

**Poslovna Informatika**



**Seminarska naloga**

**SPAM, VPLIV NA POSLOVANJE  
PODJETIJ IN SLOVENSKA  
ZAKONODAJA**

## **KAZALO**

1. UVOD.....	3
2. SPLOŠNO O SPAMU.....	4
Zgodovina.....	4
Komu in zakaj se spamanje izplača?.....	5
Kako spamerji dobijo naše elektronske naslove?.....	6
Zakaj spam ni zaželen?.....	6
3. SPLETNO OGLAŠEVANJE, VPLIV NEZAŽELJENEGA OGLAŠEVANJA (SPAM) TER BORBA PROTI NJEMU.....	7
Netvertising – spletno oglaševanje.....	7
Trženje z dovoljenjem (permission marketing) .....	7
Primer neustreznega oglaševanja po internetu iz tujine.....	8
Stroški spama v podjetjih in doma.....	8
Preventiva, kurativa, pritožbe.....	9
4. SPAM IN SLOVENSKA ZAKONODAJA.....	10
Primerjava Slovenije z ostalimi državami.....	10
Zakon o varstvu potrošnikov.....	10
Zakon o elektronskih komunikacijah.....	12
5. SKLEP.....	13
6. LITERATURA IN VIRI.....	14
Slika 1: Mesni narezek Spam, po katerem je nezaželjena pošta dobila svoje ime.....	5
Tabela 1: Anketa o pogostosti prejemanja nezaželenih sporočil.....	8

## **1. UVOD**

Oglaševanje raznovrstnih izdelkov nas spremlja že dolgo časa. Reklame na televiziji ter radiu, gigantski posterji ob cestah, deljenje reklamnih letakov in njihovo zatikanje v poštne nabiralnike so le najbolj tipični predstavniki oglaševanja, ki smo se ga morali hočeš-nočeš navaditi. Dokler ne preseže meja dobrega okusa, seveda.

Razmah interneta je oglaševalcem odprl nove poti. Poglavitna prednost internetnega oglaševanja je namreč cenovna ugodnost, saj od oglaševalcev zahteva zgolj razvoj propagandnega gradiva in plačilo spletnim stranem za njegovo prikazovanje, odpade pa potreba po tiskanju in distribuciji materiala. Podobno kot pri televizijskih reklamah, le da je zakup oglasnega prostora na internetu mnogo cenejši.

Poleg prikazovanja oglasov na spletnih straneh pa je na internetu mogoče oglaševati tudi preko elektronske pošte. Pri oglaševanju preko elektronske pošte so stroški oglaševanja še nižji, zato je tako oglaševanje za oglaševalce zelo mamljivo. Če potegnemo analogijo s klasičnim deljenjem letakov v poštni nabiralnik - tam mora podjetje oblikovati prospekte, jih natisniti in poskrbeti za distribucijo, pri oglaševanju preko elektronske pošte pa stroški tiska odpadejo, stroški distribucije pa so zmanjšani na minimum.

Po zgornjem opisu sodeč lahko sklepamo, da je dandanašnji za podjetja in samostojne podjetnike pravi raj na področju oglaševanja. Vprašamo pa se lahko kaj vse to pomeni za večino uporabnikov osebnih računalnikov, za prejemnike vsega tega reklamnega materiala?

To, kar je za ustvarjalce reklamnih oglasov raj, je za prejemnike teh istih oglasov pekel. V letu 2004 je po podatkih raziskave podjetja Ferris Research približno 30 odstotkov vse pošte, ki je prišla na zasebne elektronske naslove, zasedla nenaročena oglasna pošta. Pri poslovnih elektronskih naslovih je bila ta številka nekoliko manjša, saj je nezaželjena pošta predstavljala nekje med 15 in 20 odstotki celotne prispelne pošte. Tovrstni nezaželeni oz. nenaročeni pošti pravimo spam (v slovenščini nismo našli domačega izraza, ki bi zaobjel celotno področje, ki ga razumemo z izrazom spam, zato smo le-tega prevzeli tudi v domačo rabo). Spam je dokaj moderen »izum«, saj se je tovrstno početje - nenadzorovano in nenaročeno pošiljanje reklamnih oglasov začelo bohotiti šele v zadnjem desetletju prejšnjega stoletja.

V zadnjih desetletjih letih poteka ogorčen boj in uporaba vseh sredstev za boj proti nezaželeni pošti. Svoje, poleg vseh tehnoloških sredstev, v večini držav doda tudi zakonodaja, saj se dandanes vse bolj uveljavljajo moderne oblike poslovanj ter beleženj in spremljanj podatkov tudi na področju javne uprave. V zakonskih rešitvah tega področja sta se uveljavili predvsem dve rešitvi: opt-in ter opt-out.

V sloveniji tako to področje urejata *Zakon o varstvu potrošnikov* ter *Zakon o elektronskih komunikacijah*. Naša država sodi v skupino skrbnejših držav, saj se je pri nas v zakonu uveljavilo načelo opt-in. Kljub temu, pa nas to ne more rešiti pred spamom iz tujine- problem spama je namreč globalen problem, zato bi morali celoten problem spama tudi reševati na globalni ravni. Lokalno delovanje resda pripomore k zmanjšanju spama, a srž problema tako ostaja nedotaknjena.

## **2. SPLOŠNO O SPAMU**

*V splošnem lahko za spam sporočilo smatramo vsako sporočilo, ki je poslano večjemu številu naslovnikov, z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Ponavadi se s spam pošto oglašujejo izdelki ali storitve dvomljive kvalitete, velikokrat pa gre za goljufije (tipičen primer je *nigerijska prevara*, ki prevarantom včasih uspe tudi pri nas).*

Univerzalna in za vse veljavna definicija spama žal ne obstaja. Nekateri trdijo, da so spam vsa sporočila, ki so množična in nenaročena, pri čemer kot mejo za množičnost postavljajo npr. 20 različnih naslovnikov. Strogo upoštevanje take definicije bi lahko pomenilo, da je spam tudi vabilo na zabavo, ki ga je nekdo poslal svojim 21 prijateljem brez predhodnega dogovora. Po drugi definiciji naj bi bil spam vsako nenaročeno reklamno sporočilo (oziroma celo vsako nenaročeno sporočilo nasploh), vendar je tu pomembno tudi kdo sporočilo pošlje. Če dobi uporabnik od svojega ISP-ja nenaročeno sporočilo, da je za svoje uporabnike uvedel nekatere nove storitve, to še ni spam.

Treba je poudariti, da je oglaševanje preko elektronskih sporočil lahko povsem koristno in nemoteče. Seveda pa mora pošiljatelj spoštovati vsaj dve osnovni pravili:

- *Vsebina reklamnih sporočil naj ne bi bila nelegalna in goljufiva*, saj je ta že po zakonu prepovedana. V večini držav je zakonsko regulirano oglaševanje in distribucija pornografije, v nekaterih državah (npr. Sloveniji) pa je prepovedano tudi oglaševanje in prodaja zdravil preko interneta. Po ocenah podjetja Brightmail je največ spama, ki oglašuje izdelke, vsebuje finančne ponudbe ter pornografijo (*The Deadly Duo: Spam and Viruses, June 2003*).
- *Prejemnik naj bi imel možnost odločitve, da elektronskih sporočil ne želi več sprejemati*. Dlje časa že poteka spor okrog dveh konceptov. Prvi je tako imenovani opt-in, torej zahteva, da se uporabnik sam prijavi na tovrstno storitev, druga pa je opt-out, ki zahteva, da mora imeti prejemnik možnost, da se od storitve odjavi. Minimum, ki ga mora spoštovati pošiljatelj, je torej vsaj opt-out, torej možnost odjave. Vendar nekateri pošiljatelji možnost odjave ponujajo samo navidezno in z zlimi nameni.

### **Zgodovina**

Izvor izraza spam je zelo zanimiv. Prvič so ga uporabili pri podjetju Hormel Foodsa, ki je prodajalo konzervirano šunko pod tem imenom. Krivec, da se je izraz uveljavil kot sinonim za nezaželeno elektronsko pošto, je Monty Python's Flying Circus s svojim skečem. V njem neka restavracija streže raznovrstno hrano, ki je vsa polna šunke, tako da natarica mnogokrat ponovi besedo spam, ko opisuje, iz česa je posamezen obrok. Skeč se konča, ko skupina Vikings v ozadju začne peti Spam, spam, spam ... tako da preglasijo vse ostale in se sliši samo še spam.



Izraz spam se je uveljavil aprila 1994, ko sta dva odvetnika iz Phoenixa najela programerja, ki je napisal preprosto skripto, s pomočjo katere sta nato odvetnika poslala sporočilo, ali bolje rečeno, reklamo o svojih uslugah na vse USENET konference. Ljudje so takrat pričeli uporabljati izraz spam in ta se je, kot vidite, prijel. Omeniti velja, da je to resda prvi "napad", pri katerem je bil uporabljen termin spam, zagotovo pa to ni bil začetek le-tega.

**Slika 1:** Mesni narezek Spam, po katerem je nezaželjena pošta dobila svoje ime

Letos praznujemo praznujemo 28. obletnico prvega e-poštnega spama, ki se je bil pojavil 1978 v ameriškem vojaškem predhodniku interneta, ARPANETu. DEC, ki je sedaj v Compaqovi lasti, je takrat objavil reklamo za nov računalnik DEC-20 in jo poslal na vse naslove na ameriški zahodni obali. Takrat je bil DEC kaznovan zaradi kršitve pravil uporabe ARPANETA, ostali pa so bili opozorjeni, naj tega nihče več ne počenja. Očitno ni zaleglo.

Naslednji pomemben korak so bila sporočila *MAKE MONEY FAST*, standardna verižna pisma, ki so krožila po USENETu v osemdesetih in devetdesetih letih. Ker je bil USENET tako ranljiv za spam (ki se takrat sicer še ni imenoval tako), je Richard Depew leta 1993 objavil kontroverzna idejo o uvedbi t.i. moderiranih USENET konferenc, kjer bi moderatorji vsako sporočilo pred objavo prebrali in tista, ki kršijo pravila (spam), izločili. Ideja je dobro uspevala, pojavile so se moderirane konference, ki so bile dokaj "čiste". Kasneje so ljudi resnično razburili dogodki 31. marca 1993, ko se je Depew igral s svojim orodjem za moderiranje, imenovanim ARMM. Pokazalo se je, da ima hrošča, ki je ob zagonu poslal dvesto sporočil v konferenco news.admin.policy. Depew se je za nezgodo opravičil, a spam je bil rojen.

Naslednji gigantski in tedaj daleč največji spam se je januarja 1994 prav tako zgodil na USENET omrežju, ko je vsaka konferenca prejela sporočilo Global Alert for All: Jesus is Coming Soon, ki ga je poslal administrator na Andrews University. Naslednji masivni spam pa je bil delo poprej omenjenih odvetnikov iz Phoenixa aprila 1994.

Od tistih časov se kaj bistvenega ni spremenilo, saj spam še vedno ostaja, oziroma se celo krepi. Morda glavna razlika je, da je postal bolj oseben, saj so se spamerji preusmerili s pošiljanja sporočil v USENET konference na pošiljanje na elektronske naslove. Razlog za to je gotovo zamiranje USENETa, saj ga v zadnjem času vedno bolj nadomeščajo internetni forumi, ki so skrbno moderirani, tako da spamerjem večinoma preostaja le elektronska pošta.

## **Komu in zakaj se spamanje izplača?**

Definitivno se spamanje splača tistim, ki tovrstna sporočila pošiljajo. Stroške imajo minimalne, prepričani pa ste lahko, da svojim naročnikom razložijo, da je to zanje (za spammerje, ne naročnike) tvegan posel in jim to tveganje tudi mastno zaračunajo. Kaj pa naročniki? Čeprav večina ljudi na goljufive in sumljive ponudbe verjetno ne reagira, pa se

vedno najde nekaj naivnežev, ki takšne izdelke ali storitve dejansko kupujejo. Ker so reklamna sporočila poslana v milijonskih izvodih, pošiljanje pa je za pošiljatelja poceni, bo nekdo zagotovo imel lep dobiček. Se splača? Spamerjem zagotovo.

## **Kako spamerji dobijo naše elektronske naslove?**

Ena bistvenih nalog vsakega spamerja je iskanje oziroma pridobitev e-naslovov. Kaj jim bodo vse priprave in orodja, če spama nimajo kam pošiljati? V lovu za veljavnimi in po možnosti še najpomembnejšimi e-poštnimi naslovi uporabljajo vse, od najbolj nedolžnih zvijač do res umazanih trikov in goljufij. Najpogostejši načini za pridobivanje e-naslovov so: *skeniranje internetnih strani* (s pomočjo programa spamerji preskenirajo celotne strani z vsemi pripadajočimi podstranmi in poskušajo v izvorni kodi izbrane strani najti koščke besedila, ki bi lahko predstavljali elektronski naslov), *izkoriščanje naivnosti uporabnikov* (vnašanje e-naslovov, verižna pisma, unsubscribe povezave), *spyware in virusi* (elektronski naslov vam lahko izmakne tudi kakšen vohunski program ali virus, pravzaprav vam lahko izmakne kar cel vaš adresar), *vdiranje na strežnike* (z malo hekerskega znanja ali več crackerske sreče lahko spamerji vdrejo na strežnike velikih podjetij, ki seveda hranijo vse podatke svojih uporabnikov), *ugibanje s pomočjo prijaznih poštnih strežnikov* (zelo prikladna metoda za ugibanje so e-mail naslovi v obliki ime.priimek@ponudnikinterneta.domena; spamer najprej dobi bazo imen in priimekov, nato pa jih iz njih ustvarja kombinacije elektronskih naslovov in na prav vse pošlje testno sporočilo ali pa kar pravi spam; dosti takšnih naslovov ne deluje in strežnik pošiljatelju vrne že omenjeno sporočilo o napaki, za tiste naslove, na katere je pošiljanje potekalo brez napak, pa lahko spamer sklepa, da so v uporabi in jih tako veselo uvrsti v svoj seznam) ter *nakup naslovov* (bogatejšim spamerjem seveda ni treba iskati elektronskih naslovov, temveč jih enostavno kupijo od podjetij ali pa od ostalih spamerjev).

## **Zakaj spam ni zaželen?**

Zakaj se pravzaprav tako upiramo spamu, ko pa vsakodnevno prejemamo papirnate oglase po navadni pošti in stalno gledamo oglase na televizijskih kanalih? V literaturi se pojavlja pet glavnih razlogov: *večino stroškov spama nosijo prejemniki, pri spamu gre za krajo resursov, spam ponavadi ni vreden počenega groša, pošiljatelj spama večinoma želi zavesti ali ogoljufati, spam sili uporabnike interneta v skrivanje svojega pravega e-poštnega naslova, s tem se okrne komunikacija v javno dostopnih debatnih skupinah in konferencah.*

Nemalokrat se pošiljatelj oglasa zagovarja, da so naslovi bili nabrani na javno dostopnih spletnih straneh. Tak argument sicer legalistično morda celo drži, vendar pa ne reši *izvornega problema spam pošte*. Ta problem je, *da poplava neželenih sporočil omejuje uporabnikovo komuniciranje na omrežju*. Obrnemo se lahko k analogiji: tudi telefonske številke je možno nabrati iz javnih virov. Vendar legalnost zbiranja številčk na tak način ne pomeni, da neprestano zvonjenje domačega telefona zaradi različnih "anket" in snubljenj k "predstavitvi na domu" za konkretnega naročnika ni moteče.

### **3. SPLETNO OGLAŠEVANJE, VPLIV NEZAŽELJENEGA OGLAŠEVANJA (SPAM) TER BORBA PROTI NJEMU**

#### **Netvertising – spletno oglaševanje**

Oglaševanje spletnih strani je nenadoma postalo množični posel, vreden milijarde ameriških dolarjev. Za podjetja, ki nimajo svojih strani na internetu, ni prihodnosti.

Internet pomeni na področju trženja nov tip interaktivnega oglaševanja, ki poleg samega oglaševanja omogoča še dvostransko komunikacijo. Ker je po svojih lastnostih in zmožnostih bistveno drugačen od ostalih medijev, morajo podjetja oglaševalsko strategijo zasnovati drugače kot pri ostalih medijih.

Prvotni cilj oglaševalcev je večja prepoznavnost podjetja. Namen oglaševanja je tudi v tem, da oglaševalec pritegne čim več potencialnih strank na svojo spletno stran, kjer jim lahko ponudi še več informacij o določenem izdelku ali storitvi, ter ga tako vzpodbudi k nakupu. Prednosti oglaševanja na internetu so v tem, da je komuniciranje interaktivno, dopolnjuje blagovno znamko, uveljavlja podjetje (branding) in poenostavlja prodajne poti. Oglaševalci lahko na internetu ugotovijo koliko uporabnikov si je ogledalo stran z njihovim oglasom, in kar je še pomembnejše, koliko ljudi je s klikom na oglas prišlo do njihove spletne strani.

#### **Trženje z dovoljenjem (permission marketing)**

Podjetje lahko oglašuje tudi brez spama in ima še vedno na voljo naslednje možnosti:

- oglaševanje na spletu in vpis v iskalnike,
- oglaševanje po elektronski pošti, vendar samo na naslove, katerih uporabniki so se predhodno strinjali, da želijo biti obveščeni o dejavnosti podjetja oz. produktov in storitev.

**1.korak:** Spletno trženje je spletna storitev. Hladnokrvno obstreljevanje kupcev (bela pika) z izdelki (črna pika) lahko pripelje do odkritega negodovanja kupcev. Model imenujemo B2C - mi do strank. Uspešnejši model je B+C. S plusom je poudarjen pomen enakopravnega sodelovanja nas in strank. V modelu je stranka še vedno bela pika in izdelek črna pika. Nova je siva pika, ki predstavlja spletno storitev, ki spoji stranko in izdelek v zadovoljnega kupca. Trženje tako postane miroljubno spajanje stranke z izdelkom.

**2. korak:** Spletno trženje je proces preoblikovanja obiskovalcev v zadovoljne kupce, ki zahteva uporabo različnih orodij. Poudarek je na besedi proces. Procesni vidik spletnega trženja lahko predstavimo z modelom lijaka. V njem se gnetejo obiskovalci, izdelki in prodajne storitve. Do večje prodaje vodi več obiskovalcev, več izdelkov in boljše prodajne storitve (bolj lepljive storitve). Pomembna je privlačnost izložbe, način in obseg predstavitve

ponudbe, enostaven nakupni proces in hitra oskrba naročila.

Najprej so samo obiskovalci. Ko jih spoznamo (nam zaupajo svoj e-poštni naslov) jih lahko uvrstimo v skupino registriranih uporabnikov. Brez obiskovalcev in uporabnikov ni kupcev (tako v fizični kot v spletni prodaji).

## Primer neustreznega oglaševanja po internetu iz tujine

Nissan je v ZDA pred slabim letom poslal 24.000 kupcem sporočilo o svojem novem modelu avtomobila. Namesto, da bi uporabili kakšen dober program za pošiljanje takšne količine sporočil, ali pa da bi najeli profesionalce za to, so se akcije lotili kar sami. Vse naslove prejemnikov so postavili v polje "To:" namesto v polje "Bcc:". Rezultat: vsak prejemnik, je v glavi 300 KB dolgega sporočila prejel 24.000 naslovov prejemnikov sporočila. Če torej podjetje ni strokovno podkvano, potem naj raje najame profesionalce, ki bodo oglaševanje po internetu pravilno izvedli.

## Stroški spama v podjetjih in doma

Stroškovni vidik spama ne prihaja v ospredje zgolj v poslovnem svetu, temveč tudi pri zasebni uporabi. Veliko ljudi namreč še vedno plačuje impulze in naročnino, ki se zaradi tega

### Koliko neželenih sporočil dnevno prejmete v svoj elektronski poštni nabiralnik?

Nobenega	19,63 %	189
1-5	33,54 %	323
6-10	16,72 %	161
11-20	12,05 %	116
21-50	10,49 %	101
51-100	3,95 %	38
več kot 100	3,63 %	35

Skupaj odgovorov: 963

(Začetek ankete:

7. 7. 2003, 03:45)

Vir:SiOL

povečuje. V letu 2004 je po podatkih raziskave podjetja Ferris Research približno 30 odstotkov vse pošte, ki je prišla na zasebne elektronske naslove, zasedla nenaročena oglasna pošta. Pri poslovnih elektronskih naslovih je bila ta številka nekoliko manjša, saj je spam predstavljal nekje med 15 in 20 odstotki celotne prispele pošte. Podatki sami sicer ne delujejo alarmantno, vendar pa naj bi to pomenilo izgubo desetih dolarjev na zaposlenega mesečno.

**Tabela 1:** Anketa o pogostosti prejemanja nezaželenih sporočil

Posledice se kažejo tudi v podjetjih, kjer jim nezaželjena pošta povzroča dodatne, nepotrebne stroške, v katere so vračunane izgube produktivnosti in izgubljene delovne ure ter stroški, ki nastanejo zaradi zakasnenih poslovnih komunikacij, porabe strežniških virov in dela administratorjev računalniških mrež. Dodatno se kopičijo stroški tudi s tem, ko odpravljamo škodo, povzročeno z zaostanki, ki so posledica prezasičenja z elektronsko pošto. Problematične so tudi posledice virusov, ki jih spam prenaša. Ocenjena škoda za ameriška podjetja v letu 2003 zaradi nezaželenih sporočil znaša 10 milijard dolarjev stroškov. Zmanjša se tudi produktivnost zaposlenih, ki prejemajo spam. Ocenjeno je, da se produktivnost



zaposlenega zaradi zaradi 13 nezaželjenih sporočil zmanjša za 1,4 %, saj ukradejo 6 minut delovnega časa.

Ker se podjetja želijo zaščititi pred nezaželeno pošto, prepovedujejo uporabljati službeni e-naslov pri spletnem nakupovanju, naročanju na e-publikacije, ki niso povezane z delovnim področjem in delovnimi nalogami zaposlenega. Podjetja omejujejo prejemanje nezaželjene pošte z odstranjevanjem elektronskih naslovov s svoje spletne strani in z nameščanjem obrazcev, preko katerih potencialne stranke navežejo stik s podjetjem.

## **Preventiva, kurativa, pritožbe**

**Objavljanje elektronskega naslova:** Pozorni bodite, kje svoj poštni naslov objavite. Pošiljatelji spam pošte pogosto s posebnimi programi prečešajo spletne strani in iz njih izbrskajo vse, kar izgleda kot veljaven elektronski naslov. Na spletu najdemo tudi specializirane storitve npr. Spam bournet. Tam lahko registriramo nov elektronski naslov in določimo, kam naj se pošta, ki pride na ta naslov posreduje, ter koliko sporočil naj se posreduje, preden se naslov zavrže. Ta storitev je namenjena predvsem registracijam produktov preko spleta, kjer moramo vpisati delujoč elektronski naslov, da lahko podjetje pošlje podatke za uporabo ali aktivacijo svojega produkta.

**Parazitski programi:** Nekateri programi vsebujejo skrite komponente, ki na našem računalniku poiščejo elektronske naslove, ki jih uporabljamo in jih pošljejo zbiralcem naslovov. Ti jih nato prodajo naprej oglaševalcem.

**Opozorilo za skrbnike:** Če smo skrbniki poštnega strežnika, obvezno preverimo, ali naš strežnik dovoli posredovanje pošte za poljubne naslove (angl. open relay). Tega strežniki večinoma ne pustijo.

**Kurativa:** Ko smo enkrat soočeni z veliko količino spam pošte, je za preventivo že prepozno. Takrat že potrebujemo filter, ki nam bo odstranil nenaročena sporočila (ali vsaj večino njih). Večina programov, ki so namenjeni odstranjevanju spam sporočil bodisi le pomaga uporabniku da izbriše sporočila, preden jih prenese v celoti na svoj računalnik, ali pa uporablja nekaj enostavnih pravil, ki poskušajo ugotoviti, kaj je spam in kaj ne. Primer takšnega programa za MS Windows operacijske sisteme je denimo *MailWasher*. Program, ki izstopa, je *SpamAssassin*, ki vsebuje veliko število pravil, ki se uporabljajo za točkovanje. Če število točk določenega sporočila preseže neko vnaprej določeno mejo, se sporočilo označi kot spam.

**Pritožbe:** Načeloma velja dogovor, da se pritožbe pošiljajo na naslov [abuse@ponudnik.com](mailto:abuse@ponudnik.com). Od prijave ISP-ju sicer ne pričakujte preveč, saj se utegne zgoditi, da vas bodo spamerji še vedno pridno spamali, a škoditi ne more.

## **4. SPAM IN SLOVENSKA ZAKONODAJA**

V svetu obstaja več različnih programov, ki preprečujejo pošiljanje nezaželene e-pošte. Ti delujejo na principu, blokiranja pošte, ki vsebuje določene ključne besede. S tem pa lahko pride do težav, saj bi se lahko nehote znebili pošte, ki bi za nas lahko bila pomembna.

Poleg tehničnih sredstev obstaja za borbo proti spamu tudi več pravnih sredstev. Tako je množično pošiljanje neželenih sporočil v nekaterih informacijsko bolj razvitih okoljih že pripeljalo do zakonskega urejanja tega področja. V zakonodajah sta poznana dva glavna sistema: "Opt-In" in "Opt-Out". Prvi sistem prepoveduje pošiljanje reklamnih sporočil po e-pošti brez poprejšnje privolitve prejemnika. Sistem "Opt-Out" pa prepoveduje pošiljanje reklamnih sporočil po e-pošti osebam, ki so izrecno izjavile, da takšnih sporočil ne želijo prejemati.

### **Primerjava Slovenije z ostalimi državami**

V evropskih državah kot so Avstrija, Danska, Finska, Nemčija, Grčija in Italija, pa tudi na Japonskem so že uvedli opt-in načelo, ki uporabnike v zadostni meri ščiti pred spamom. Tudi Slovenija se nahaja v tej skupini.

Spamerjem se je odločila stopiti na prste tudi EU. Evropski poslanci so dali zeleno luč predlogu direktive 2002/58/EC o zasebnosti elektronskih komunikacij, ki med drugim obravnava tudi problematiko pošiljanja komercialnih e-poštnih sporočil. Direktiva izrecno določa, da je uporaba e-pošte za namene neposrednega trženja dovoljena samo, kadar je posameznik to izrecno dovolil.

Področje v Sloveniji urejata dva zakona: *Zakon o varstvu potrošnikov* (uradno prečiščeno besedilo) (ZVPot-UPB2) ter *Zakon o elektronskih komunikacijah* (ZEKom).

### **Zakon o varstvu potrošnikov**

*Zakon o varstvu potrošnikov (uradno prečiščeno besedilo) (ZVPot-UPB2)*, objavljen v Uradnem listu RS št. 98/2004 (9.9.2004), in je stopil v veljavo 10.9.2004, vsebuje naslednje, za nas zanimive, člene:

#### **45.a člen**

*(1) Podjetje lahko uporablja sistem klicev brez posredovanja človeka, faksimile napravo in elektronsko pošto samo z vnaprejšnjim soglasjem posameznega potrošnika, ki mu je sporočilo namenjeno.*

4) Če potrošnik pri kateremkoli stiku, vzpostavljenim s sredstvom za komunikacijo, ki omogoča osebna sporočila, izjavi, da ne želi več prejemati sporočil na takšen način, mu podjetje ne sme več pošiljati nobenih sporočil, ki so namenjena sklenitvi pogodbe za dobavo kateregakoli blaga ali katerekoli storitve.

Ta člen določa t.i. opt-in načelo, ki je izjema od splošnega opt-out načela, ki določa, da je uporaba individualnih komunikacijskih sredstev (torej tudi elektronske pošte) dovoljena, če potrošnik temu ne nasprotuje. Če potrošnik izjavi, da ne želi več prejemati sporočil, mu podjetje ne sme več pošiljati nobenih sporočil, ki so namenjena sklenitvi pogodbe za dobavo kateregakoli blaga ali katerekoli storitve. Prejemnik sporočil mora namreč imeti nadzor nad dialogom, s tem pa tudi možnost, da se vsak trenutek lahko odnaroči od prejemanja sporočil.

### 77. člen

(1) Samostojni podjetnik posameznik se kaznuje za prekršek z globo od 1,000.000 tolarjev do 5,000.000 tolarjev, pravna oseba pa z globo od 3,000.000 tolarjev do 10,000.000 tolarjev, če:

...

22. uporablja sistem klicev brez posredovanja človeka, faksimile napravo in elektronsko pošto brez vnaprejšnjega soglasja potrošnika, ki mu je bilo sporočilo namenjeno (prvi odstavek 45.a člena);

...

(2) Z globo od 300.000 do 1,000.000 tolarjev se za prekršek kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, če stori prekršek iz prejšnjega odstavka.

V kolikor podjetje uporablja elektronski naslov brez potrošnikovega predhodnega soglasja je zaradi storjenega prekrška kaznovano s strani pristojnega nadzornega organa. Sankcije za nespoštovanje zakona so precej rigorozne, saj se lahko posameznik kaznuje z denarno kaznijo najmanj 1.000.000 tolarjev, pravna oseba pa z najmanj 3.000.000 tolarjev. Za nadziranje uresničevanja zakona skrbi Tržni inšpektorat RS, ki deluje v sklopu Ministrstva za gospodarstvo, medtem ko urad RS za varstvo potrošnikov le-te poučuje o njihovih pravicah ter jim jih pomaga uveljavljati.

Če je podjetje obtoženo pošiljanja nezaželnih elektronskih sporočil, mora dokazati, da je pred pošiljanjem sporočil pridobilo soglasje potrošnika. Urška Zupan iz Urada za varstvo potrošnikov, nam je povedala, da zakon pri tem ne predpisuje oblike omenjenega soglasja, temveč to prepušča podjetjem, ki nosijo dokazno breme, kar pomeni, da morajo v primeru nadzora s strani pristojnega organa dokazati, da so pridobili potrošnikov predhodno soglasje. V izogib morebitnim nevšečnostim se podjetjem priporoča, da skrbno dokumentirajo vsako pridobitev soglasja s strani potrošnikov.

## **Zakon o elektronskih komunikacijah**

*Zakon o elektronskih komunikacijah (ZEKom)*, objavljen v Uradnem listu RS št. 43/2004 (26.4.2004), in je stopil v veljavo 1.5.2004, vsebuje naslednje, za nas zanimive, člene:

### **109. člen (neželene komunikacije)**

*(1) Uporaba samodejnih klicnih sistemov za opravljanje klicev na naročnikovo telefonsko številko brez človekovega posredovanja (klicni avtomati), faksimilnih naprav ali elektronske pošte za namene neposrednega trženja je dovoljena samo, če naročnik predhodno soglaša s tem.*

*(2) Ne glede na določbe prejšnjega odstavka lahko fizična ali pravna oseba, ki od kupca svojih izdelkov ali storitev pridobi njegov elektronski naslov za elektronsko pošto, ta naslov uporablja za neposredno trženje svojih podobnih izdelkov ali storitev, vendar mora kupcu dati možnost, da kadarkoli na brezplačen in enostaven način zavrne takšno uporabo njegovega elektronskega naslova.*

*(3) Uporaba drugačnih sredstev za neposredno trženje s pomočjo elektronskih komunikacij kot so določena v prejšnjih dveh odstavkih tega člena, je dovoljena le s soglasjem naročnika.*

*(4) Elektronske pošte za potrebe neposrednega trženja s skrito ali prikrito identiteto pošiljatelja, v imenu katerega se sporočilo pošilja, ali brez veljavnega naslova, na katerega lahko prejemnik pošlje zahtevo za prekinitev takega neposrednega trženja, ni dovoljeno pošiljati.*

### **152. člen (prekrški)**

*(1) Z globo od 2,000.000 do 10,000.000 tolarjev se za prekršek kaznuje pravna oseba, če:*

...

*49. elektronski naslov kupca uporablja za neposredno trženje, kljub temu, da je kupec tako neposredno trženje odklonil (drugi odstavek 109. člena);*

*50. uporablja elektronske komunikacije za neposredno trženje brez soglasja naročnika (prvi odstavek 109. člena oziroma tretji odstavek 109. člena);*

*51. pri neposrednem trženju z uporabo elektronskih komunikacij uporablja lažno identiteto ali lažni naslov (četrti odstavek 109. člena);*

Za konec bi lahko dejali, da je najbolj pomembno to, da je bil storjen prvi (in to precej velik) korak v smeri zaščite uporabnikov pred nezaželeno e-pošto. Je pa res, da je zakon še precej nedodelan in da bo čas pokazal, kako bi se ta problem najboljše reševalo. Vsak posameznik, ki se zavestno odloči, da želi prejemati reklamna elektronska sporočila, mora za to imeti zagotovljeno pravico. Iz tega tudi sledi, da je kakršnokoli filtriranje elektronske pošte brez uporabnikovega soglasja nelegitimno.

## **5. SKLEP**

Živimo v dobi telekomunikacij, v dobi informacij in v dobi vse hujšega življenjskega tempa. V našem vsakdanjem življenju se zdi spam pošta kot nekakšen zaviralec, nekakšna ovira na poti do popolnega nadzora nad časom. Kakorkoli že poskušamo definirati nezaželjeno elektronsko pošto oz. spam, vedno pridemo do njenega *izvornega problema*. Ta problem je, *da poplava neželenih sporočil omejuje uporabnikovo komuniciranje na omrežju*. Ker pa se e-komuniciranje (in nasploh področje informatike ter poslovne informatike) razvija zelo hitro in iz dneva v dan vse več ljudi spoznava njegove prednosti, se zdi, da bo v prihodnjih letih problem spama uvrščen še na višja mesta kot dandanes.

Za konec ponovimo nekatera osupljiva dejstva, ki lepo predstavijo, za kako velik problem pri učinku spama na posameznika ter na poslovanje podjetij pravzaprav gre.

V letu 2004 je po podatkih raziskave podjetja Ferris Research približno 30 odstotkov vse pošte, ki je prišla na zasebne elektronske naslove, zasedla nenaročena oglasna pošta. Pri poslovnih elektronskih naslovih je bila ta številka nekoliko manjša, saj je spam predstavljal nekje med 15 in 20 odstotki celotne prispele pošte. Podatki sami sicer ne delujejo alarmantno, vendar pa naj bi to pomenilo izgubo desetih dolarjev na zaposlenega mesečno.

Ocenjena škoda za ameriška podjetja v letu 2003 zaradi nezaželenih sporočil znaša 10 milijard dolarjev stroškov. Zmanjša se tudi produktivnost zaposlenih, ki prejemajo spam. Ocenjeno je, da se produktivnost zaposlenega zaradi zaradi 13 nezaželenih sporočil zmanjša za 1,4 %, saj ukradejo 6 minut delovnega časa.

V zakonodajah sta poznana dva glavna sistema urejanja področja nezaželjene pošte: "Opt-In" in "Opt-Out". Prvi sistem prepoveduje pošiljanje reklamnih sporočil po e-pošti brez poprejšnje privolitve prejemnika. Sistem "Opt-Out" pa prepoveduje pošiljanje reklamnih sporočil po e-pošti osebam, ki so izrecno izjavile, da takšnih sporočil ne želijo prejemati. V evropskih državah kot so Avstrija, Danska, Finska, Nemčija, Grčija in Italija, pa tudi na Japonskem so že uvedli opt-in načelo, ki uporabnike v zadostni meri ščiti pred spamom. Tudi Slovenija se nahaja v tej skupini. Spamerjem se je odločila stopiti na prste tudi EU.

Žal pa državam, ki so ustrezno zaščitile svoje uporabnike, vsa ta zakonodaja ne pomaga kaj prida, dokler ves svet ne bo primerno zakonsko uredil tega področja. Tako imamo na eni strani skupino prizadevnih držav, ki poskušajo, če že ne odpraviti, pa vsaj omejiti spam, na drugi strani pa kup držav, ki tega vprašanja sploh nimajo urejenega, ali pa imajo to področje urejeno z opt-out načelom.

Zaradi globalne narave interneta so tako uporabniki sicer zaščiteni pred spamom iz Slovenije in tistih držav, ki imajo opt-in zakonodajo, ne morejo pa si kaj dosti pomagati pri boju proti spamu od drugod. Spam je globalen problem, zato bi bilo njegovo problematiko potrebno tudi reševati na globalni ravni.

## **6. LITERATURA IN VIRI**

- Skrt Radoš: In vendar se premika. Moj mikro, Ljubljana, 9.9.2003, str. 56-58.
- Gradišar Miro (et al.): Osnove poslovne informatike. Ljubljana : Ekonomska fakulteta, 2005.
- Cene Bavec (et al.): Spam – zloraba interneta. Informacijska družba IS '01, Ljubljana : Institut Jožef Stefan, 2001, str. 319-323.
- Matas Sašo: Elektronska nezaželena reklamna sporočila – spam. Pravna praksa, Ljubljana, 15/16 (2003), str. 4-6.
- [URL: <http://www.uradni-list.si/index.jsp>], 5.1.2006.
- [URL: <http://www.wikipedia.org>], 6.1.2006
- [URL: <http://www.google.com>; slikovno gradivo], 5.1.2006
- [URL: <http://www.najdi.si>; iskalni niz: “spam in slovenska zakonodaja”], 5.1.2006