Stručni članak
658.8:342.738
366.5:658.8
Primljeno: 6. rujna 2005.

Zaštita privatnosti i sigurnost pohranjenih podataka s osvrtom na izravni (direktni) marketing

MIRNA SUDAR-KULČAR*

Sažetak

Zaštita privatnosti i sigurnost podataka sve više dobivaju na važnosti u poslovanju. Istodobno se povećava zabrinutost potrošača zbog moguće zlouporabe njihovih osobnih podataka. Zbog toga su doneseni novi zakoni i pravila ponašanja, kako u svijetu, tako konačno i kod nas, kojima se regulira način na koji treba komunicirati s potrošačima i određuju se kazne za one koji ne poštuju pravila pristojnosti, nenametljivosti i sigurnosti.

Izravni marketing pretpostavlja izravnu komunikaciju s potrošačima i interesentima. Baze podataka s njihovim imenima, adresama, kupovnim navikama i sl. podloga su za kreiranje uspjelih kampanja ciljanoga marketinga. Izravnim marketerima koji odašilju svoje promotivne materijale potencijalnim kupcima od iznimnog su značenja popisi adresa. Katkad potrošači nisu zadovoljni aktivnostima marketera zbog straha od neodgovornoga korištenja njihovih podataka, narušavanja privatnosti i dodijavanja.

Ključne riječi: zaštita privatnosti, sigurnost podataka, zakoni i propisi, novi aspekti marketinga, izravni marketing, politika zaštite privatnosti

Primjena novih tehnologija (osobito informacijske i komunikacijske tehnologije) u svim područjima ljudskih djelatnosti, od gospodarstva, obrazovanja, znanosti do kulture, sporta i ostalog, pokretač je društvenog i gospodarskog razvoja i prosperiteta svake zemlje. Brz i jednostavan način prikupljanja, pohranjivanja, obradbe, prenošenja, razmjene, pristupa i korištenja velikih količina najrazličitijih podataka i informacija[1] svakodnevna su poja-

* *Mirna Sudar-Kulčar,* doktor znanosti iz područja ekonomije.

[1] Razlika između podatka i informacije jest u tome što informaciju čine obrađeni podatci stavljeni u određeni kontekst.

va u gotovo svim segmentima ekonomskih i društvenih aktivnosti. Sve veći zahtjevi i potražnja za brojnim informacijama rezultirali su stvaranjem niza zbirki (baza) podataka. Glavnina pohranjenih podataka odnosi se na osobne (privatne) podatke pojedinaca. Gotovo da nema ustanove ili tvrtke koja ne koristi takve zbirke podataka.

Državna tijela, agencije i institucije koriste ih za potrebe evidencije i izradbe različitih analiza, izvješća i odgovarajućih programa. Tvrtke prikupljanjem podataka o potrošačima, korisnicima i interesentima nastoje prilagoditi proizvode i usluge njihovim potrebama i unaprijediti svoje poslovanje. Neprofitne organizacije pokušavaju približiti i osvijestiti kod određenih skupina ljudi ulogu i značenje odabranih projekata za cijelu društvenu zajednicu. Političke se stranke trude predstaviti programe što većem broju osoba, poglavito onima o čijim stajalištima, željama i mišljenjima imaju određene spoznaje, a vjeruju da bi mogli pridobiti njihove glasove. Kulturne i sportske institucije analizom pohranjenih podataka o hobijima i sklonostima pojedinaca dolaze do dragocjenih informacija temeljem kojih lakše osmišljavaju svoju ponudu u nadi privlačenja što većeg broja stalnih posjetitelja, tj. pretplatnika.

Mogli bismo još nabrajati. Međutim, zbog dosad navedenoga lako je zaključiti da će se taj trend nastaviti i ubuduće, ali uz korištenje sve sofisticiranije tehnologije koja uz brojne prednosti ima i niz nedostataka vezanih uz pojavu nedopuštenog i zakonom umnogome sankcioniranog djelovanja. Prednosti uključuju profitabilnije, jednostavnije i brže poslovanje, uspjeliji nastup na domaćem i inozemnom tržištu, kvalitetnije programe prilagođene stvarnim potrebama pojedinca i zajednice, sniženje troškova, bolji standard i sigurnije okruženje (vezano uz zaštitu okoliša, održiv razvoj, učinkovitiju obranu od terorizma i različitih oblika kriminala). Nedostatci se očituju u sve većoj zabrinutosti ljudi što se zadire u njihove slobode i pravo na privatnost, primjerice primjenom (RFID)[2] tehnologije, tj. radiofrekvencijske identifikacije koja omogućuje praćenje; uvođenjem elektroničke, biometrijske putovnice[3] koja osim uobičajenih podataka na čipu sadržava pohranjene podatke o vlasniku putovnice, digitalnu fotografiju, potpis, otisak prsta; korištenjem

[2] Radio Frequency Identification (RFID) – ugradnjom mikročipova na palete, transportne kutije, proizvode (od primjerice kozmetike do odjeće), iskaznice (u školama, knjižnicama), kartice trgovačkih kuća, prati se njihovo "kretanje" i ti se podatci registriraju u bazi podataka. Uz nesumnjive koristi navedene tehnologije vezano uz smanjenje troškova praćenja zaliha, preciznost i brzinu isporuke, povećanje prometa, smanjenja broja krađa, navedena je tehnologija izazvala burne reakcije mnogobrojnih udruženja koja vode brigu o zaštiti privatnosti potrošača (CASPIAN – *Consumers Against Supermarket Privacy Invasion and Numbering*; FoeBud – njemačka udruga).

[3] Večernji list od 17. lipnja 2005. članak "Od listopada obvezne biometrijske putovnice", str. 15 – SAD uvjetuje zemljama čiji građani ne trebaju vizu za ulazak u SAD posjedovanje elektroničke putovnice.

bežičnih uređaja i modernih softverskih programa radi trenutačnoga dobivanja detaljne povratne informacije o određenoj osobi putem povezivanja s različitim zbirkama podataka[4], snimanjem na javnim mjestima bez znanja i pristanka onoga koga se snima.[5] Strah od zlouporabe prikupljenih podataka svakim je danom sve veći s obzirom na pojavu krađe identiteta[6], *phishing*[7] – lažne dojave o osvajanju nagrada, te *skimming*[8]. Napastovanje i uznemiravanje telefonom, telefaksom, poštom ili elektroničkom poštom radi nuđenja netraženih proizvoda i usluga postala je uobičajena praksa neodgovornih tvrtki koje se bave telemarketingom.

Pojava Interneta, koji je danas postao globalni medij, promijenila je način života i poslovanja nametnuvši nova pravila ponašanja, ali i nužnost pojačane kontrole i kažnjavanja njegove uporabe za neprimjerene ili nedopuštene djelatnosti.

Kako bi se spriječile negativne pojave vezane uz pohranjivanje i raspolaganje osobnim podatcima, neprimjereno korištenje Interneta, elektroničke pošte i telefona u brojnim su zemljama Europe i Amerike državna tijela, kao i različite institucije direktivama, zakonskim mjerama, propisima, kodeksima ponašanja i smjernicama nastojali regulirati način na koji se mogu koristiti podatci i informacije o pojedincima koje u svojim zbirkama čuvaju brojne tvrtke ili institucije, te kako se treba ponašati na Internetu. Regulativa uključuje pravila ponašanja i uvjete poslovanja pravnih osoba, te dopustiv način komuniciranja s korisnicima i potrošačima.

[4] Programom Matrix koji je financiran iz federalnog proračuna SAD-a američka policija ima mogućnost trenutačnog pristupa bežičnim prijenosnim uređajima, kako svojim zbirkama podataka, tako i podatcima različitih komercijalnih baza podataka (izvor: Večernji list od 7. srpnja 2004. članak "Zaštita prava građana ili ugrožavanje privatnosti").

[5] Primjerice, prema istraživanjima, jedna petina svih kamera na svijetu služi za videonadzor; u Velikoj Britaniji na 14 stanovnika dolazi po jedna kamera zatvorenoga televizijskog sustava (izvor: Večernji list od 18. siječnja 2004. članak "Svaki Londončanin dnevno snimljen 300 puta", str. 51).

[6] Engl. *Identity Theft* – podrazumijeva prijevaru korištenjem i krivotvorenjem tuđih podataka radi dobivanja kredita ili kreditnih kartica.

[7] Primatelja se elektroničkom poštom ili SMS-porukom obavještava da je osvojio neku nagradu u novcu, stvarima ili atraktivan put u inozemstvo, te ga se umoljava da dostavi svoje podatke (broj bankovnog računa, adresu, fotokopiju putovnice). Ako "dobitnik" odgovori na poruku i dostavi tražene podatke, zatraži ga se da dostavi određenu svotu novca za "troškove" (bankarske provizije, dostave, izradbe vize za put u neku egzotičnu zemlju).

[8] Od engl. riječi *skim* što znači obrati mlijeko, a označuje pojavu kad se elektroničkom poštom lažno predstavljaju krivotvoritelji kartica i traže brojeve računa ili PIN-a. Često kreiraju i lažne mrežne stranice koje su vizualno gotovo identične pravim stranicama neke banke ili tvrtke koja izdaje kreditne kartice, a posjetitelja se umoljava da unese tražene podatke radi kontrole ili ispravka. Primjenom čip-tehnologije i zamjenom magnetnoga zapisa na karticama nastoji se onemogućiti izradba lažnih, ilegalnih kopija kartica.

Europska komisija načinila je u svibnju 2001. dokument pod nazivom Zaštita podataka u Europskoj Uniji. Vijeće Europe još je u siječnju 1981. godine donijelo Konvenciju o zaštiti pojedinaca u vezi s automatskom obradbom osobnih podataka, a u veljači 1999. godine Preporuku br. (99) 5 koja se odnosi na Internet, tj. korisnike i pružatelje usluga na mreži. U Direktivi Europskoga parlamenta pod oznakom 95/46/EC iz listopada 1995. napominje se da treba voditi računa o osnovnim pravima pojedinaca, bez obzira na to što je unutar Unije osigurano slobodno kretanje osoba, roba, usluga i kapitala. Direktiva 2002/58/EC iz lipnja 2002. odnosi se na obradbu osobnih podataka i zaštitu privatnosti u području elektroničke komunikacije. Organizacija za europsku suradnju i razvoj donijela je tijekom godina cijeli niz smjernica, primjerice:

- u rujnu 1980. godine Smjernice za zaštitu privatnosti i prekograničnoga "protoka", tj. prometa osobnih podataka;
- u veljači 1998. godine Smjernice koje se odnose na privatnost u elektroničkom okruženju: fokus na Internet;
- u prosincu 1999. godine Smjernice za zaštitu potrošača vezano uz trgovanje na mreži (elektronička trgovina);

FTC također donosi niz dokumenata, primjerice:

- u veljači 2000. godine – Pravila vezana uz zaštitu privatnosti djece na mreži;
- u lipnju 2001. godine – Zakon o tajnosti financijskih podataka potrošača tzv. Gramm-Leach-Blileyjev zakon (GLB *Act*), kao i dokument koji se odnosi na ograničenja vezana uz objavljivanje brojeva bankarskih računa;
- u rujnu 2001. – Dokument koji se odnosi na pohranjene podatke o brojevima pod kojima se vode krediti pojedinoga dužnika;
- prosinac 2001. godine – Korištenje izvještaja o potrošačima: Što trebaju znati posjednici?;
- travanj 2003. godine – Zakon o poštenim i preciznim (točnim) transakcijama.[9]

Iako je svrha brojnih zakona u različitim državama, kojima se propisuju načini postupanja s osobnim podatcima, zaštita slobode i prava pojedinca na privatnost (primjerice čl. 8 Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda) prevladava mišljenje da zakoni, ako su u nekim zemljama

[9] *Fair and Accurate Transaction Act* (FACTA) koji osim definiranja poštenog načina izvještavanja o kreditnim zaduženjima obrađuje i pojavu neautorizirane objave tuđih podataka od strane zaposlenika, te krađu identiteta.

uopće doneseni, nedovoljno štite pojedinca od gubitka ili neovlaštene promjene podataka, krađe identiteta (koja je sve učestalija, osobito u SAD-u), nadgledanja i praćenja.

Postoji niz preporuka koje su pojedine države objavile u obliku Kodeksa ponašanja, pa se tako Kodeks vezan u praksu poštenog informiranja[10] temelji na pet osnovnih načela:

- "ne smije postojati sustav unutar kojega su pohranjeni podatci, a da se ne zna za njegovo postojanje;
- pojedincu treba biti omogućen uvid u podatke koji su o njemu pohranjeni i poznat način na koji su prikupljeni;
- pojedinac mora imati mogućnost spriječiti korištenje podataka koji su prikupljeni s jednom namjenom, a namjerava ih se koristiti za drugu, a pritom se ne zatraži njegov pristanak;
- pojedincu treba biti omogućen ispravak pohranjenih podataka;
- agencije koje se bave kreiranjem, održavanjem ili diseminacijom osobnih podataka moraju voditi brigu o njihovoj pouzdanosti kao i mjerama predostrožnosti radi izbjegavanja zlouporaba".

Pojedina udruženja, kako u Europi, tako i u Americi, također su izradila kodekse ponašanja koji zapravo predstavljaju samoregulativu (engl. *self-regulation*).

Povjerenstvo za etičnu poslovnu praksu američkog Udruženja za izravni marketing (DMA) izdalo je niz dokumenata od kojih ćemo spomenuti:

- Smjernice vezane uz prikupljanje podataka koji se koriste u marketinške svrhe – one obvezuju kompanije da informiraju potrošače i korisnike o tome koje podatke prikupljaju, s kojom namjerom i ustupaju li ih drugim tvrtkama; obveza im je također dati jasne upute kako (poštom, telefonom, e-mailom, klikom miša na određenom mjestu na mrežnoj stranici) zainteresirani pojedinci mogu od kompanije zatražiti uvid u pohranjene podatke o njima, te zabraniti kompaniji njihovo korištenje ili ustupanje drugima;
- Vodič kroz odredbe zakona donesenoga 1998. godine kojim se željelo spriječiti primanje lažne i neželjene pošte (engl. *spam*);
- Smjernice koje se odnose na prikupljanje, korištenje i prijenos zdravstvenih podataka;

[10] Code of Fair Information Practice, http://aspe.hhs.gov./dataevid/1973privacy/summary.htm

- Smjernice u vezi s prijenosom, prodajom ili razmjenom popisa adresa (engl. *mailing list*) između vlasnika, sastavljača, posrednika, korisnika i agenata;
- Smjernice odobrene od Upravnog odbora u listopadu 2001. godine, kojima se posjetitelje mrežnih stranica upućuje na mogućnost izbora žele li ubuduće biti kontaktirani od kompanije čije su mrežne stranice posjetili.

Ljudi su osobito osjetljivi kad se evidentiraju njihovi intimni podatci (primjerice podatci o zdravlju i seksualnom životu, podatci vezani uz etničku ili vjersku pripadnost, socijalni status, informacije o broju socijalnog i zdravstvenog osiguranja, JMBG-u, broju bankovnoga računa, brojevima kreditnih kartica) stoga se nastoji zakonskim mjerama obvezati posjednike takvih podataka da ih zaštite i da se prema njima odnose s dužnom pozornošću prilikom obradbe, pohranjivanja ili ažuriranja. Brojni primjeri govore u prilog navedenom. U SAD-u je odjel HHS-a donio Standarde zaštite zdravstvenih podataka, a postoji i zakon iz 1996. godine koji se bavi razmjenom zdravstvenih informacija elektroničkim putem (HIPAA) uz amandmane iz 2003. godine u kojima se osobito naglašava pravo uvida bolesnika u vlastite podatke, uz mogućnost izmjene pogrešno unesenih podataka i postavljanje zahtjeva da se podatci javno ne objavljuju. Zbog razloga čuvanja privatnosti korisnika na mreži osnovan je 1997. godine TRUSTe[11] kao neprofitna i neovisna inicijativa posvećena izgradnji povjerenja korisnika Interneta. TRUSTe omogućuje pojedincima i organizacijama ostvarivanje međusobnog odnosa na temelju uzajamnog povjerenja glede poštovanja privatnosti i zaštite osobnih informacija. Kad se na bilo kojoj mrežnoj stranici nalazi njihov znak, posjetitelj može biti siguran da se njegovi osobni podatci neće zlouporabiti i da će mu privatnost biti zaštićena. TRUSTe provjerava tvrtke kojima su izdali certifikate i koje su dobile pravo korištenja njihova znaka. Svako toliko, tijekom određenoga razdoblja, posjećuju mrežne stranice spomenutih tvrtki i izvrše provjeru poštuju li se, prilikom dostavljanja nečijih osobnih podataka, pravila politike zaštite privatnosti. Razvili su i različite programe[12] kojima jamče zaštitu i sigurnost osobnih podataka i privatnosti.[13] U tu se skupinu ubrajaju poseban program zaštite privatnosti djece[14] (koji je u skladu sa Zakonom o zaštiti privatnosti djece prisutne na mreži)[15], program

[11] Rick Bruner u časopisu Advertising Age od 9.6.1997., str. 36 i http://www.truste.org

[12] Programi jamstava kojima se potvrđuje da je određena mrežna stranica u skladu s prihvaćenim standardima zaštite privatnosti – takve certifikate izdaju TRUSTe, BBBOnLine i CPA Web Trust.

[13] TRUSTe Privacy Seal Program.

[14] TRUSTe Childrens Privacy Seal Program.

[15] Children's Online Privacy Protection Act (COPPA).

zaštite zdravstvenih podataka[16], potom program koji vodi računa o pravilima europskog programa zaštite podataka[17] (tzv. EU *Safe Harbor Program*), a namijenjen je onim kompanijama koje posluju s europskim kompanijama kao i s fizičkim osobama izvan SAD-a. Program sadržava sedam načela:

"1. davanje obavijesti (*Notice*) – korisnici moraju znati za koju se namjenu prikupljaju podatci, kome su dostupni i kako korisnik može stupiti u kontakt s kompanijom ako želi ograničiti ili zabraniti korištenje pohranjenih podataka;

2. mogućnost izbora (*Choice*) – korisnik može zabraniti da se podatci (osobito oni intimni) dostavljaju trećim osobama;

3. daljnji prijenos (*Onward Transfer*) – ako treća strana koristi podatke, mora se obvezati da će poštovati navedena načela:

4. zaštita (*Security*) – podrazumijeva zaštitu prikupljenih podataka od gubitka, zlouporabe, neovlaštenog pristupa, objavljivanja, izmjene ili gubitka;

5. cjelovitost podataka (*Data Integrity*) – prikupljeni podatci trebaju biti korišteni samo za svrhu za koju su prikupljeni;

6. mogućnost pristupa (*Access*) – korisnicima je omogućen pristup prikupljenim podatcima o njima, ali tako da se ne naruši privatnost ostalih (pristup je omogućen samo vlastitim podatcima, dok uvid u tuđe podatke nije moguć):

7. provođenje (*Enforcement*) – osigurani su mehanizmi koji štite korisnike ako bi došlo do zlouporabe njihovih podataka".

Ovim smo kraćim pregledom nastojali prikazati napore koji se ulažu u stvaranje takvog okruženja u kojem se određenim zakonskim i regulacijskim okvirom pokušava olakšati i osigurati nesmetano poslovanje u novim uvjetima s obzirom na činjenicu neprestane promjene uvjetovane primjenom naprednih tehnologija u svim dijelovima društva.

Marketing, kao proces kontinuirane aktivnosti koja se stalno usklađuje s gospodarskim, društveno-ekonomskim, ekološkim, političkim i drugim kretanjima, u svojem razvoju poprima nove vidove, od kojih je jedan i izravni marketing koji je nastao kao rezultat novog pristupa tržišnom poslovanju usmjerenom na pojedinca koji želi da se poštuje njegova osobnost.

Zahvaljujući razvoju tehnike i tehnologije koja omogućuje stvaranje baza podataka o svakom pojedinom potrošaču (gdje se osim njegove adrese, brojeva telefona, podataka o posljednjoj kupovini, novčanom iznosu kupnje,

[16] TRUSTe E-Health Seal Program.

[17] Program osigurava usklađenost američkih propisa s pravilima EU-direktive koja se odnosi na zaštitu podataka. Program se primjenjuje od listopada 1998. godine (izvor: http://www.bbbonline.org/understandingprivacy/).

učestalosti kupnje, vrsti kupljenih proizvoda ili korištenih usluga, nalaze i informacije o njegovim stajalištima, posebnim željama, potrebama, hobijima i sklonostima), tvrtke su dobile mogućnost uspostavljanja dugoročnijeg i uspješnijeg odnosa sa svojim kupcima i prilagođivanje ponude svakom od njih. Bob Stone piše: "Neki kažu da je marketing baze podataka "tajno oružje" izravnog marketinga … Izravni marketeri znaju tko su im kupci, što kupuju, koliko često, kupuju li telefonski ili poštom, koliko potroše i kako plaćaju" (Stone, 1988.: 27).

Izravni (direktni) marketing definiramo kao specifičan marketinški sustav u kojem marketer na temelju baze (zbirke) podataka uspostavlja izravni odnos s poznatim pojedincima putem interaktivne komunikacije. Obilježavaju ga neposredan kontakt s krajnjim potrošačem (korisnikom), bez posrednika i mogućnost trenutačne reakcije potencijalnoga kupca ili interesenta (primjerice slanje upita ili narudžbe putem telefona, pošte, elektroničke pošte, mrežnih stranica, izravna prodaja putem televizije (aukcije, posebne emisije), elektronička trgovina).

Izravni marketeri sve više uz osnovne podatke (ime, prezime, brojevi telefona i mobitela) koriste demografska i psihografska obilježja kupaca i potrošača radi ciljanog plasmana svojih poruka izravno pojedincima određene ciljne skupine za koje pretpostavljaju da bi mogli postati kupcima njihovih proizvoda ili korisnicima njihovih usluga. Primjerice iz podatka o kućnoj adresi lako se može doći do zaključka glede imovinskog stanja i načina života dotične osobe; podatak o vrsti časopisa koji se naručuje upućuje na interese, slobodne aktivnosti, pa i stil života primatelja; temeljem informacije o dosadašnjim kupnjama moguće je predvidjeti koje će proizvode i usluge dotična osoba ubuduće naručivati.

S obzirom na činjenicu da velik broj tvrtki raspolaže različitim zbirkama podataka o korisnicima, potrošačima, interesentima, dobavljačima i partnerima, briga o sigurnosti tih podataka od zlouporabe i zaštita privatnosti postala je znatnim čimbenikom u poslovanju.

Uporaba Interneta još je više potaknula korisnike da se osiguraju od neodgovornoga korištenja njihovih osobnih podataka. Pojedinci često smatraju da su izgubili kontrolu ako se informacije i podatci o njima koriste i postavljaju sebi pitanje je li ugrožena njihova intima i njihov privatni život. L. Petrison, P. Wang i D. Messik (Reitman, 1995.: 47) smatraju da postoji najmanje pet razloga zašto bi potrošači mogli biti ogorčeni na izravne marketere:

- "strah od neodgovornoga korištenja podataka;
- strah od "velikog brata" – prema Orwelovu romanu *1984.*;
- smetanje i nedopuštene djelatnosti;

- zagađivanje okoliša i nepotrebno bacanje materijala;
- napastovanje."

Da su predviđanja navedenih autora bila točna, potvrđuju nam vijesti koje čujemo na radiju, gledamo na televiziji ili o kojima čitamo u dnevnom tisku ili se informiramo putem Interneta. Nedavni događaj[18] gubitka osobnih podataka 3,9 milijuna korisnika usluga *CitiFinancial Branch Network-a*, čiji su osobni podatci bili pohranjeni na kompjutorskim trakama, a izgubljeni su prilikom prenošenja u kreditni odjel od strane kurirske službe UPS-a, pokazuje da su mnogi ljudi opravdano zabrinuti glede pohranjenih podataka. Iako je korporacija, sukladno dobroj poslovnoj praksi, brzo reagirala slanjem pisama isprike korisnicima u kojima ih obavještava da se incident dogodio unatoč primjeni poboljšanih procedura zaštite, da je pokrenuta istraga, da su obaviještene nadležne institucije, te da je korisnicima osigurano besplatno nadgledanje računa unutar 90 dana radi prevencije moguće krađe identiteta, događaj izaziva opravdani strah. Svakako treba, u vezi s navedenim, spomenuti i probleme koje su imali izdavači kreditnih kartica s upadom *hackera* u njihove baze podataka, praksu ugradnje mikročipova u proizvode, odjeću ili ambalažu, pojavu mobitela s mogućnošću snimanja, napastovanje i nuđenje proizvoda i usluga telefonom u svako doba dana, pretrpavanje poštanskih sandučića netraženim promotivnim materijalima, slanje netraženih poruka (*spam*) putem elektroničke pošte ili slanje netraženih SMS ili MMS poruka putem mobitela.

Osnovno je u izravnom marketingu doznati što više podataka o potencijalnim i sadašnjim potrošačima i korisnicima usluga, te njihovim željama i sklonostima, kako radi potrebe sastavljanja kvalitetne baze podataka koja uključuje njihova imena, prezimena i adrese, tako i radi kreiranja uspješnih kampanja ciljanog marketinga (engl. *target marketing campaign*).

Bitno obilježje komunikacije je neposredno, individualno obraćanje odabranim pojedincima. Kad se odabere ciljna skupina kojoj se želi uputiti određena promocijska poruka, postavlja se pitanje raspolaže li se adresama pojedinaca koji pripadaju željenoj ciljnoj skupini.

Popise, liste adresa i zbirke podataka možemo podijeliti na: interne (unutarnje, vlastite) i eksterne (vanjske). Internu listu čini popis adresa koje su pohranjene u datotekama tvrtki, a sastoji se od adresa kupaca i potrošača dobivenih putem narudžbenica, kupona, upita, korespondencije, jamstava, sudjelovanjem u nagradnim igrama i slično. Vlastite adresne liste predstavljaju najbolji adresni materijal, jer su relativno dobro održavane, aktualizirane novim podatcima dobivenim izravnim kontaktiranjem pojedinaca s popisa.

[18] Najveća američka bankarska grupa Citigroup, priopćenje od 6. lipnja 2005., izvor: http://www.citigroup.com/citigroup/press/2005/050606a.htm

Eksterne liste sadržavaju adrese dobivene iz više izvora izvan poduzeća, a mogu biti posuđene ili kupljene od tzv. izdavača adresnih lista ili razmijenjene s drugim poduzećima koja nisu izravna konkurencija poduzeću koje je vlasnik liste.

Često poduzeća koja nisu konkurenti (primjerice izravni prodavači vina i izravni prodavači delikatesa; izravni prodavači knjiga i izravni prodavači proizvoda namijenjenih slobodnim aktivnostima, potom izdavači kreditnih kartica kao i ostala poduzeća koja posjeduju bilo kakve popise određene skupine ljudi) međusobno razmjenjuju popise adresa ili zbirke podataka. Razmjena je dopuštena samo ako se poštuju doneseni zakoni, smjernice ili, u najmanju ruku, pravila etičnog ponašanja, u zemljama gdje takvi zakoni ne postoje, a odnose se na potrebu dobivanja suglasnosti od osoba čijim se podatcima raspolaže.

Poduzeća koja prodaju ili posuđuju popise adresa moraju se zaštititi od onih koji na ilegalan način pokušavaju doći do adresa. To rješavaju tako da u svoju listu ubacuju kontrolnu adresu (Suppmayer/Gliss, 2002.: 26) na koju se uistinu može isporučiti pošiljka. Na toj adresi postoji fizička osoba koja je suglasna s time da se navedena adresa koristi samo u svrhu kontrole, a za svoje osobne potrebe koristi se drugom adresom.

Dillon daje nekoliko savjeta kako se lakše može otkriti neovlaštenog korisnika liste (Dillon, 1976.: 76):

- uključiti tajna imena suradnika;
- prigodom svakoga novog posuđivanja liste u listu uključiti i nekoliko novih imena koja nemaju izravne veze s ciljnom skupinom adresne liste (primjerice ime suradnice iz odjela unosa podataka);
- svaki puta neznatno promijeniti imena i označiti takvu promjenu prilikom davanja liste na korištenje novom korisniku;
- s obzirom na to da je opasno mijenjati ili pogrešno napisati adresu, najbolje je promijeniti samo inicijale ili ime korisnika ili dodati izmišljeni broj stana u uobičajenoj adresi;
- u svaki ugovor o posuđivanju liste adresa nužno je uključiti uvjet da posuditelj prihvaća sustav detekcije na temelju podmetnutih imena (engl. *dummy names*).

Podmetnuta imena unutar adresnih lista nazivaju se još i adrese spavači (engl. *sleepers*) ili adrese krtice (engl. *mole*).

Prilikom posuđivanja adresa uputno je poslovati s poznatim i poštovanja vrijednim poslovnim partnerima, a kvalitetnim ugovorima zaštititi se od neovlaštenog korištenja. Istraživanja (Suppmayer/Gliss, 2002.: 26) koje su

provele tvrtke Arthur Andersen i KPMG pokazala su da u tvrtkama postoji uvjerenje da se zlouporaba korištenja podataka događa drugima. Tvrtke stoga radije ulažu sredstva u oglašavanje nego u zaštitu sigurnosti podataka.

Studije su također pokazale da 45% kažnjivog rukovanja povjerljivim podatcima dolazi od zaposlenih u kompaniji, a samo manji broj od vanjskih suradnika. Osim adresnih lista otuđuju se i elektronički adresari s popisima adresa elektroničke pošte, te zbirke podataka o klijentima. Kako bi se kompanija zaštitila od neodgovornih zaposlenika, uputno je povjerljive liste skloniti na sigurno s naznakom da su unutar njih ubačeni podatci koji služe za provjeru jesu li liste bile korištene samo od ovlaštenih osoba i za unaprijed odobrene akcije. Ako su podatci pohranjeni u elektroničkom obliku, svakako ih treba zaštititi lozinkama. U tvrtkama, zbog navedenih razloga, sve više na značenju dobiva upravljanje digitalnim pravima (engl. *Digital Rights Management*), te propisivanje politike sigurnosti unutar koje se objavljuje koje korake tvrtka poduzima u vezi sa zaštitom privatnosti i sigurnošću podataka.

Dok nisu bili doneseni novi zakoni i postroženi postojeći, koji se odnose na zabranu korištenja nečijih podataka bez suglasnosti, postojale su tvrtke (sastavljači adresa – engl. *compilers*) koje su kreirale liste na temelju različitih javnih dokumenata (primjerice popisa vozačkih dozvola, popisa registriranih automobila, jamstava, novinskih oglasa i slično).

Tako sastavljene liste adresa prodavali su posrednicima ili izravno tvrtkama koja su takve adrese trebale. Primjerice u SAD-u je iz tog razloga donesen Zakon o zaštiti privatnosti vozača[19]. Tim se zakonom zabranjuje pristup podatcima vezanim uz dob i spol vlasnika automobila i vrsti automobila koji vozi, a zahtijeva se od vlasnika automobila da dade svoj pristanak ako je suglasan da njegovi osobni podatci postanu dostupni oglašivačima.

U većini slučajeva navedeni zakoni ograničavaju marketere koji analiziranjem različitih prikupljenih podataka mogu lakše razumjeti potrošače i predvidjeti njihove potrebe i kupovno ponašanje u budućnosti. Zbog nedostatnih informacija marketeri su prisiljeni obuhvatiti veće ciljne skupine potrošača promotivnim akcijama, što povećava njihove troškove od 3 do 11%. Ipak, bez obzira na tu činjenicu, takvi su zakoni nužnost jer svaki pojedinac treba imati mogućnost odabira i slobodno odlučiti kome će povjeriti svoje osobne podatke.

U nastavku teksta navest ćemo primjere nekoliko pisama čiji sadržaj kod primatelja izaziva, ako ne zabrinutost i ljutnju, onda najvjerojatnije čuđenje, nepovjerenje i loš dojam o tvrtkama koje su ih poslale:

[19] Drivers Privacy Protection Act (DPPA).

Primjer 1.

"Cijenjeni,

Predmet: ponuda za suradnju

Tvrtka ABC osnovana je … (slijede podatci o sjedištu tvrtke, adresa i telefonski brojevi).

Razvojna strategija naše tvrtke oslanja se na rad s građanima kao klijentima s očekivanjem da će razvijanjem odnosa sa širokom bazom klijenata ova strategija dugoročno predstavljati najstabilniji razvojni dio naše tvrtke.

U navedenom kontekstu, ovu ponudu treba razumjeti kao prijedlog početka međusobne, nadamo se, uspješne suradnje između Vas kao mogućeg klijenta i naše tvrtke.

Metodom "slučajnog uzorka" primijenjenoj na ukupnoj populaciji, identificirali smo Vas kao mogućeg dioničara neke od najznačajnijih tvrtki.

Slijedom navedenog ukoliko ste dioničar jedne od slijedećih tvrtki:

1. tvrtke D 2. tvrtke E 3. tvrtke F 4. tvrtke G

nudimo Vam slijedeću grupu usluga vezanih za vrijednosne papire u Vašem posjedu:

1…… 2…… 3…… (slijedi popis usluga koje nude)

Ukoliko ste zainteresirani za bilo koji od ponuđenih oblika suradnje molimo Vas da nam se obratite.

Uz Vaše razumijevanje, biti ćemo slobodni da Vas u vezi s ovom ponudom i telefonski kontaktiramo.

S osobitim poštovanjem, Tvrtka ABC" (Sudar-Kulčar, 2003.)

Ovo je pismo odaslano na ime i prezime primatelja koji uistinu posjeduje dionice jedne od navedenih tvrtki, te se stoga navođenje metode "slučajnog uzorka" u tekstu pisma teško može prihvatiti kao istinito. Čitajući pismo, postavlja se pitanje etičnoga poslovnog ponašanja pravne osobe koja je povjerljive podatke doznačila trećoj osobi, a da za takav postupak nije imala pristanak stranke čije podatke prosljeđuje. Odgovor je u činjenici da zakonska regulativa, koja u Hrvatskoj postoji tek kraće vrijeme, nije poznata tvrtkama koje šalju takva pisma ili svjesno krše propise oslanjajući se na mogućnost da takva praksa neće biti prepoznata i da još nisu dovoljno razvijeni mehanizmi kontrole i sankcioniranja prekršitelja novčanom, a u težem slučaju i zatvorskom kaznom. Iako je u navedenom pismu poštovano pravilo prema

kojem se tvrtka koja nudi proizvod ili uslugu treba predstaviti navodeći svoju adresu, brojeve telefona, kao i razraditi ponudu, te eventualno priložiti kuvertu koju ne treba frankirati (plaćeni odgovor) ako se potencijalni korisnik želi odazvati na ponudu, pismo može izazvati revolt primatelja, jer se tvrtka poslužila neistinitim podatkom glede načina na koji je došla do osobnih podataka primatelja (imena, adrese).

Primjer 2.

"Poštovani,

osobito nam je zadovoljstvo ponuditi Vam, kao članu udruge "321", našu kreditnu karticu (pismo je poslala kartičarska kuća) s kojom ostvarujete posebne pogodnosti:

- mjesečnu članarinu Udruge možete plaćati putem trajnog naloga;
- u službi Udruge možete plaćati dodatne usluge (a… b… c… – slijedi popis usluga) na tri, šest ili osam mjesečnih rata;
- u službi Udruge možete plaćati troškove usluga i za osobe koje nisu članovi Udruge na tri, šest ili osam mjesečnih rata; ……..…… (ostale pogodnosti)

Uz navedeno, korištenje naše kartice donosi čitav niz prednosti (i…. ii…. iii…. – u nastavku slijedi njihov opis).

Zatražite našu karticu i pritom iskoristite poseban popust:

ovom prigodom štedite iznos upisnine od xxx kn i iznos članarine od yyy kn za prvu godinu članstva!

Srdačan pozdrav
ime tvrtke (izdavača kreditne kartice)

Dovoljno je da popunite pristupnicu s poleđine i potrebnu dokumentaciju dostavite na (adresa kartičarske kuće)

Zaštitni znak	**Zaštitni znak**
kartičarske kuće	Udruge "321"
(adresa, telefonski broj, web adresa)	(adresa, telefonski broj)"

Citirano pismo odaslano je na ime i prezime osobe, člana Udruge, koja je bila neugodno iznenađena činjenicom što je kartičarska kuća došla u posjed povjerljivih podataka (činjenice da je član dotične Udruge) i osobnih podataka (imena, prezimena, adrese) s obzirom na to da Udruga nije kontaktirala svog člana i dobila suglasnost za daljnje prosljeđivanje informacija.

U poslovnom svijetu uobičajena je takozvana kooperativna (zajednička) promocija tvrtki čiji se proizvodi/usluge nadopunjavaju, pa tvrtke zajedničkim akcijama (u ovom slučaju putem izravne pošte) nastoje pridobiti nove potrošače ili korisnike. Međutim, način na koji su u ovom slučaju prikupljeni (dobiveni) podatci za kreiranje baze podataka ciljne skupine potencijalnih korisnika, tj. primatelja pisama, nije uobičajen u razvijenim zemljama u kojima se ponajprije poštuje integritet, dostojanstvo i pravo na privatnost svakog pojedinca.

Primjer 3.

"Poštovana gospodo (gospodine) X,

S obzirom na to da vi sada imate 55 godina, pretpostavka je da ćete u budućnosti trebati dodatnu zdravstvenu ili drugu skrb koja nije jeftina. S vaših 30.000,00 kuna na bankovnom računu i sadašnjom zaradom od 5.000,00 kuna mjesečno, uplatom u mirovinsko osiguranje od 1.600,00 kuna zapitate li se hoćete li ćete u budućnosti biti u mogućnosti (s obzirom na visinu buduće mirovine) plaćati dodatne troškove?

Naše poduzeće XYZ ima rješenje za Vas ..... (slijede prijedlozi poslovne suradnje)

S poštovanjem direktor IQ 70"

Primitak navedenog pisma ili elektroničke pošte sličnog sadržaja ni u kom slučaju neće kod primatelja izazvati oduševljenje, prije će reakcija biti ogorčenost i ljutnja, te pitanje kako je i od koga tvrtka XYZ došla do osobnih podataka.

Navedeni nas primjeri navode da se zamislimo. Trebali bismo početi pridavati više pozornosti kome, kada i zbog kojeg razloga dajemo svoje podatke. Informiranje o pouzdanosti onoga tko prikuplja podatke treba postati *condicio sine qua non* donošenja odluke pojedinca o tome hoće li i u kolikoj će mjeri nekome povjeriti svoje podatke.

Svaka bi ozbiljna tvrtka prisutna na tržištu (osobito ako komunicira i posluje putem Interneta) veliku pozornost trebala posvetiti kreiranju politike zaštite privatnosti. S tom politikom treba upoznati svoje kupce, dobavljače i ostale poslovne partnere. Prigodom kreiranja politike zaštite privatnosti tvrtka treba imati na umu koja joj je vrsta osobnih podataka potrebna za normalno obavljanje posla, kako ih planira prikupljati i koristiti, kako pohranjene podatke namjerava osigurati od neovlaštenog korištenja, koje zakone i pravila ponašanja mora poštovati, te na koji način planira o tome informirati svoje potrošače.

Udruženje za izravni marketing u SAD-u predložilo je listu pitanja (*check list*) na koja trebaju odgovoriti rukovoditelji u tvrtki zaduženi za zaštitu podataka i privatnosti:

1. Postoji li u tvrtki politika zaštite podataka unutar informacijskog sustava (u to se, između ostalog, ubraja izradba pisanog plana zaštite, potpisane ugovore sa zaposlenicima o čuvanju poslovne tajne (podataka), investiranje u programe i ostale "alate" nužne za zaštitu podataka, suradnju sa stručnjacima izvan tvrtke koji nadgledaju sigurnosni sustav)?
2. Ima li tvrtka osiguranu edukaciju i način kontrole osoblja koje rukuje osobnim podatcima?
3. Koristi li se tvrtka adekvatnim tehnologijama koje omogućuju zaštitu osobnih podataka (primjerice, antivirusne programe, sustav autorizacije prije pristupa podatcima, lozinke)?
4. Jesu li dobavljači i poslovni partneri informirani o politici tvrtke i zahtijeva li se od njih jamstvo i odgovorno ponašanje glede poštovanja postavljenih standarda zaštite podataka?

Kako bi tvrtkama približili i olakšali kreiranje vlastite politike zaštite privatnosti, Udruženje za izravni marketing na svojim je mrežnim stranicama dalo predložak[20] koje informacije treba sadržavati obavijest potrošačima koja se odnosi na politiku tvrtke vezanu uz zaštitu privatnosti i pohranjenih podataka (primjerice informacija o tome koje podatke server poduzeća automatski registrira kad posjetitelj dođe na njihovu mrežnu stranicu, koju vrstu podataka prikupljaju i zašto ih koriste, ustupaju li ih, kao i njihovu adresu elektroničke pošte ili telefonski broj, drugim poduzećima koja nude proizvode za koje smatraju da bi bili zanimljivi posjetitelju njihove stranice, koriste li tzv. "kolačiće"[21] i zašto, koriste li standardne tehnologije kriptozaštite, omogućuju li posjetiteljima izbor žele li da se njihovi podatci ustupaju drugima i dopuštaju li im pristup njihovim podatcima, jesu li posjetiteljima na mrežnoj stranici dostupne adrese za kontakt i telefonski brojevi organizacija kojima se mogu požaliti ako smatraju da tvrtka ne djeluje u skladu s navedenom politikom).

Ako se na kraju osvrnemo na stanje u našoj zemlji, možemo ustvrditi da brojne institucije i ostali poslovni subjekti prikupljaju različite podatke o pojedincima i pohranjuju ih u različitim zbirkama podataka, kako radi vođe-

[20] Direct Marketing Association (http://www.the-dma.org) – Create Your Privacy Policy Now (Kreirajte odmah svoju politiku zaštite privatnosti).

[21] *Cookie* – mala tekstualna datoteka koja se instalira na tvrdi disk posjetitelja mrežne stranice. Ta datoteka registrira podatke vezane uz to koje je stranice posjetitelj vidio i koje je priloge na stranici pregledao. Da bi se spriječilo instaliranje kolačića od vlasnika mrežne stranice ili oglašivača, osmišljen je softverski program tzv. *cookie buster*.

nja određenih evidencija, izradbe statističkih izvješća, tako i radi profitabilnijeg poslovanja. Brojne su tvrtke prihvatile praksu izravnog marketinga i nastoje uspostaviti izravni kontakt s dosadašnjim, ali i potencijalnim potrošačima poštujući etičke norme i pravila dobre poslovne prakse. Međutim, pojedine tvrtke su, zbog neznanja ili radi probitka, iskoristile nepostojanje odgovarajućih zakona i propisa i nisu se s dužnim oprezom odnosile prema osobnim podatcima i željama pojedinaca. Zakoni koji se odnose na zaštitu privatnosti, sigurnost podataka, zaštitu potrošača, pravo na pristup informacijama, elektroničke medije, elektroničku trgovinu, kao i uredbe o načinu pohranjivanja prikupljenih osobnih podataka i evidentiranje zbirki osobnih podataka doneseni su nedavno.[22]

Pregledavanjem velikog broja hrvatskih mrežnih stranica (javnih institucija, ministarstava, ureda državne uprave, gospodarskih subjekata koji nude različite proizvode i usluge) može se uočiti da samo manji broj njih (veće hrvatske kompanije, neke banke i javna glasila) na naslovnoj stranici (engl. *home page*) daju informaciju o uvjetima i pravnim učincima korištenja mrežnih stranica. Stanje na naslovnicama većine europskih i američkih tvrtki i organizacija potpuno je drukčije. Na naslovnici je odmah uočljiva obavijest vezana uz zaštitu privatnosti (engl. *Privacy Notice*) koja uključuje sve informacije koje bi mogle zanimati posjetitelja stranice ili demanti (engl. *Disclaimer*) u kojima se vlasnici mrežne stranice jasno i nedvosmisleno određuju vezano uz nedopuštenu ili nemoralnu praksu, i tako šalju poruku da su njihove stranice sigurne, da se bez straha može pregledavati ili preuzimati njihov sadržaj i uspostaviti sigurna interaktivna komunikacija.

Kako bi zadobile povjerenje potrošača, brojne kompanije osiguravaju potrošačima uvid u njihove podatke uz mogućnost zabrane ustupanja tih podataka drugim kompanijama. Osim toga, sve se više prihvaća praksa dopuštenoga marketinga (engl. *permission marketing*) čija je osnovna pretpostavka dobivanje suglasnosti od pojedinaca čije podatke kompanija posjeduje žele li da im se poštom dostavljaju promocijske poruke ili materijali ili da ih se kontaktira telefonom, elektroničkom poštom ili SMS-om. Prednost takve prakse vezana je uz smanjenje nezadovoljstva onih koji ne žele da ih se uznemirava.

Pretpostavka dugoročnoga, uspješnog poslovanja jest kontinuirano usvajanje novih znanja i praksi, poštovanje zakona, etično ponašanje u odnosu

[22] Zakon o zaštiti osobnih podataka (NN 103/03), Zakon o privatnoj zaštiti (NN 68/03), Zakon o zaštiti potrošača (NN 96/03), Zakon o elektroničkim medijima (NN 122/03), Zakon o elektroničkoj trgovini (NN 173/03), Zakon o pravu na pristup informacijama (NN 172/03), zakon o prikupljanju informacija po osiguranicima o doprinosima za obvezna mirovinska osiguranja (NN 177/04), Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN 139/04), Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (NN 105/04).

prema korisnicima, potrošačima, kupcima i interesentima, poštovanje njihovih želja i zadovoljavanje njihovih potreba, kao i uspostavljanje odgovornoga, partnerskog, prijateljskog i na povjerenju utemeljenog odnosa. Alternative nema.

Literatura

Dillon, John, 1976.: *Handbook of International Direct Marketing*, Mc Graw Hill, UK,1976

Reitman, J.I., 1995.: *Beyond 2000 – The Future of Direct Marketing*, NTC, Business Books, Lincolnwood

Stone, Bob, 1988.: *Successful Direct Marketing Methods*, IV, NTC Business Books, Lincolnwood, Illinois

Sudar-Kulčar, Mirna, 2003.: *Pravni aspekt primjene izravnog marketinga*, Informator, instruktivno-informativni list za ekonomska i pravna pitanja, 9/2003, Zagreb

Suppmayer, Dieter/Gliss, Hans, 2002.: *Kontrolladressen: Sicherung gegen Datenmissbrauch* (*Kontrolne adrese: Sigurnost podataka nasuprot zlouporabi*), Direkt Marketing, 9/2002; IM Marketing – Forum Gmbh, Ettlingen

Mirna Sudar-Kulčar

PRIVACY PROTECTION AND DATA SECURITY REFERING TO DIRECT MARKETING

Summary

Privacy protection and data security become important part of business practice. In the same time customers are concernd about personal data missusage. Regarding this, in the world, and finally in Croatia, new laws and codes have been created to regulate and recommend how to communicate with customers and for those who do not respect decency, discretion and safety to set penalties. In direct marketing straight communication with prospective buyers and customers is essential. Target marketing campaigns are based on data base (which f.e. include consumer name, address, information about purchase behaviour etc.). Mailing lists are important for direct marketers because they send advertising materials to the potential buyers. Sometimes consumers are not satisfied with marketing activities because they are frightened of inappropriate data usage, privacy disturbance and bothering.

Key words: privacy protection, data security, privacy protection and data security laws, new aspects of marketing, direct marketing, privacy policy

Mailing address: Hrvatski studiji, Ulica grada Vukovara 68, HR 10 000 Zagreb. *E-mail:* mirna.sudar-kulcar@zg.t-com.hr