara od žrtava iz svih 50 država SAD.[9]

Imajući u vidu navedeno Federalna trgovinska komisija SAD daje savete, šta pojedinci treba da čine, kako bi sprečili krađu privatnosti i šta žrtva treba da čini u slučaju već izvršene krađe identiteta. Slično čine i korporativne bankarske, trgovinske i druge organizacije. Konačno, vrši se i obuka i trening osoblja u uslužnim organizacijama kako bi se brzo reagovalo na prijavu o krađi identiteta.

Pravna regulativa o privatnosti

Imajući u vidu značaj privatnosti za svakog pojedinca, veliki broj zemalja nastoji da ovo pitanje reguliše putem određenih pravnih normi, često i najvišeg ranga, kao što je ustav. Međutim, pokazuje se da na tom planu ne postoji harmonizacija, čak i u najdemokratskijim zemljama sveta. Tako, Sjedinjene Države nemaju dosledan set zakona koji štite privatnost informacija, iako su se neki zakoni pokazali opravdanim. To je slučaj sa donetim Zakonom o zdravstvenom osiguranju (Health Insurance Portability and Accountability Act - HIPAA) koji je donet 1996. godine sa ciljem zaštite informacija o pacijentima. Zakon je propisao sledeće:[10]

- Da se ograniči korišćenje zdravstvenih informacija bez odobrenja pojedinca;
- Da se pacijentima omogućava pristup kartonima i da imaju pravo da steknu uvid ko je još koristio njegov karton;
- Da se procenjuju okolnosti pod kojima istražni organi i ostali mogu da pregledaju medicinske kartone;
- Da se obelodane samo one informacije o zdravlju koje se moraju objaviti;
- Da se dozvoli obelodanjivanje zaštićenih zdravstvenih informacija za poslovne razloge sve dok primalac prihvata, napismeno, da štiti tu informaciju.

SAD je donela i druge zakone da bi se uspostavila pravna regulativa iz informatičke oblasti. Zakon o modernizaciji finansijskih usluga zahteva da finansijske institucije štite lične informacije potrošača i da imaju odobrenje potrošača, pre nego što podele takvu informaciju sa drugim preduzećima. Međutim, zakon sadrži klauzulu koja dozvoljava deljenje informacija za svrhe legitimnog poslovanja, kao što su finansijski izveštaji potencijalnim investitorima i drugim zainteresovanim subjektima sve do objavljivanja istih u javnim sredstvima informisanja ili formiranjem posebnih agencija za pružanje pomoći u uspešnosti kompanija.

[9] Detaljnije o navedenom se može videti u: S. Haag i drugi: Management information systems – for the information age", McGraw Hill, Irwin, Boston, 2007. p. 363.

[10] Više o navedenom može se pronaći u Serbanes-Oxley u Extended Learning Module H: Computer Crime and Forensics

Rešenje problema narušavanja privatnosti informacije, posebno krađe identiteta leži u saradnji državnih i korporativnih organizacija i promene u praksi korišćenja i prepoznavanju identiteta, odnosno u podizanju kulture zaposlenih po ovom pitanju. Dakle, korporativni menadžment ne može ostati po strani po pitanju dešavanja u okruženju. S obzirom na to da su zaposleni deo okruženja, korporativni menadžment putem edukacije može da utiče na smanjenje ovog problema, kako zaposleni ne bi imali štete po ovom osnovu. Na primer, majčino devojačko ime ili socijalni broj se može lako naći, i podaci iz prošlosti ili od predaka iskoristiti u negativnom kontekstu, što se i dešavalo, a i danas dešava u zemljama tranzicije. Ali u informatičkom dobu, kao mera zaštite se mogu koristiti tehnike biometrike i enkripcije, da bi se identitet sačuvao i na taj način otežalo lopovima da do istog dođu.

Za kvalitetnu analizu i razmatranje problematike etike u informacionom dobu, potrebno je odrediti odnos između nemoralnog ponašanja i kriminala. Krađa identiteta je očigledno kriminal. Svakako, mnoga „iskorišćavanja" kompjuterskih informacija možda nije kriminalno delo, ali mnogi smatraju nemoralnim radnjama i postupcima, pa se kao takvi i nemoralno ocenjuju. Kako tehnologija napreduje i dozvoljava ljudima da rade nešto što nisu mogli ranije raditi, postojeći zakoni često se ne primenjuju za te novonastale situacije. Zato se često u raspravama i potеže pitanje da li nešto što nije kriminalno, može u isto vreme biti i moralno, odnosno da li je svaki zakonski postupak u isto vreme i moralan.

Korporativna odgovornost za zaštitu privatnosti zaposlenih

Korporativni menadžment, kako je konstatovano ima višedimenzionalnu odgovornost. Međutim, njegova primarna odgovornost je prema zaposlenima, utoliko pre što se od zaposlenih zahteva da deponuju svoje lične podatke, kao i njihovo permanentno ažuriranje i usklađivanje sa stvarnim stanjem. Neretko se kroz socijalne karte zahteva čak i imovno stanje zaposlenih, kako bi se kroz poseban set privilegija isti doveli na nivo prosečnosti u životnom standardu.

Kompanije raspolažu detaljnim podacima o svakom zaposlenom. Podaci se dostavljaju prilikom konkurisanja, iako je evidentno da najveći broj prijavljenih neće biti primljen. Prijave na konkurs koje nisu praćene traženim podacima odbacuju se, tako da su ljudi prinuđeni da daju tražene podatke. Njihovi podaci su evidentirani u odgovarajuće preglede i liste, tako da ostaju u kompaniji i nakon povratka originalne dokumentacije na osnovu koje su i konkurisali.

Praksa pokazuje da se ljudi protive što je toliko detalja o njihovim životima dostupno drugima. Pored identifikacionih ličnih podataka, potencijalni poslodavci ili bilo ko drugi, može saznati kreditno stanje, upotrebu telefona, pokrivenost osiguranjem i mnoge druge zanimljive stvari. Poslodavac takođe može pribaviti informacije o tome šta je konkurisano lice radilo u prošlosti, kakav je rejting imao na ranijem radnom mestu ili koji je raniji problem bio sa poslodavcem. Poslodavac može da pita kandidata i o nekim ličnim stvarima, čak i da uzme test na drogu, kao što to čini veliki maloprodajni sistem *Wal-Mart* i test inteligencije, čiji rezultati postaju vlasništvo kompanije.[11]

Pošto se osoba primi, poslodavac može da prati i nadgleda osobu, i to: gde ide, šta radi, šta priča i šta piše, od koga dobija i kome šalje mejlove – barem tokom radnog vremena. Neke kompanije, posebno u nedemokratskim zemljama, žele da kontrolišu odlazak zaposlenih u druge zemlje ili kompanije, te kontrolisanje šta su zaposleni govorili o svojoj kompaniji, itd. Američka menadžerska asocijacija kaže da je od marta 2005. godine oko 60% procenata poslodavaca pratilo mejlove radnika, kako dolazeće tako i odlazeće, što je bilo značajno povećanje, jer je ta cifra u 2001. godini iznosila oko 47%.[12]

[11] Ž. Radosavljević, *Ekonomika trgovine*, CERK, Beograd, 2006, str. 341.

[12] Prema: Kris Maker i drugi: „Snooping E-mail by Software is Now a Workplace Norm", The Wall Street Journal, march 9, 2005, pp. B1 – B2

Jedan od razloga zašto korporativni menadžment prati mejlove radnika je što kompanije mogu da budu tužene za ono što radnici šalju jedni drugima i ljudima izvan firme i da po tom osnovu isplaćuju štetu.[13]

Oko 70% veb saobraćaja odvija se tokom radnog vremena. Ovo je dovoljan razlog za kompanije da prate šta i koliko dugo, radnici traže na vebu. Federalna organizacija FBI izveštava, da 78% anketiranih kompanija navodi da su radnici zloupotrebili internet privilegije, skidajući pornografiju, piratski softver ili nekom drugom radnjom koja nije poslovno orijentisana. Takođe, 60% radnika je istaklo da je na poslu posetilo veb-sajtove ili surfovalo za sopstvene potrebe. Zbog navedenog došlo je do tzv. paradoksa u internet produktivnosti. Dakako, ovaj paradoks manifestuje se u činjenici da uvođenjem informatičke tehnologije trebalo i da raste produktivnost u administrativnim stručnim poslovima. Do toga ipak ne dolazi u velikom broju organizacija, jer se veliki deo vremena provodi na Internetu, koristeći ga za svoje potrebe.

Firme imaju dovoljno razloga za traženje i čuvanje ličnih informacija o radnicima. One:

- Žele da zaposle najbolje moguće radnike i da izbegnu da ih tuže zbog istraživanja njihovih ličnih podataka i istorije rada;
- Poslodavci žele da budu sigurni da se članovi osoblja ponašaju pristojno i da ne troše ili upotrebljavaju resurse kompanije na pogrešan način. Finansijske institucije su čak zakonski obavezane da prate sve komunikacije uključujući mejlove i telefonske razgovore;
- Mogu biti odgovorni za postupke njihovih radnika, kao što je to bio slučaj sa Shevronom i Microsoftom.

Imajući u vidu navedeno, kompanija izgrađuje tehnologije i koncepte za nadgledanje ponašanja zaposlenih po navedenim pitanjima. Postoje softveri koji mogu da skeniraju mejlove, kako dolazeće tako i odlazeće. Softver može da traži specifične reči ili fraze u naslovu poruke ili u samom tekstu poruke. Program koji skenira mejlove može da se ugradi u kompjuter u obliku trojanca. Odnosno, može da se sakrije u mejl običnog izgleda ili neki drugi fajl ili softver.[14]

Neke kompanije koriste manje napadan pristup od stvarnog čitanja mejl poruka radnika. Njihovi programi za pregled mejlova proveravaju samo određeni nivo mejlova na i sa neke adrese. Ovo nagoveštava da možda postoji problem i radnik se obaveštava o situaciji i biva upućen da to ispravi. Napadno nadgledačko, odnosno „njuškanje" i u opravdanim slučajevima nailazi na reakciju zaposlenih.

Poslodavac može da prati aktivnost tastature i miša sa nekom vrstom *key logger* softvera o kome je pojedinac čitao u prethodnom delu. Alternativa koja se ponekada teže detektuje je hardverski *key logger*, odnosno uređaj koji hvata otkucaje na tastaturi na putu od tastature do matične ploče. Ovi uređaji mogu biti u obliku konektora na sistemskoj jedinici na kraju kabla između tastature i sistemske jedinice.

Istraživanja pokazuju da ima malo simpatija u legalnom sistemu za procenjenih 27 miliona radnika za koje Američko menadžersko udruženje kaže da su pod prismotrom. Poslodavci imaju zakonsko pravo da nadgledaju upotrebu njihovih resursa, uključujući i način korišćenja radnog vremena za koje su plaćeni da obavljaju poslove. Nasuprot kućnom okruženju, nemate očekivanja za privatnošću kada koristite kompanijske resurse.

Poslednji federalni zakon koji se odnosio na elektronsko nadgledanje radnika je Akt o privatnosti elektronskih komunikacija iz 1986. godine. Mada, uopšteno, zabranjuje presretanje žičanih ili elektronskih komunikacija, ima izuzetke i za slučajeve za koje su imali raniji pristanak i za poslovnu upotrebu.

---

[13] Tako na primer, korporacija Chevron i Microsoft su se nagodili za seksualna uznemiravanja cifrom od 2. 2 miliona dolara pojedinačno, zato što su radnici slali uvredljive mejlove drugim radnicima, a uprava nije intervenisala. Druge kompanije kao što su Dow Chemical Company, Xerox, New York Times Company, i Edward Jones preduzeli su preventivne mere tako što su otpuštali ljude koji su slali ili čuvali pornografske ili nasilne mejl poruke. Citirano prema: D. Corbin: „Keeping a Virtual Eye on Employees", Occupational Health and Safety, Novembar 2000. pp. 24–28.

[14] L. Pilagas: „Learning IT Right from Wrong", InfoWorld, October 2, 2000, pp. 39 – 40.

Neki državni zakoni su se posvetili problemu i istraživali koliko daleko poslodavci mogu otići i šta mogu da urade da bi pratili radnike. Konektiket ima zakon koji je stupio na snagu 1990. godine, a koji zahteva od poslodavaca u privatnom sektoru da pismeno obaveste radnike o elektronskom nadgledanju. A Pensilvanija, godinu dana ranije, dozvolila je telemarketerima da prisluškuju pozive u svrhu kontrole kvaliteta, dok god je bar jedna strana svesna tog postupka.[15]

Korporativna odgovornost za zaštitu privatnosti kupaca-potrošača

Kompanije se suočavaju sa velikim brojem dilema u donošenju upravljačkih korporativnih odluka. Ipak, za kompaniju najveći značaj imaju kupci, odnosno potrošači, zbog čega oni nastoje da upoznaju iste, po brojnim pitanjima, kako bi ovladali, ali i upravljali njihovim zahtevima, ili potrebama. Razlozi za upoznavanje kupaca se nalaze u sledećem:

- Kompanije hoće da znaju ko su njihovi potrošači. Međutim, potrošači žele da ih kompanije što je moguće više ostave na miru;
- Potrošači žele da im kompanije obezbede ono što im je potrebno i što hoće, ali, u isto vreme, ne žele da kompanije znaju previše o njima samima i njihovim željama, navikama i osobinama;
- Potrošači hoće da ih kompanije obaveste o proizvodima i uslugama koje bi možda želeli da imaju, ali ne žele da budu preplavljeni sa ubitačnim reklamama.

Dakle, enormne količine ličnih informacija su dostupne kompanijama iz različitih izvora, kao što su: sajtovi, statistika, časopisi, korporativne publikacije, itd. Relativno veliki veb-sajt može dobiti oko 100 miliona podataka pretrage na dan, što znači da sajt dobija oko 200 bajtova informacija za svaki pogodak pretrage. To je oko 20 gigabajta informacija na dan. Ovaj nivo priliva informacija je pomogao da sistem elektronskog upravljanja odnosima sa potrošačima (electronic customer relationship managenent - eCRM) postane jedna od oblasti sa najbržim rastom softverske industrije. Deo održavanja potrošačkih odnosa je personalizacija. Veb-sajtovi koji često pozdravljaju po imenu i *amazon.com* poznate preporuke „ljudi koji su kupili ovaj proizvod takođe su kupili i deo kompanije" su primeri personalizacije, koja je omogućena veb-sajtovima znanjem o pojedincima.[16]

Osim toga što može da prikupi potrebne informacije o potrošačima, kompanija može spremno da pristupi informacijama o korisnicima na drugom mestu. Kompanije za kreditne kartice prodaju informacije, kao i Popisni biro i kompanije za mejling liste. Kompanije za praćenje veb saobraćaja kao što je DoubleClick prate pojedince (i druge surfere) kroz veb i onda prodaju informacije o tome gde je neko išao, koliko dugo se zadržao. DoubleClick može tokom vremena sakupiti informacije o bilo kome i proslediti svojim korisnicima veoma profilisan link. DoubleClick je takođe i posrednik za kompanije koje žele da se reklamiraju veb surferima. Kada je unajmljen od strane kompanije koja želi da proda nešto, DoubleClick identifikuje ljude koji bi možda bili zainteresovani i šalje reklame njima u obliku banera ili pop-up prozora. Zagovarači ove prakse tvrde da je dobro za surfere zato što dobijaju ciljane reklame i manje nepoželjnih reklama. Svako može proceniti koliko je istinita ova izjava. DoubleClick je, u početku, otpočeo sa praćenjem korisnika bez povezivanja njihovih identiteta sa informacijama. Zatim, 1999. godine DoubleClick promenio je svoju politiku i najavio da će prikačinjati imena korisnika sa ličnim informacijama i mejl adresama. Međutim, kao odgovor na negativnu reakciju potrošača, DoubleClick je povukao svoju najavljenu promenu. Zanimljivo,

[15] Prema American Business Review, January 2000, pp. 107 – 114.
[16] Prema C. Medfordu: „Know Who I am", PC Magazin, February No 7, 2000. pp. 58 – 64.

DoubleClick nije naveo da nikada neće nastaviti napuštenu politiku, ali je samo pristao da sačeka dok standardi za takvu politiku ne dođu na svoje mesto.[17]

Treba na kraju napomenuti da čak iako kompanija obećava i namerava da zaštiti informaciju klijenata, to često ne čini. Kada se suoči sa sudskim nalogom, kompanija se mora odreći zapisa o korisnicima. Štaviše, sudovi su presuđivali u slučajevim bankrota kompanija da su korisnički fajlovi roba, kao i svaka druga koja se može prodati, da bi se namirila dugovanja.

Načini očuvanja privatnosti na on-lajn kupovini

Pitanje zaštite privatnosti se nemeće kao logično i neophodno, jer se pokazuje da i u informatičkom dobu, niko ne može sačuvati privatnost pojedinca, ukoliko to on prethodno ne učini. Ukazivanje na načine očuvanja privatnosti je preventiva koja sprečava da ona bude i iskorišćena i zloupotrebljena.

Praksa pokazuje da pojedinci pri kupovini na kredit moraju iscrpno popunjavati formular radi odobravanja kredita. Na formularu postoje bitni podaci privatnosti. Bez ovih podataka kreditna kupovina se ne bi mogla realizovati. Ista je situacija i sa podizanjem pozajmice kod bankarskih i drugih finansijskih institucija, podizanju vaučera za turističko putovanje, pa i podizanje avionske karte.

U svim ovim situacijama, kao i kupovina putem Interneta, prodavac nije dužan, niti ima zakonskih obaveza da poštuje i čuva privatnost klijenta. Drugim rečima, prodavac može da prati klijenta i vidi koju robu gleda, koju gleda detaljno, a koju improvizovano, koji je proizvod odabrao i na kraju kupio, koji metod plaćanja je koristio i na kraju adresa na koju robu treba isporučiti. Posle sakupljanja svih navedenih informacija, nesavestan prodavac, ili bankarski službenik, radnik turističke agencije itd. može da proda tu informaciju drugima, da je ustupi besplatno, itd. Rezultat toga može biti dolazak poziva na kućnu ili mejl adresu sa molbom da se objavi oglas, kupi neka roba ili usluga, ili da se bude donator u korisnoj akciji nevladinih organizacija. Pored poruke, na adresu klijenta može doći i elektronski spam ili pozivi telemarketinga.

Praksa i istraživanje potrošača po ovom pitanju su evidentni. Oni su u brojnim anketama bili zabrinuti on-lajn kupovinom. Većina klijenta je zabrinuta zbog ugrožavanja privatnosti i mogućnosti odavanja privatnih informacija tokom kupovine. Udruženja za zaštitu potrošača su reagovala i vršila pritisak na državne organe da prodavce učine odgovornijim prilikom korišćenja informacija o privatnosti na svojim veb stranicama. Nažalost, često ta obaveštenja i pritisci ne štite na pravi način pravo potrošača na privatnost.

Da bi zaštitili sebe, potrošači treba da pogledaju i dokument koji govori o privatnosti, kao što je to misija organizacije ili strategija komuniciranja sa potrošačima. Shodno navedenom, potrošač se treba odlučiti za kupovinu kod onog prodavca koji garantuje privatnost. Mnogi su čak spremni da plate i veću cenu, ukoliko im je obezbeđena zaštita privatnosti. Mnoga udruženja potrošača insistiraju kod prodavaca da istaknu listu mera koje preduzimaju u vezi sa zaštitm privatnosti. Relativno dobra slika u nivou zaštite privatnosti može se videti na listi koju je formulisalo Udruženje potrošačke zaštite. Ova lista treba da pokazuje sledeće elemente:[18]

- Koje informacije prodavac sakuplja od klijenta;
- Kako će prodavac koristiti informaciju;
- Kako se može „prekinut" saradnja i povući podaci.

[17] Uz modifikaciju preuzeto od: D. Charters: Electronic Monitoring and Privacy Issues in Business_Marketing: The Ethics, of the DoubleClick Experience", Journal of Business Ethics, February 2002. pp. 243 – 254.
[18] Radna grupa Američkog Bar-a na safeshopping.org.

Najveći deo mera i aktivnosti u vezi sa zaštitom privatnosti je ipak u rukama potrošača. Zato pojedinci koji imaju nameru da kupuju, ili koriste usluge pojedinih uslužnih kompanija, mogu da naprave dodatne korake, kako bi bili sigurni, u zaštitu svoje privatnosti. Radi se o sledećim merama, i to:

- Izabrati sajtove koji su nadgledani od strane nezavisnih, odnosno nevladinih organizacija. Nekoliko nezavisnih organizacija nadgledaju poštovanje privatnosti i poslovnu praksu veb- sajtova. Primera radi, organizacije kao što su http://www.epubliceye.com i http://www.openratings.com, obezbeđuju važnu uslugu potrošačima, tako što nadgledaju poslovnu praksu prodavca i potvrđuju standard ili ističu i preporučuju kupovinu kod istog. Birajući sajtove koji su ocenjeni od strane nezavisnih kompanija sa jakom reputacijom, relativno je dobar način da se osigura privatnost.
- Izbegavati primanje *cookies* na računaru. Mnogi komercijalni veb-sajtovi napravljeni su tako da ostave *mali fajl* na hard disku da bi vlasnik mogao da nadgleda gde pojedinac ide i šta radi na sajtu. Moguće je da vlasnik sajta dobije mejl adresu od posete i potencijalno da pošalje nepoželjni spam na vaš mejl. Na sreću, mnogi veb čitači nude opciju za isključenje *cookies* ili imaju opciju u vezi sa prihvatanjem istog. Uz niz dodatnih podešavanja veb čitača, može se nabaviti specijalni „upravljači" *cookies* programe za zaštitu privatnost.[19]
- Sajtove treba posećivati anonimno, zašto postoje tehnička rešenja. Koristeći usluge kompanije kao što je Anonymizer (http://www.anonymizer.com/index.cgi), obezbeđuje se potpuna privatnost od marketinga, krađe identiteta, pa čak i od poslovnih kolega, dok se surfuje veb stranicama. Njihov softver blokira *cookies*.
- Treba biti pažljiv kada kupac zahteva mejl za potvrđivanje. Kad se kupuje proizvod on-lajn, mnoge kompanije šalju mejl radi potvrde da je porudžbina pravilno isporučena. Ako se koristi računar koji se deli sa drugim ili se kupuje putem računara s posla gde određene aktivnosti mogu biti praćene, treba paziti na zaštitu privatnosti kupovine. Dobra strategija je da kupac ima poseban mejl nalog, kao što postoje na veb čitaču, koji se uglavnom koristi tokom on-lajn kupovine. Na primer, *Hotmail, Yahoo!, Excite*, i mnogi drugi veb portali nude besplatnu mejl uslugu, kojom se može pristupiti, koristeći standardni veb čitač. To dozvoljava da se sačuva primarna mejl adresa daleko od nesavesnih prodavaca i marketinga i takođe sačuva lično poslovanje od nekog ko možda ima pristup računaru.

Naravno, nema apsolutne garancije da će sva on-lajn komunikacije biti bez problema, ali ako se prate navedena uputstva, verovatno će se smanjiti mogućnost zloupotrebe privatnosti, odnosno preživeti i uspeti u svetu on-lajn trgovine.

Zaključak

U savremenom svetu najveći problem više ne predstavlja prikupljanje i manipulacija podacima, već stvaranje bezbednih uslova za njihovo čuvanje. U savremenim uslovima potrebno je obezbediti takav sistem u kome neće biti ugroženi ni podaci, ni ljudi na koje se ti podaci odnose. Informacije se moraju koristiti na etičan način uz zaštitu privatnosti, kako svojih, tako i drugih ljudi.

Privatnost je normalna težnja svake osobe i ogleda se u ispoljavanju želje za kontrolisanjem svog života i da bude ostavljena na miru kada to želi. Ovaj problem je danas veoma izražen, imajući u vidu da se gotovo čitav život nalazi na Internetu, odnosno da se svi lični podaci čuvaju u elektronskoj formi, a da su računari povezani u globalnu mrežu. Navedeno ostavlja mogućnost zlonamernima da zaobiđu bezbedonosne sisteme i iskoriste informacije o pojedincima. Na primer, osoba može da pretrpi velike štete ukoliko joj napadač „ukrade identitet", tj. nakon što pribavi podatke, kao što su brojevi kreditnih kartica i slično, iskoristi iste za

[19] Više o navedenom može se pogledati u http://www.cookiecentral.com gde se može naći i više *cookise* upravljačkih opcija

kupovinu stvari koje su mu potrebne. Iako se na prvi pogled čini da su kompjuterski sistemi veoma bezbedni, u stvarnosti se vrlo često dešavaju prevare koje ponekad pogađaju milione ljudi često sa tragičnim ishodima.

Kao što se iz navedenog može zaključiti, država i korporacije moraju stvoriti preduslove za bezbedno čuvanje podataka, kako ne bi pali u pogrešne ruke. Pod ovim se podrazumeva da se upotrebe sva visokotehnološka rešenja (antivirusni programi, *firewall*, programi protiv *spyware*...), ali i klasične metode zaštite od fizičkih krađa. Posebno treba obratiti pažnju na unutrašnju kontrolu, odnosno kontrolu zaposlenih, jer se često dešava da velike štete nastaju zbog neodgovornog ili čak zlonamernog ponašanja pojedinaca ili grupa u samoj organizaciji.

Literatura

[1] Anonimus, *Deloitte Cheif Ethics Officer Tinkler Outlines three critical elements to creating a foundation for an Ethicaly-Managed company: Culture, control, consequencies are the core requirments to ethical security*, Deloitte Press Release 16.03.2004.

[2] Charters, D., *Electronic Monitoring and Privacy Issues in Business Marketing: The Ethics, of the DoubleClick Experience*, „Journal of Business Ethics", II/2002.

[3] Haag, S., *Management information systems – for the information age*, McGraw Hill, Irwin, Boston, 2007.

[4] Maker, K., *Snooping E-mail by Software is Now a Workplace Norm*, „The Wall Street Journal", 09.05.2005.

[5] Mason, R., *Four Ethical issues for the Information Age*, MIS Quarterly 16.

[6] Medfordu, C., *Know Who I am*, PC Magazin, 07.02.2000.

[7] Pilagas, L., *Learning IT Right from Wrong*, InfoWorld, 02.10.2000.

[8] Radosavljević, D., „Etika i kompjuterski kriminal", *Naučni skup Radmil*, Beograd, 2008.

[9] Radosavljević, Ž., *Ekonomika trgovine*, CERK, Beograd, 2006.

[10] Stephen, H. i dr., *Management information Systems – for the information age*, McGraw-Hill, Irwin Boston, 2007.

[11] Tofler, A., *Treći talas*, Otokar Keršovani, Rijeka, 1992.

[12] www.deloitte.com (dtt) press_release, 14.10.2004.