UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

E- POŠTA KOT KOMUNIKACIJSKI KANAL NA DELOVNEM MESTU V JAVNI UPRAVI: VIDIK ZASEBNOSTI

Metka Guttmann

Ljubljana, december 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

E- POŠTA KOT KOMUNIKACIJSKI KANAL NA DELOVNEM MESTU V JAVNI UPRAVI: VIDIK ZASEBNOSTI

Kandidatka: Metka Guttmann
Številka indeksa: 04037919
Študijski program: visokošolski strokovni študijski program Uprava prva stopnja

Mentor: viš. pred. dr. Mitja Dečman

Ljubljana, december 2011

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Metka Guttmann, študentka Visokošolskega strokovnega študijskega programa Uprava, z vpisno številko 04037919, sem avtorica diplomskega z naslovom: E-pošta kot komunikacijski kanal na delovnem mestu v javni upravi: vidik zasebnosti.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili,
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisala v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata, bodisi v obliki skoraj dobesednega parafraziranja, bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu in sorodnih pravicah, Ur. list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo,
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko lektorirala: mag. Blanka Erhartič, prof.

Ljubljana,

Podpis avtorice:

POVZETEK

Elektronska pošta je ena izmed najbolj priljubljenih storitev zaradi prilagodljivosti, enostavne uporabe in velike učinkovitosti. Postala je eden glavnih načinov komuniciranja v informacijski družbi, predvsem v poslovnem svetu.
V prvem delu diplomske naloge se bom posvetila raziskavi pojma elektronske pošte, varnosti e-pošte, nevarnostih pri uporabi e-pošte, uporabe na delovnem mestu, ugotavljala, kakšne so pravice zaposlenih in delodajalcev v zvezi z uporabo službenega računalnika za pošiljanje elektronskih sporočil, kateri zakoni ali drugi pravni akti urejajo to področje, kako je urejeno področje drugje, izven Slovenije, kakšna je pravna praksa pri nas in v tujini v zvezi z zasebnostjo in kako je urejeno področje zasebnosti privatne elektronske pošte na področju javne uprave. V drugem delu diplomske naloge bom uporabila metodo raziskovanja s pomočjo anketnega vprašalnika. Zanima me predvsem, kakšno je znanje zaposlenih o pravicah in dolžnostih pri uporabi elektronske pošte na službenem računalniku, v kolikšni meri so seznanjeni s pravicami na podlagi zakonskih predpisov, ali so jim znane ureditve področja zasebnosti v drugih državah in še veliko drugih zanimivih vprašanj. Za analizo bom uporabila kvantitativno metodo proučevanja. Rezultate ankete bom ponazorila z grafi, in sicer za vsako vprašanje posebej, ter na podlagi rezultatov ankete prišla do samostojnih sklepov.

KLJUČNE BESEDE: sestavni deli elektronske pošte, prednosti, pomanjkljivosti, varnost in zaščita, zasebnost, nezaželena pošta, internetna pravila, poslovno komuniciranje v praksi.

SUMMARY

E-mail as a communication channel to work in public administration: privacy aspects

E-mail is one of the most popular services because of the flexibility, ease of use and great efficiency. Email has become one of the main ways of communication in the information society, especially in the business world.

In the first part of the thesis I will focus on study of the concept of email, email security, the risks of using e-mail use at work, what are the rights of employees and employers in connection with the use of company computer to send e-mails, which laws or other legal acts regulating this area, how is the scope elsewhere, outside of Slovenia, what is the legal practice at home and abroad in relation to privacy and how it regulates private e-mail privacy in public administration. In the second part of thesis research and the method by means of a questionnaire. I am interested, above all, what is the knowledge of employees about their rights and obligations when using electronic mail, a computer at work, to what extent are familiar with the rights of the right to legal regulations, or who have known the scope of privacy legislation in other countries and many other interesting issues. For the analysis I will use a quantitative method of studying.Survey results will illustrate with graphs and for each question separately and the results of the survey came to separate conclusions.

KEYWORDS: email composition, advantages, disadvantages, security and protection, privacy, SPAM, Internet rules, business communication in practice.

KAZALO

KAZALO PONAZORITEV

KAZALO GRAFOV

KAZALO SLIK

KAZALO PRILOG

1 UVOD

Hitri razvoj interneta in še posebej e-komunikacij je v našem medsebojnem komuniciranju povzročil številne korenite spremembe. Komunikacija je bila že od nekdaj temelj razvoja, e-komunikacije pa so z razvojem interneta postale življenjskega pomena.
Človeka med seboj komunicirata tako, da drug drugemu pošljeta določeno informacijo, torej je informacija poslano sporočilo med pošiljateljem in prejemnikom. V idealni situaciji sta oba na istem mestu, torej vidno ali slušno dosegljiva. Če nista, se informacija prenese po določeni prenosni poti in za izmenjavo informacij so se razvile posamezne oblike prenosnih poti, ki jih imenujemo prenosni medij ali prenosni kanal. Z razvojem računalništva so se v komunikacije vključili tudi računalniki, ki so postali najbolj zmogljiv prenosni medij za izmenjavo sporočil.
Ko se priključimo na Internet, nam elektronska pošta omogoča, da poceni in učinkovito pošiljamo sporočila s svojega računalnika preko Interneta drugim uporabnikom omrežja. Elektronska pošta je ena izmed najbolj priljubljenih storitev zaradi prilagodljivosti, enostavne uporabe in velike učinkovitosti. Postala je eden glavnih načinov komuniciranja v informacijski družbi, predvsem v poslovnem svetu. Ena njenih glavnih prednosti je hiter prenos podatkov do prejemnika, kar pa se lahko izkaže tudi za slabost, saj se z gostoto prometa povečuje tudi možnost napak in zmede. Če bomo upoštevali vsa priporočila in se izognili slabostim, bomo lahko še dolgo uživali v prednostih takega komuniciranja. Tajnost elektronske pošte je »ranljiva« na več načinov in na več mestih.
Poraja se tudi večno vprašanje zasebnosti elektronske pošte na delovnem mestu. Vprašanje zasebnosti e-pošte v odnosu delodajalec-delojemalec je še posebej občutljivo, ker še vedno ni znano, kakšno stopnjo zasebnosti lahko zaposleni na delovnem mestu pričakuje. Prisotna sta interes delodajalca in interes zaposlenega, ki si seveda nasprotujeta.
Praviloma je računalnik, ki ga zaposleni uporablja, v lasti delodajalca, prav tako je elektronski naslov delojemalcu dodeljen le za opravljanje službenih zadev. Po drugi strani pa ima zaposleni pravico do zasebnosti tudi na delovnem mestu. In ker še vedno najpogosteje vstopamo do interneta prek službenih računalnikov in službenih povezav, je mnenje mnogih delodajalcev, da je pomembno, da se zavedamo osnovnega pravila, naj bi se e-komunikacija prek službenega računalnika s službenim e-naslovom nanašala predvsem na poslovno e-komunikacijo določenega podjetja. Vendar je realnost bistveno drugačna, velikokrat se uporablja službeni računalnik za pošiljanje privatnih sporočil. Seveda pa zaposlenega ščitijo ustava in zakoni, ki pravijo, da ima zaposleni pravico do zasebnosti na delovnem mestu, kar potrjuje tudi evropska pravna praksa, ki je na strani zaposlenega in ga vidi kot človeško bitje z določenimi pravicami.
Slovenija je razmeroma dobro razvita informacijska družba. Predvsem na področju javne uprave je porast uporabe interneta, elektronske pošte in drugih možnosti elektronskega poslovanja in komuniciranja zelo velika.
Namen moje diplomske naloge je celovito prikazati pravice na področju uporabe in zasebnosti elektronskih sporočil na delovnem mestu, kar vključuje tudi primerjave z ureditvijo področja zasebnosti elektronskih sporočil v nekaterih drugih državah Evropske unije in v Ameriki.
Cilj naloge je raziskati vse pozitivne in negativne učinke uporabe elektronske pošte na delovnem mestu in predvsem ugotoviti, kakšno je védenje zaposlenih o pravicah v zvezi z zasebnostjo uporabe privatnih elektronskih sporočil na delovnem mestu. Če torej menimo, da nam je delodajalec v skladu z ustavo in drugimi pravnimi akti kršil pravico do varstva osebnih podatkov, s tem ko je pogledal v podatke naše elektronske pošte, bi morali primerno ukrepati. Cilj naloge je tudi ugotoviti, kakšni so v takšnem primeru naši nadaljnji

koraki ter kaj lahko storimo mi in kaj država, da v prihodnosti preprečimo takšna ravnanja.

2 ELEKTRONSKA POŠTA

2.1 ZGODOVINA ELEKTRONSKE POŠTE

Elektronska pošta je že pred leti postala prevladujoč način pisne komunikacije, pravzaprav je v marsičem izpodrinila klasično pošto. Če smo še pred leti vse uradne zadeve urejali po klasični priporočeni pošti, je dandanes elektronska pošta tudi za večino teh opravil precej enostavnejša in hitrejša alternativna možnost.
Elektronska pošta se zdi precej nova tehnologija, pa vendar zametki segajo v zgodnja šestdeseta leta. Takrat so nastali prvi računalniki, na katerih se je lahko izvajalo več programov hkrati, in že takrat so nekateri raziskovalni centri v ZDA razvili programe za prenos besedilnih sporočil znotraj podjetja. Ključni korak pa je naredilo ameriško ministrstvo za obrambo s projektom ARPANET (Advanced Research Projects Agency Network), ki velja za prvo delujoče omrežje za izmenjavo paketov in je bilo predhodnik globalnih omrežij (internet). ARPANET je bil tudi temelj razvoja drugih tehnologij, ki temeljijo na izmenjavi podatkov prek omrežij. V zgodnjih sedemdesetih letih se je pravi razvoj take komunikacije začel tudi v smeri elektronske pošte, kot jo poznamo danes. Leta 1983 se je to omrežje preimenovalo v MILNET (military) in takrat so prvič vključili privatno elektronsko pošto (e-mail). Naslednji preskok se je zgodil, ko je Marty Yonke razvil program z nenavadnim imenom WRD/BANANARD - to je bil prvi program, ki je omogočal branje in pošiljanje pošte. Pred tem je bilo branje in pošiljanje besedila ter datotek popolnoma ločeno. Prvi "moderni" program za izmenjavo elektronske pošte je z izboljšavo BANANARD-a uspel Johnu Vittalu, saj je vključil še posredovanje sporočil, prilagodljiv uporabniški vmesnik in avtomatični odzivnik. Ray Tomlinson je iskal primeren znak in pri tem hotel zagotoviti, da se ta znak ne bo pojavljal v nobenem drugem delu sporočila. Izbira je bila logična, danes pa se je znak @ udomačil kot zaščitni znak Interneta.Komercializacija elektronske pošte se je začela okrog leta 1988, ko je prišlo do poskusne uporabe omrežja NSFNET (National Science Foundation Network). Omrežje so uporabljali predvsem inštituti, obsegalo pa je več kot 170 podomrežij. Leta 1991 je NSFNET odprl svoj dostop in prešel v komercialno rabo. Zaradi tega se je začel silno hitro širiti. Leta 1993, ko sta velika ameriška ponudnika omrežnih storitev America Online in Delphi svoji omrežji za elektronsko pošto povezala v internet, je elektronska pošta postala globalni standard (Humar, 2006).
Nekateri trdijo, da se je leta 1976, ko je britanska kraljica Elizabeta II. poslala prvo elektronsko pošto, začelo novo obdobje našega medsebojnega komuniciranja.

2.2 POJEM ELEKTRONSKE POŠTE

Elektronska pošta je ena izmed osnovnih storitev in hkrati najbolj razširjen del Interneta. Omogoča nam pošiljanje sporočil na drugo računalniško omrežje in zato se vedno bolj vpliva na opuščanje tradicionalne metode "pisala in papirja", ki je zelo počasna in imenovana "polžja pošta" (snail mail).
Elektronska pošta ima sposobnosti in značilnosti, ki presegajo vsak medij, ki ga je svet kadar koli videl ali uporabljal. Medij je metoda, po kateri prenesemo sporočilo. Elektronska pošta spada v sredino vseh drugih medijev (osebni kontakt, telefonski klic, faks, hitra dostava, standardna pošta ...), saj prispe dokaj hitro in tudi nujnost odgovora je dokaj visoka. Elektronska pošta je pošta, ki jo izdelamo in pošiljamo elektronsko, torej je poslana s pomočjo nekega računalnika in sprejeta s pomočjo nekega drugega računalnika na drugi lokaciji. Na področju elektronskega sporočanja se uveljavlja izraz »nematerializirana oblika«, kar pomeni, da na papirju ni materializirana. S fizikalnega stališča je to neutemeljena raba, saj za neposredno prepoznavanje vsebine potrebujemo

posebno napravo in takšna sklepanja sodobnih oblik poslovanja ne podpirajo, temveč jih celo ovirajo (Alspah,1996).
Poznamo dva tipa elektronske pošte: lokalna elektronska pošta (Intranet) in Internet elektronska pošta. Lokalna elektronska pošta je navadno pošta znotraj določenega sistema (znotraj delovne organizacije). Zelo je dobrodošla pri seznanjanju zaposlenih:

- z novimi zakoni in predpisi
- s pravilniki
- z notranjimi navodili
- za okrožnice
- s pomembnimi sklepi organov
- z novimi obrazci
- z razporedi dela
- z letnim koledarjem, novimi poslovnimi partnerji itd.

Internet elektronska pošta lahko potuje do kogar koli v katerem koli sistemu, če je ta povezan na Internet. Preprosto bi lahko rekli, da gre za sistem, ki skrbi za pošiljanje tekstovnih sporočil drugim uporabnikom.

2.3 SISTEM ELEKTRONSKE POŠTE

»Ko pošljemo elektronsko pošto, naš računalnik sporočilo preda strežniku SMTP. Navadno je to strežnik našega internetnega ponudnika ali pa strežnik v krajevnem omrežju. Ta strežnik je praviloma nastavljen tako, da vedno sprejme našo pošto, ker prihaja iz krajevnega omrežja, ki mu strežnik lahko zaupa.
Strežnik potem pregleda naslove prejemnikov, če strežnika za dostavo ne najde, mora sporočilo zavrniti. Noben poštni strežnik v nobenem primeru ne sme tiho požreti sporočila, edina izjema od tega pravila pa je sporočilo o dvojni napaki (ko obvestila o napaki pri dostavi ni mogoče dostaviti, ker je pošiljateljev naslov neveljaven in nima smisla generirati še enega obvestila, ker ga nimamo komu poslati). Takoj ko poštni strežnik sporočilo sprejme in potrdi prejem, postane odgovoren za njegovo pravilno dostavo; če dostava ni možna, mora poslati sporočilo o napaki na naslov pošiljatelja.

Slika 1: Sistem elektronske pošte

Vir: www.arnes.si (2006)

Ko poštni strežnik sprejme pošto, ki je namenjena v poštni predal v samem strežniku, navadno sporočilo dostavi naravnost na disk. Ko je sporočilo dostavljeno v uporabnikov predal, je njegova pot skozi omrežje SMTP končana« (Koren, 2005).

3 PREDNOSTI IN POMANJKLJIVOSTI ELEKTRONSKE POŠTE

3.1 E-POŠTA KOT ALTERNATIVA

Zelo težko je določiti, kdaj je primerneje uporabiti elektronsko pošto namesto katerega bolj tradicionalnega orodja za komuniciranje. Možnost za izbiro nam ponudi primerjava prednosti in slabosti elektronske pošte v nasprotju z ostalimi mediji. Vsekakor pa elektronska pošta ni nadomestek za ostale komunikacijske možnosti, ampak kvečjemu alternativa današnje dobe.

OSEBNI KONTAKT V PRIMERJAVI Z ELEKTRONSKO POŠTO
Osebi kontakt je najučinkovitejša in hkrati najtežja oblika komuniciranja. Sporočilo je običajno v celoti spontano, besede mogoče ne bodo vedno izražale našega mišljenja, to pa lahko zaostri komuniciranje. V primerjavi z osebnim kontaktom je elektronska pošta lažja oblika komuniciranja, je zelo primerna za vzpostavitev kontakta in pri tem ne potrebujemo niti poslovne obleke, razen tega si lahko vzamemo čas za pripravo sporočil. Težava nastane samo v primeru, kadar prejemnik sporočila ne prebere in ga preprosto izbriše iz računalnika.

TELEFONSKI KLICI V PRIMERJAVI Z ELEKTRONSKO POŠTO
Telefon je primernejša oblika komuniciranja kot osebni kontakt, lahko kličemo od koderkoli, lahko si pripravimo zapiske za pogovor ali se kako drugače pripravimo nanj, smer pogovora lahko prilagajamo sebi in s tem pridobimo prednost pred sogovornikom. Pošiljanje elektronske pošte nam nudi možnost in oblast, da izrazimo svoje misli in zapiske, pri telefonskem pogovoru pa je prisotna stalna interakcija in prekinjanje z nasprotne strani.

FAKS V PRIMERJAVI Z ELEKTRONSKO POŠTO
Faks je komunikacijska oblika, ki je najbolj podobna elektronski pošti. Razlika je predvsem v kvaliteti. Izpis faksa je večinoma težko berljiv, sporočilo je potrebno stiskati in ga poslati skozi faks napravo. Nasprotno pa je kvaliteta elektronske pošte na Internetu vedno tako dobra, kot je kvaliteten prikaz besedila na prejemnikovem monitorju.

POŠTNI SERVIS V PRIMERJAVI Z ELEKTRONSKO POŠTO
Pošiljanje pošte preko poštnega servisa v primerjavi z elektronsko pošto je časovno neugodno, predvsem kadar pošiljamo pismo nekomu na drug konec sveta, lahko to traja več dni.

3.2 PREDNOSTI IN POMANKLJIVOSTI ELEKTRONSKE POŠTE

Ugotovili smo, da se elektronska pošta splača, saj prinaša posredne in neposredne koristi kot so finančni prihranki in boljša obveščenost, ki je eden ključnih pogojev za uspešno sodelovanje.

Prednosti elektronske pošte so naslednje:
- nizka cena v primerjavi s pismom, telefaksom ali telefonskim pogovorom,
- večja hitrost v primerjavi z običajno pošto,
- prihranek časa,
- kakovost napisanega sporočila se ne spremeni in je na voljo za nadaljnjo obdelavo v računalniku,
- možnost pošiljanja istega sporočila enemu ali več naslovnikom hkrati,

- zanesljivost delovanja elektronske pošte je precej večja v primerjavi z običajno pošto,
- omogoča nam boljši stik s strankami (sprejemanje želja, kritik, pripomb …),
- naročimo lahko prejemanje elektronskih dokumentov (obvestila, cenike, novice …),
- lahko jo uporabimo za bančno poslovanje,
- uporabimo jo lahko tudi za tržne raziskave s pomočjo vprašalnikov,
- prednost elektronske pošte je prav tako možnost iskanja prejetih in poslanih sporočil,
- študij na daljavo (prejemanje gradiva, komunikacija s profesorji …).

Verjetno je še kar nekaj prednosti, ki bi jih lahko našteli, vendar ima vsak dobra stvar tudi slabosti, ki pa so lahko v primeru elektronske pošte zelo nevarne, če ne upoštevamo pravil in priporočil za njihovo preprečevanje.

Slabe strani so:
- možnost, da elektronsko pošto preberejo nepooblaščene osebe,
- napake v programu poštnega strežnika – izguba pošte,
- možnost, da prejmemo računalniški virus,
- nezaželena elektronska pošta ali SPAM,
- prikrajšani smo za osebni stik - elektronske čestitke nimajo enakega pomena kot tiste, ki smo jih napisali z roko in pozabimo na sproščen pogovor ob dobri glasbi med prijatelji,
- odvisnost od elektronske pošte itd.

Tajnost elektronske pošte je »ranljiva« na več načinov in na več mestih. Dandanes obstajajo različna sredstva varovanja, ki takšen vdor v zaupnost sporočila lahko preprečijo. S tehničnega vidika je možno poseči na več mestih: v računalniku pošiljatelja ali naslovnika, v računalniku strežnika ponudnika dostopa do interneta, med potovanjem elektronske pošte po telefonskem ali drugem kablu do omenjenega strežnika in med potovanjem elektronske pošte v globalnem računalniškem omrežju.

3.3 VARNOST E-POŠTE

Pogoj za uspešno komuniciranje je tudi zagotavljanje varnosti in zasebnosti na internetu. Poskrbimo, da bo naša komunikacija z zunanjim svetom varna in zakonsko neoporečna.
Nova tehnologija ponuja vrsto rešitev, tako strojnih in programskih, ki služijo zavarovanosti posameznika in podjetja pri uporabi interneta in e-pošte. Posebej zanimive in povprečnemu posamezniku dostopne so programske rešitve, t.i. Tehnologije za dviganje ravni varstva zasebnosti (Privacy - Enhancing Technologies). Sem spadajo požarni zidovi, programska oprema za filtriranje pošte, »ubijalci« piškotkov, šifriranje - kodiranje elektronske pošte, digitalni podpis, digitalni certifikat itd. (po Makaroviču in dr., 2001, str. 145).
Z uporabo ustreznih tehnologij in programov poskrbimo za zaščito računalnika pri povezavi na internet kot tudi pred napadi virusov in vdori hekerjev. Poskrbimo, da bomo imeli nameščene najnovejše popravke operacijskega sistema, posodobljene različice proti virusnih programov in programov, ki jih uporabljamo za komunikacijo. Uporaba protivirusnih programov naj bo na prioritetni listi, saj se nam tako ne bo potrebno opravičevati, če bomo nehote razpošiljali viruse svojim prijateljem, znancem in poslovnim partnerjem. Če ne uporabljamo postopkov enkripcije, se moramo zavedati, da obstaja verjetnost, da bo nepooblaščena oseba prebrala naše sporočilo.

Zaradi tega je priporočljivo, da naše sporočilo ne vsebuje ničesar, česar si ne bi upali napisati na dopisnico, ter da si ob službenem e-naslovu odpremo pri enem izmed spletnih ponudnikov brezplačne e-pošte še dodatni e-naslov, ki ga bomo uporabljali za zasebno korespondenco.

3.4 NEVARNOSTI E-POŠTE

E-pošta je v komuniciranju ponudila veliko možnosti za komuniciranje kadarkoli, s komerkoli, ki je vključen v internet. Zaradi relativno lahko dosegljivih e-poštnih naslovov mnogi izkoriščajo e-pošto tudi za doseganje različnih ciljev ali za razširjanje različnih idej. Izogibamo se vsem e-sporočilom, ki obljubljajo lahko delo, celo delo na domu, ob katerem boste veliko zaslužili; investicije, vlaganje denarja v vsemogoče projekte, ob katerih boste veliko zaslužili; piramidne in verižne oblike velikega zaslužka, ko nekomu pošljete denar in nekdo pošlje denar tudi vam; ugodne kredite, pri katerih ne boste nikoli na zgubi; velik dobitek ali nagrado, če boste poklicali določeno telefonsko številko, ki je običajno mednarodna številka in za katero plačate več, ali pa lokalna telefonska številka z dragimi telefonskimi impulzi; čudeže z uporabo diet, medicinske pomoči ali drugačnih izdelkov; srečo v igrah verižnih pisem in uspeh, če odkrijete kakšen vaš podatek, telefonsko številko, številko kreditne kartice ali kaj podobnega.
V e-pošti so posebej izpostavljeni otroci oz. najmlajši, predvsem zaradi neprimernega seksualnega, pornografskega, pedofilskega in podobnega materiala; zaradi vznemirjanja; ponujanja različnih priložnosti za uspeh; vdora v zasebnost ob odkrivanju podatkov o družini; zagovarjanja mamil, alkohola, tobačnih izdelkov in ponujanja iger na srečo.

3.5 SPAM – NEZAŽELENA POŠTA

Nenaročeno oglasno pošto v angleško govorečih državah imenujejo SPAM, ta naziv pa se je dodobra udomačil tudi pri nas. Spam je angleška beseda za mesni narezek, nenaročene pošte pa se je ta vzdevek prijel po skeču kultnih Monty Python. Seveda pa spam kot takšen ni prav nič zabaven in duhovit, saj je v zadnjih letih iz razmeroma neškodljive in nevljudne motnje postal že prava digitalna kuga. Najbrž ne bi več mogli najti uporabnika interneta, ki na svoj elektronski naslov še nikoli ni prejel nenaročenega oglasnega sporočila.
Proti nezaželeni pošti se je izredno težko boriti, saj najdejo pošiljatelji vedno nove in nove načine, da pridejo v naš e-poštni predal. Kljub vsem orodjem in možnostim, ki jih imajo podjetja na voljo pri omejevanju nezaželene elektronske pošte, celovite rešitve žal ni.
Zaščita pred nezaželeno pošto je sila težavna, saj praviloma elektronska sporočila ne nosijo nekega skupnega imenovalca, po katerem jih je možno prepoznati in ukiniti. Nezaželeno pošto lahko omejimo, nikakor pa je ne moremo v celoti odpraviti. Pomagamo si lahko s programi, ki nezaželeno elektronsko pošto blokirajo na e-poštnem strežniku ali pa pri končnem prejemniku e-sporočil.
Rezultati raziskav kažejo, da je 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 (Ocvirk, 2003).
Število neželenih ali SPAM elektronskih sporočil nezadržno narašča. Spam filtri njenemu naraščanju niso več kos, saj ti odstranjujejo vedno več želenih e-sporočil, kar uporabnikom povzroča precej težav.

SPAM in slovenska zakonodaja
Dopolnjen Zakon o varstvu potrošnikov obravnava med drugim tudi pošiljanje nezaželene elektronske pošte. Navedeno problematiko ureja omenjeni zakon v 45. a členu, ki določa,

da lahko podjetje uporablja elektronsko pošto samo z vnaprejšnjim soglasjem posameznega potrošnika, ki mu je sporočilo namenjeno. Pri tem gre za t.i. pot-in načelo, ki je izjema od splošnega pot-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. V kolikor podjetje uporablja elektronski naslov brez potrošnikovega predhodnega soglasja, je zaradi storjenega prekrška kaznovano s strani pristojnega nadzornega organa (Radoš,2003).
Za nadziranje uresničevanja zakona skrbi Tržni inšpektorat RS, ki deluje v sklopu Ministrstva za gospodarstvo, medtem ko urad RS za varstvo potrošnikov te poučuje o njihovih pravicah ter jim jih pomaga uveljavljati.

3.6 VIRUSI

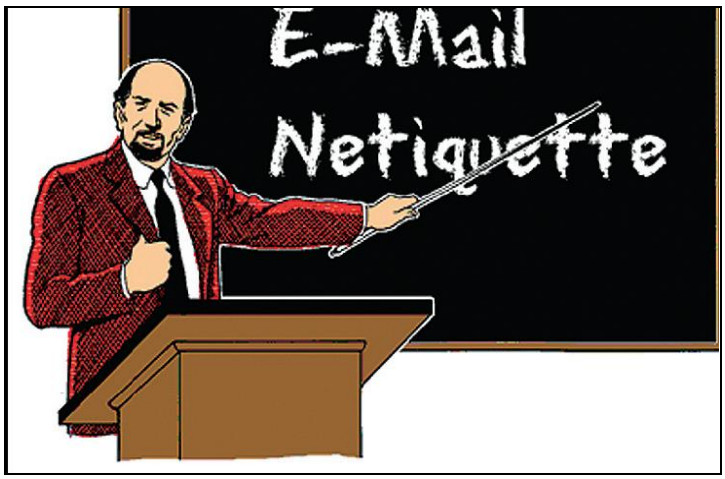
Na področju tehnologije računalniških virusov in črvov pogosto svet pretrese novica o tem ali onem črvu, ki pustoši po internetu. Virus predstavlja posebno vrsto računalniškega programa, napisanega z namenom, da uničuje podatke v osebnem računalniku oziroma otežuje delo s programsko opremo, ki je nameščena na osebnem računalniku.
Samo ime "virus" izhaja iz dejstva, da je virus potem, ko je okužil magnetni medij, težko odkriti, saj lahko preteče nekaj časa od okužbe pa do trenutka, ko virus začne povzročati težave (virusi, ki se zaženejo na določen datum).
Z razvojem Interneta pa se virusi danes prenašajo in okužujejo računalnike - magnetne medije s pomočjo elektronskih sporočil, ki so jim pripeti virusi v obliki priloženih datotek, oziroma preko drugačnih načinov izmenjave podatkov.
Virusi večinoma napadajo ukazne datoteke (bat, Ece, dom, Sas), kar ima za posledico nepravilno delovanje programov ali celo izgubo podatkov zaradi sprememb, nastalih v ukaznih datotekah, ki so spremenile lastnosti "originalnih" datotek. Vse bolj pa se "uveljavljajo" MACRO virusi, ki se širijo preko dokumentov, napisanih na primer z urejevalnikom besedil (Ministrstvo za šolstvo in šport in Zavod Republike Slovenije za šolstvo, 2011).
In čeprav dandanes vemo o virusih veliko več kot, recimo, pred dvema letoma, še vedno podlegamo istim starim zvijačam. Morda bi morali na te težave pogledati iz drugega zornega kota in jih morda tudi drugače ovrednotiti. Najbrž je že res napočil čas, da se vprašamo, zakaj se nam vedno dogajajo ene in iste reči.
V naš poštni predal prispe sporočilo s priponko, mi kliknemo nanjo in cirkus se začne. Vzroke lahko strnemo v tri glavne skupine: radovednost, premajhna skrb za proti virusne programe in prevelika ranljivost programske opreme ter operacijskih sistemov nasploh. Na prvem mestu je najbrž pregovorna človeška radovednost. Priponke, na katere neutrudno klikamo, čeprav vemo, kaj to pomeni, lahko enačimo z velikim rdečim gumbom na steni kakšne jedrske elektrarne, ob katerem visi kričeč napis: »Strogo prepovedano pritisniti na rdeči gumb!«. Odgovor lahko potegnemo kar iz domače psihološke delavnice: prav radovednost je tista, ki nas sili v dejanja, ki so v svoji naravi povsem sprta z logiko. Virusi, črvi in trojanski konji delujejo prav po tem načelu. Logika, ki stoji za škodljivo kodo v priponki, sklepa, da se ne bomo mogli upreti radovednosti in bomo kliknili na priponko. Stvar postane še toliko bolj zanimiva, če smo sporočilo prejeli od znanega uporabnika. Med goro SPAMA-a se znajde sporočilo, ki nam ga je poslal nekdo, ki ga poznamo. Le zakaj ne bi kliknili na priponko? Prav to je največja napaka, saj večina najbolj prodornih virusov za lastno razmnoževanje uporabi naslove, ki jih pobere v imeniku okuženega računalnika. In kdo drug bo imel naš naslov, če ne ravno nekdo, ki ga poznamo?« (Ocvirk, 2003).

S hitrim porastom števila vedno novih virusov se je zelo težko ubraniti pred vdorom virusov v računalnik. Antivirusni programi, ki so pisani z namenom preprečevanja, odkrivanja in brisanja virusov, hitro zastarajo, saj starejši ne vsebujejo informacij o novo nastalih virusih in jih tudi ne odkrijejo.
Do neke mere se tej nevšečnosti izognemo s stalnim (mesečnim) obnavljanjem antivirusnih programov.

3.7 BONTON IN KULTURA PRI MEDSEBOJNI KOMUNIKACIJI S UPORABO E-POŠTE

Začetno obdobje razvoja elektronskih komunikacij je še vedno vsebovalo običajna in tradicionalna pravila lepega vedenja, obnašanja, kjer sta bila pozdrav in takojšnji odgovor samoumevna. V začetnem obdobju razvoja interneta je veljalo osnovno opozorilo vsem, ki so sodelovali v tem omrežju, da je pomembno, da se zavedajo svoje odgovornosti, ko vstopajo na takrat redke spletne strani, ko se vključujejo v pogovorne skupine ali pošiljajo elektronsko pošto.
»Tako kot v normalnem okolju pri vsakodnevnem komuniciranju z ljudmi, je potrebno tudi na internetu upoštevati poleg pravnih zakonov, ki predpisujejo, kaj je dovoljeno in kaj ne, tudi določena pravila obnašanja in nenapisane norme, če želimo, da bo komunikacija z ostalimi uporabniki potekala normalno in na spodobnem nivoju.« (Radoš, 2005)
Osnove tega bontona v e-dopisovanju oz. e-pošti so izredno pomembne, saj nas lahko neobičajno pogosti način e-sporazumevanja včasih privede tudi v nenavadne situacije, ko lahko zaradi »lahkotnosti« pisanja pisem iz pričakovane formalne komunikacije preidemo v neformalno komuniciranje. In tudi to zahteva in potrebuje določena pravila »e-vedenja«.
Ob takšni razprostranjenosti in pogostosti e-komuniciranja pa je vse bolj izginjalo upoštevanje osnovnih pravil lepega vedenja, ki še vedno veljajo v medsebojnem sporazumevanju, med prijatelji, partnerji ali, še pomembnejše, med neznanci. Zato so že na začetku razvoja interneta in e-pošte nastala določena pravila lepega vedenja, bonton e-sporazumevanja, imenovan tudi omrežni bonton oz. »netiketa« (netiquette) (Radoš, 2005).

Slika 2: Omrežni bonton – Netiquette



Vir: Radoš (2005)

Med uporabniki elektronske pošte pogosto prihaja do nesporazumov, zato je dobro, če poznamo nekaj osnovnih pravil lepega vedenja:

- prek elektronske pošte nikoli ne pošiljajte oglasov;
- sporočil ne zapisujte s samimi velikimi črkami;
- jezik, ki ga uporabljate, naj ne bo preveč osoren;
- na verižna pisma ne odgovarjajte;
- preden pošljete sporočilo, preverite, če je sporočilo primerno napisano in če ga pošiljate resnično pravi osebi;
- skrivnosti in zaupne podatke ne pošiljajte po elektronski pošti, saj vemo, da ta ni povsem varna;
- izogibajte se pripenjanju večjih datotek, posebej takrat, kadar jih prejemnik ne pričakuje;
- ne uporabljajte elektronske pošte do onemoglosti in za vsako malenkost, nepomembna sporočila nimajo nobenega smisla, o nekaterih stvareh se lahko bolje pogovorimo po telefonu ali v neposrednem stiku;
- ne pošiljajte drugim osebam filmskih posnetkov, zabavnih programov, raznih fotografij, slik in podobnih stvari, če niste prepričani, da oseba na drugi strani to želi;
- ne govorite/sporočajte brez cilja, saj je lahko to utrudljivo, bodite kratki in jedrnati;
- ne opravljajte drugih ljudi, saj lahko elektronska pošta kar hitro zaide v neprave roke;
- odgovarjajte hitro;
- nikoli ne pošiljate po elektronski pošti sporočil, ki bi jih tudi ustno ne izrekli;
- prepričajte se, da vrstica za opis namena sporočila resnično izraža vsebino sporočila;
- do vseh se obnašajte kot do človeških bitij – vsaka oseba si zasluži spoštovanje;
- preverite svojo elektronsko pošto vsaj enkrat dnevno;
- podpisi naj bodo krajši od vsebine sporočila;
- ne predpostavljajte spola prejemnika, saj je iz naslova elektronske pošte velikokrat nemogoče ugotoviti spol prejemnika;
- izognite se seksualnemu namigovanju;
- vaše besede kreirajo vašo podobo, prejemnik mogoče ne bo edina oseba, ki bo brala vaše sporočilo.

Verjetno je še precej več pravil, ki bi jih morali upoštevati, vendar bo zadoščalo, če upoštevamo teh nekaj najpomembnejših nasvetov in osnovno pravilo vsakega bontona, ki pravi, da moramo ne glede na okoliščine spoštovati in biti pozorni do drugih ljudi.

3.8 VPLIV UPORABE ELEKTRONSKE POŠTE NA NAŠE ZDRAVJE

Delo z računalnikom je lahko utrujajoče in lahko negativno vpliva na uporabnikovo zdravje. Načela ureditve učinkovitega in za zdravje čim manj obremenjujočega delovnega mesta so starejša od računalniške tehnologije. Vprašanje pa je, ali se teh načel držimo?
»Zdravstveni strokovnjaki opozarjajo, da zaposleni ljudje v pisarnah premalo poskrbijo za gibanje svojega telesa. Glavni razlog za to naj bi bila elektronska pošta. Svojemu sodelavcu tako raje pošljejo elektronsko sporočilo, kot da bi vstali in mu novico predali ustno. Mednarodni strokovnjak za srčne težave dr. Dorian Dugmoren je prepričan, da bi povečanje telesne aktivnosti za vsaj 10 odstotkov zmanjšalo število smrti za vsaj 6000 ljudi. S tem bi hkrati privarčevali veliko denarja.

Tako so se nekatere družbe, zlasti v Britaniji, odločile, da bodo uvedle ***"dan brez elektronske pošte"***. Na ta dan zaposleni ne bodo smeli niti prebrati niti napisati nobenega elektronskega sporočila. Če bodo sodelavcu želeli kaj povedati, bodo pač morali vstati in jim to povedati ustno« (M.K., 2005).

3.9 KRIPTOGRAFIJA – TAJNOPISNE TEHNIKE

»Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). Beseda prihaja iz grščine: kryptos logos pomeni skrita beseda. Uporabljata se še pojma enkripcija (šifriranje) in dekripcija.
Osnovno sporočilo po navadi imenujemo čistopis (cleartext, plaintext), zašifrirano pa šifropis ali tajnopis(kriptogram, ciphertext)« (SERŠ Maribor, 2011).
Z besedo *kriptografija* označujemo metode za zaščito vsebine podatkov. Sporočilo zakrijemo z enkripcijsko metodo in enkripcijskim ključem ter dobimo kriptogram, ki ga lahko pošljemo naslovniku. Naslovnik nato kriptogram s pomočjo dekripcijske metode in dekripcijskega ključa predela v izvorno obliko sporočila. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila.
Začetki uporabe kriptografije segajo v čase pred našim štetjem. Razvitih je bilo nešteto načinov za zakrivanje sporočil. Prestrezanje sporočil ni bilo v navadi samo v vojnih časih, predvsem prestrezanje diplomatske pošte je bila običajna praksa. Na dvorih so obstajale "črne sobe", kjer so poskušali razvozlati prestrežena in prepisana sporočila.
Špartanci so uporabljali naslednji način: na valj so navili ozek trak in sporočilo napisali pravokotno na smer traku. Poslali so odvit trak, naslovnik pa je moral imeti valj enakega premera.
Julij Cezar je svojim vojskovodjem pošiljal sporočila, kjer je vsako črko zamenjal s črko, ki je bila v abecedi nekaj mest za njo (SERŠ Maribor, 2011).
Glede enkripcijskega in dekripcijskega ključa poznamo dve vrsti kriptografije - *simetrično*, ki za kodiranje in dekodiranje sporočila uporablja isti ključ, ter *nesimetrično*, kjer je ključ za kodiranje različen od ključa za dekodiranje.
»Junija leta 1991 je Phil Zimmerman napisal program PGP (Pretty Good Privacy), ki vsebuje RSA algoritem za kodiranje sporočil na osebnih računalnikih. Razlog za to je bil v tem, da RSA kodirni algoritem za razliko od ostalih onemogoča, da bi kdorkoli - tudi država - prisluškoval (elektronskim) komunikacijam posameznika. Ker Zimmerman meni, da sta demokracija in zaščita zasebnosti neločljivo povezani, "edini način za zaščito zasebnosti pa je močna kriptografija", je sklenil, da omenjena tehnologija pripada vsem ljudem. Istega leta kot je Zimmerman napisal program PGP, je ameriški Senat obravnaval zakon, ki bi prepovedal tovrstno kriptografijo. Zimmerman je zato svoj program javno objavil in dovolil brezplačno kopiranje, neznanci pa so njegov program razširili po vsem svetu. Program je v dveh letih postal standard za učinkovito zaščito podatkov in elektronske pošte« (Kovačič, 2000).
»Predvsem informacijska in komunikacijska zasebnost se pogosto varuje s tajnostjo. Zato kriptografija velja za eno poglavitnih tehnologij zaščite zasebnosti (na internetu).
Vendar se pogosto zastavlja vprašanje, ali je upravičeno, da je vsaka zasebna stvar tudi tajna, iz česar izvirajo tudi poizkusi omejevanja kriptografije. Določena zasebna razmerja in zasebne informacije so namreč sicer lahko del zasebne sfere, a je včasih upravičeno, da "izstopijo" iz nje. Take izjeme veljajo predvsem v primerih, ko so ogroženi javni interesi (npr. varnost, javno zdravje) ali ko gre za varovanje pravic drugih posameznikov« (Kovačič, 2006, stran 44).

3.10 UPOŠTEVANJE INTERNETNIH PRAVIL

V začetnem obdobju razvoja interneta je kultura tovrstnega e-komuniciranja dosegla najvišjo raven in takrat so nastala nekakšna pravila oz. odgovornosti uporabnikov interneta. Obveljalo je večno pravilo, da na internetu in tudi v e-pošti ni nič povsem zasebno in da lahko vso e-pošto v določenih primerih lahko prebirajo tudi drugi.
Prva nenapisana pravila internetnega lepega vedenja so poudarjala, da z vstopom v to omrežje vstopamo tudi v tiste dele sveta, kjer imajo drugačno politiko, kjer imajo drugačna pravila in kjer je nekaj dovoljeno in nekaj prepovedano.
Začetni izziv interneta je prinesel ugotovitev, da uporaba svetovnega omrežja za uporabnika ni bila pravica, ampak privilegij, ki se je lahko v primeru izkoriščevalskega ali neprimernega vedenja preklical. Med takratno neprimerno vedenje je sodilo na primer prenašanje ilegalnih podatkov, uporaba grdega jezika ali zlorabe jezika v sporočilih, pošiljanje sporočil, ki imajo lahko za rezultat onemogočeno delo sistema, pošiljanje verižne pošte, t.i. Chain letters. Napisane so bile osnovne zapovedi, kot so, da računalnika ne bi uporabljali v škodo drugih, da z računalnikom ne bi motili dela drugih, ki tudi delajo z računalniki, da z računalnikom ne bi "brskali" po datotekah drugih, da računalnika ne bi uporabljali za kraje in laganje, da z računalnikom ne bi kopirali programske opreme, ki je nismo plačali oziroma kupili in ne bi uporabljali tujih računalniških virov brez dovoljenja lastnikov in si ne bi prilaščali proizvodov drugih. Predvsem pa bi morali razmišljati na posledice tistega, kar pišemo v računalnik in da bi ga uporabljali tako, da bi spoštovali in upoštevali druge.
Na koncu pa bi želela še omeniti prvo internetno pravilo, ki pravi:
» Ne stori drugemu tistega, česar ne želiš, da bi drugi storili tebi!«
Gre za osnovno pravilo, in če razumemo zapoved, ima lahko to neverjetne posledice in preostalih pravil sploh ne potrebujemo.

4 ZASEBNOST IN NADZOR ELEKTRONSKE POŠTE NA DELOVNEM MESTU

Elektronska pošta predstavlja najpogostejšo storitev v internetu in predstavlja osnovno orodje komuniciranja na daljavo. Povprečni uporabniki e-pošte v večini primerov želijo, da ostane njena vsebina nepovabljenim očem skrita in se na to tudi zanašajo. Z uporabo e-pošte pa je povezana vrsta tveganj s stališča zaupnosti in tajnosti, česar se pa običajni uporabnik v večini primerov ne zaveda (Makarovič in dr., 2001, stran 133,134).
Zasebnost ima dvojno funkcijo oziroma je povezana z nadzorom. Posamezniku omogoča, da drugim omeji dostop do sebe, po drugi strani pa mu onemogoča dostop v domeno zasebnega drugih posameznikov. Zasebnost torej pospešuje individualnost, povezovanje z drugimi in izbiro življenjskega sloga, po drugi strani pa povečuje in ponotranji družbeni nadzor (Kovačič v: Wagner DeCew, 1997, stran 68).
Zasebnost je torej pomembna, ker povečuje zmožnost posameznika, da avtonomno in neodvisno od okolice vzpostavlja odnose z drugim. Pri pravici biti puščen pri miru gre predvsem za razumevanje zasebnosti kot negativne pravice, zgodovinsko gledano naj bi posameznika pri miru pustila država. Iz tega razumevanja izvira angleška domneva o nedotakljivosti državljanovega doma oziroma nedotakljivosti stanovanja, iz katere se je pozneje razvila tudi zasebnost komunikacij in upravičeno pričakovanje zasebnosti (Kovačič, 2006, stran 42,43).
Nekateri primerjajo elektronsko pošto z dopisnico, kjer lahko skrbnik e-poštnih sistemov brez pravnih posledic pregleda vsebino. Vendar ni tako, saj je pošta shranjena v datotečni obliki, katere vsebina ni v hipu prepoznavna, torej bi moral skrbnik datoteko odpreti za jasnim namenov, kar pa pomeni poseg v zasebnost. Takšen poseg je podoben odprtju običajne pošte.
Pri uporabi e-pošte je neposredno in posredno vključenih več subjektov in vsak od njih ima s pravnega stališča in stališča varstva zasebnosti določeno vlogo:

- pošiljatelj sporočila,
- prejemnik sporočila,
- operater telekomunikacijskega omrežja,
- ponudnik internetnih storitev,
- upravljavec poštnega strežnika,
- proizvajalci programske opreme za vodenje strežnika e-pošte in strežnika ponudnika internetnih storitev ter programov, ki jih za pošiljanje e-pošte uporabljata pošiljatelj in naslovnik sporočila.

»V podjetjih je veliko e-pošte zasebne narave. Raziskovalni podjetji Mirapoint in Radicati Group sta objavili raziskavo, ki je pokazala, da je 23 odstotkov e-pošte v podjetjih zasebne narave in ni povezana z delom. Skupaj z neželeno pošto tako okrog polovica e-pošte na službenem naslovu ni povezane z delom. 8 odstotkov zaposlenih pogosto pošilja zasebno pošto preko službenih e-poštnih naslovov, 29 odstotkov uslužbencev to počne včasih, 35 odstotkov redko, 28 odstotkov pa je takšnih, ki tega ne počnejo. 72 odstotkov zaposlenih priznava, da preko službene e-pošte pošilja fotografije, kratke videoposnetke, smešnice in podobno, 12 odstotkov jih celo krši avtorske pravice, zaseda ogromno prostora na strežnikih in porablja veliko pasovne širine. 92 odstotkov anketiranih ima zasebni e-poštni naslov in kar 25 odstotkov od teh jih redno pošilja službeno pošto na svoj zasebni naslov, medtem ko jih 62 odstotkov službeno pošto pošilja z zasebnega e-poštnega naslova, s čimer je seveda ogrožena tudi varnost zaupnih podatkov podjetij« (Huber, 2006).

4.1 PRAVICA DO ZASEBNOSTI S PRAVNEGA VIDIKA

Pravica do zasebnosti ni trdno in univerzalno definirana, saj je dojemanje zasebnosti izrazito subjektivno. Poleg tega v pravu prevladuje pristop varstva in s tem definiranja pravice do zasebnosti prek poseganja vanjo (Kovačič v: Orehar-Ivanc, 2002, str. 82).
Eno najbolj pogostih in prav gotovo tudi eno težjih pravnih vprašanj je vprašanje vstopanja delodajalca v elektronsko pošto zaposlenih. Delodajalec želi vedeti, ali preko elektronske pošte morda ne odtekajo pomembni podatki, morda celo poslovne skrivnosti. V takšnem primeru moramo razumeti legitimen interes delodajalcev, da določena ravnanja na delovnem mestu prepovedujejo ter spoštovanje prepovedi nadzirajo, četudi s tem posegajo v komunikacijsko zasebnost zaposlenega. Po drugi strani pa seveda zaposleni želijo na delovnem mestu uživati varstvo pred posegi v zasebnost (Hajtnik in Stajič, 2009).

Pravico do zasebnosti in varstva osebnih podatkov pred neutemeljenimi ali neupravičenimi posegi države ali drugih pravnih in fizičnih oseb zagotavljajo pomembni mednarodni dokumenti:

- *Mednarodni pakt o državljanskih in političnih pravicah* (17. člen), ki govori o tem, da se nihče nima pravice vmešavati v zasebno življenje, v družino, stanovanje ali dopisovanje;
- *Evropska konvencija o človekovih pravicah* (8. člen), ki pravi, da ima vsak pravico do spoštovanja zasebnega in družinskega življenja, svojega doma in dopisovanja, kar velja tudi za javno oblast, razen v določenih primerih. (Makarovič in dr., 2001, stran 152).

4.2 PRAVNA UREDITEV ZASEBNOSTI V SLOVENIJI

»Tako imenovana komunikacijska zasebnost je po slovenski ustavi zelo strogo regulirana. V primeru suma odtekanja poslovnih skrivnosti ali morda celo industrijskega vohunjenja mora delodajalec najprej poklicati policijo, saj gre po našem kazenskem pravu za kaznivo dejanje. Policija je organ s preiskovalnimi pooblastili in ve, kako lahko zbere dokaze, ki bodo vzdržali v kazenskem postopku. Če delodajalec poskuša delati sam, bodo ti dokazi kmalu okuženi in odvetnik nasprotne stranke jih bo z lahkoto izločal iz postopka.« (Hajtnik in Stajič, 2009)

Slovenska ustava obravnava omenjene pravice v treh členih:

- 35. člen – varstvo pravic zasebnosti in osebnostnih pravic, ki pravi, da je vsakomur zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic;
- 37. člen – varstvo tajnosti pisem in drugih občil, ki pravi, da je poseg v komunikacijsko zasebnost dopusten samo, če so hkrati izpolnjeni trije pogoji: če takšen poseg določa zakon, če gre za odkrivanje kaznivih dejanj ali ogrožanje države in s predhodno pridobljeno odredbo sodišča;
- 38. člen – varstvo osebnih podatkov, ki pravi, da je zagotovljeno varstvo osebnih podatkov, prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov pa določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. (35., 37., 38. čl. Ustave RS)

Za poseg v zasebnost gre takrat, ko človek svojem odnosu upravičeno pričakuje, da ne bo neutemeljeno nadzorovan.
Torej se glede e-pošte soočajo različna mnenja:

- na eni strani uporabnikov, ki želijo in pričakujejo veliko mero zasebnosti pri svojem dopisovanju in
- države (tudi delodajalcev), ki želi nad e-pošto vzpostaviti čim učinkovitejši nadzor, saj v njej vidi povečano nevarnost razpečevanja otroške pornografije, sodelovanja kriminalističnih združb, terorističnih skupin ipd.

Po slovenski zakonodaji lahko v tajnost pisem in drugih občil posežeta le dva državna organa: Policija in Slovenska obveščevalno-varnostna agencija (SOVA) v primeru uvedbe in poteka kazenskega pregona zoper določeno osebo ali zaradi varnosti države (Makarovič in dr., 2001, str. 181).

4.3 PRAVNA UREDITEV V DRŽAVAH EU IN V AMERIKI

V Ameriki je pravica do zasebnosti posameznikov nasproti državi bistveno bolj zavarovana kot nasproti delodajalcem. Na delovnem mestu je zasebnost dojeta kot nekakšna boniteta, ki jo ima zaposleni. Delodajalci se v ZDA skušajo zaščititi pred izdajo poslovnih skrivnosti, prav tako pa se z nadzorom ščitijo pred odškodninskimi tožbami zaposlenih. Prodajalci nadzornih sistemov so zelo agresivni pri trženju tovrstne opreme, kar povečuje število nadzorov delodajalcev nad zaposlenimi (Kovačič, 2010, str. 56).

»Leta 1986 so v ZDA sprejeli Electronic Communication Privacy Act (ECPA; Electronic Communication Privacy Act of 1986, 18 U.S.C. (1986)), ki obravnava prisluškovanje elektronskim komunikacijam. ECPA v prvem poglavju, znanem tudi pod imenom Wiretap Act, prepoveduje prestrezanje elektronskih telekomunikacij, pri čemer je 'prestrezanje' definirano kot "zaznavanje izžarevanja [signala] (ang. aural) ali druga pridobitev vsebine žice oziroma elektronske ali ustne komunikacije, ki poteka s pomočjo uporabe kakršne koli elektronske, mehanične ali druge naprave". Bistveno pri tem je torej, da je prestrezanje definirano kot dejavnost, ki poteka hkrati s prenosom. Problem sodobne tehnologije – konkretno, nadzora elektronske pošte – pa je, da prestrezanje elektronske pošte ni nujno sočasno. Delodajalec namreč lahko dostopi do strežnika, v katerem je elektronsko sporočilo shranjeno, in s tem zaobide prepoved sočasnega prestrezanja. ECPA namreč v drugem poglavju, znanem pod imenom Stored Communications Act, ki prepoveduje dostop do shranjenih elektronskih sporočil brez soglasja nadzorovane osebe, iz prepovedi eksplicitno izključuje "osebe, ki zagotavljajo (ang. to provide) žično ali elektronsko komunikacijsko storitev". Tako so iz prepovedi ECPA izvzeti delodajalci, ki imajo v lasti komunikacijsko opremo podjetja (Sinrod v: Kovačič, 2010, str. 56).
»ECPA delodajalcem tudi sicer dovoljuje nadzor komunikacij (tudi telefonskih), a le, če zadevajo poslovanje podjetja« (Kovačič, 2010, str. 56).
Torej lahko rečemo, da imajo delodajalci v ZDA manj problemov, v primerih, kadar želijo preveriti elektronsko pošto zaposlenih v podjetju, saj jim to zakon omogoča. Lahko pa se odločijo za podpis soglasja za nadzor zaposlenega, preden ga zaposlijo in s tem rešijo marsikateri problem okoli nadzora elektronske pošte na službenem računalniku.
Nadzor komunikacij zaposlenih v ZDA precej razširjen, zakonodaja pa nadzor na delovnem mestu v veliki meri dovoljuje. Vendar je vprašanje, kako to vpliva na delo zaposlenih, njihovo lojalnost podjetju. Biti nenehno nadzorovan ne daje dobrega občutka. Postavlja se vprašanje, ali je to pravi način ugotavljanja, ali zaposleni izdajajo poslovne skrivnosti in poskrbijo za odtekanje pomembnih informacij. Verjetno obstaja še kakšen drug, bolj učinkovit in manj sporen način.

Tako je torej v Ameriki, povsem drugače pa so delavci zaščiteni v Evropi, pristop do zasebnosti je drugačen, bolj naklonjen zaposlenim. Zaposlenim priznava širok krog komunikacijske zasebnosti in prepoveduje pretirano omejevanje komunikacije z drugimi torej z zunanjim svetom. Zaposleni mora biti vsekakor vnaprej seznanjen s pravili delodajalca glede uporabe telefona, e-pošte in interneta. Delodajalec pa ga pri tem ne sme pretirano omejevati. Torej se mora zaposleni z morebitnim nadzorom strinjati, ta pa mora biti objektiven in opravičljiv. Takšno strinjanje zaposlenega mora potekati brez prisile, kljub delavčevi podrejenosti nasproti delodajalcu (po Kovačiču, 2010, str. 61).

4.3.1 PRAVICA DO ZASEBNOSTI E-POŠTE NA DELOVNEM MESTU V AVSTRIJI

Študije kažejo, da več kot 60 odstotkov vseh delavcev v Avstriji vsaj enkrat na dan uporabi internet v zasebne namene. Tudi v Avstriji se pojavlja vprašanje, ali je s strani delodajalca dovoljeno brati zasebno pošto zaposlenih. Praviloma se je potrebno pred zaposlitvijo dogovoriti, kakšne so meje uporabe interneta v zasebne namene. Delodajalec lahko načeloma prepove uporabo interneta v zasebne namene, lahko pa ga tudi dovoli. Da se izognemo nesporazumu, je potrebno v individualnih pogodbah oz. v poslovnih dogovorih, ki veljajo za vse zaposlene, točno opredeliti, kakšne pravice ima delavec pri uporabi interneta v zasebne namene.
V primeru popolne prepovedi uporabe interneta v zasebne namene in pošiljanje zasebne e-pošte iz službenega računalnika ima delodajalec pravico do nadzora in kontrole, vendar pri tem ne sme kršiti zasebnosti delavca. Delavca lahko opozori na kršitev dogovora, nikakor pa ne sme prebirati zasebnih oz. privatnih elektronskih sporočil. Tudi v primeru, kadar ima podjetje samo en skupen elektronski naslov in delodajalec pri pregledovanju e-pošte na tem naslovu naleti na zasebno pošto, te ne sme odpreti in prebrati. Čeprav je v določenih primerih iz samega naslova in pošiljatelja e-pošte težko ugotoviti, ali je pošta zasebne ali poslovne narave.
V primerih neupoštevanja pravil delodajalca glede uporabe interneta v zasebne namene ima delodajalec pravico delavca odpustiti. Prav tako delavec odgovarja za morebitno škodo, ki jo povzroči s prenosom in nalaganjem programov, iger, ki lahko škodijo računalniku. V več primerih je prišlo tudi do razrešitve delavca samo iz razloga nameščanja iger na službeni računalnik (Arbeiterkammer, 2011).

4.3.2 PRAVICA DO ZASEBNOSTI E-POŠTE NA DELOVNEM MESTU V NEMČIJI

Pravica do uporabe e-pošte in uporabe interneta v privatne namene na službenem računalniku lahko delodajalec omeji ali celo prepove z izdajo navodil. Če tega ne stori, ima zaposleni pravico do uporabo interneta v zasebne namene le v »zmernem« obsegu, če pri tem ni ogrožen interes delodajalca.
Pri vprašanju, ali sme delodajalec prebirati zasebno pošto, pa se je potrebno vprašati, kaj je zasebna in kaj službena elektronska pošta. Če delavec prejme ali pošlje e-pošto iz službenega računalnika in iz službenega elektronskega naslova, je lastnik in uporabnik elektronskega naslova delodajalec. V tem primeru bi imel delodajalec pravico prebirati takšno pošto.
Idealna rešitev je sklenitev sporazuma med delodajalcem in delojemalcem, ki natančno opredeli, kakšne so pravice obeh v primerih uporabe interneta in e-pošte v zasebne namene. V sporazumu naj bi bilo natančno zapisano, v kakšnem primeru lahko delodajalec preverja službeni računalnik zaposlenih in v kolikšnem obsegu. Takšen sporazum mora podpisati delavec in s tem tudi soglašati z morebitnim nadzorom uporabe interneta v zasebne namene in pregleda njegove zasebne e-pošte. Če zaposleni zavrne podpis takšnega sporazuma, mu lahko delodajalec popolnoma prepove uporabo interneta in pošiljanje privatne e-pošte.

Delodajalec ima pravico do naključnega preverjanja delavčeve uporabe interneta v zasebne namene, nedovoljen pa je sistematski in stalen nadzor službenih računalnikov zaposlenih in pomeni resen poseg v pravice zasebnosti posameznika.
V primeru odsotnosti zaposlenega zaradi dopusta, bolezni ..., ni dovoljen pregled in prebiranje e-pošte s strani sodelavcev brez predhodnega dovoljenja uporabnika službenega računalnika (Dr. Thomas Petri, 2011).

5 PRIMERI SODNE PRAKSE V ZDA IN EU

5.1 PRIMERI SODNE PRAKSE V ZDA

Shoars proti Epson America Inc. – Leta 1990 je zaposlena administratorka v podjetju Epson Alana Shoars ugotovila, da eden od tamkajšnjih direktorjev prebira elektronsko pošto zaposlenih v podjetju. Ker je temu nasprotovala, so jo odpustili. Zoper podjetje je vložila tožbo in tožbo izgubila. Podjetje je namreč trdilo, da gre za uporabo opreme in sistema za elektronsko pošto, ki je v njihovi lasti, zato je nadzor nad uporabo te upravičen. Sodišče v Kaliforniji je torej tožbo leta 1992 zavrnilo z obrazložitvijo, da ustava ZDA ščiti samo osebne informacije, ne pa tudi poslovnih komunikacij (po Kovačiču, 2010, str. 57).

Bonita P. Bourke, et. al. proti Nissan Motor Corporation – tudi v tem primeru je Kalifornijsko sodišče zavrnilo pritožbo , saj je zaposlena predhodno podpisala izjavo, da bo elektronsko pošto uporabljala le v službene namene, zato nadzor ne pomeni neupravičenega vdora v zasebnost zaposlene (Klemenčič v: Kovačič, 2010, str. 57).

Smyth proti Pillsbury – leta 1994 je zaposleni Michael Smith sodelavcu poslal elektronsko sporočilo, v katerem je zapisal, da so nadrejeni zahrbtne barabe. Tudi v tem podjetju so nadzirali e-pošto zaposlenih. Smytha so odpustili z obrazložitvijo, da je njegovo pisanje neprofesionalno in neustrezno. Smyth se je pritožil na sodišče, saj je bil prepričan, da mu je podjetje zagotovilo zasebnost komunikacij. Sodišče je primer zavrglo in ponovno dalo prav delodajalcu (po Kovačiču, 2010, str. 57).

U. S. A proti Councilman - Ponudnik brezplačne elektronske pošte je prestrezal elektronsko pošto svojih uporabnikov z namenom ugotoviti, katere knjige kupujejo uporabniki od konkurenčnih prodajalnah knjig. Podjetje se je namreč ukvarjalo s prodajo rabljenih knjig. S prebiranjem e-pošte je podjetje prišlo do pomembnih informacij o tem, kakšne knjige uporabniki kupujejo in po kakšnih cenah ter s tem pridobilo prednost pred drugimi ponudniki prodaje knjig. Zanimiv je ta primer predvsem zato, ker je sodišče leta 2004 razsodilo, da je takšno prestrezanje e-pošte zakonito in v skladu z zakonom (ECPA). Očitno je to tipičen primer nejasne zakonodaje. Odločitev sodišča je bila kasneje leta 2005 revidirana, sodišče v Massachusettsu je odločilo, da je takšen nadzor elektronske pošte nezakonit (po Kovačiču, 2010, str. 57).

Schill proti Wisconsin Rapids School District – 16. julija 2010 je Vrhovno sodišče ameriške zvezne države odločilo, da je elektronska pošta, ki jo vladni uslužbenci pošljejo z računalnika na delovnem mestu, lahko zasebne narave. Državljan Don Bubolz je namreč zahteval na podlagi zakonodaje o dostopu informacij javnega značaja izpis elektronske pošte petih učiteljev. Šola je želela ugoditi, saj so bila sporočila poslana iz službenega računalnika. Učitelji so se na to odločitev šole pritožili. Na prvi stopnji so pritožbo izgubili, Vrhovno sodišče pa je presodilo, da vsebina zasebnih sporočil vladnih uslužbencev ni stvar javnosti (Matej Kovačič, 2010).

5.2 PRIMERI SODNE PRAKSE V EVROPI

Halford proti Združenemu kraljestvu - uslužbenka policije ga. Halford je leta 1997 sprožila postopek proti svojemu delodajalcu zaradi diskriminacije na delovnem mestu. Delodajalec je nato nadzoroval telefonske klice samo zato, da bi zbral gradivo za postopek na sodišču. Evropsko sodišče za človekove pravice je je presodilo, da je delodajalec kršil

8. čl. Evropske konvencije o človekovih pravicah in v razsodbi zapisalo, da je na delovnem mestu upravičeno pričakovati zasebnost (po Kovačiču, 2010, str. 59).

8. čl. Evropske konvencije govori o pravici do spoštovanja zasebnega in družinskega življenja:
»Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi« (Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin, 8. čl).

Copland proti Združenemu kraljestvu - nadrejeni je pregledoval izpiske telefonskih številk in sezname spletnih strani ter elektronsko pošto zaposlene Lynette Copland. Želel je ugotoviti, ali zaposlena uporablja službena sredstva v zasebne namene. Lynette Copland se je pritožila na Evropsko sodišče za človekove pravice, ki je leta 2007 prav tako presodilo, da gre v tem primeru za kršenje 8.čl. Evropske konvencije o človekovih pravicah, torej za neupravičeno poseganje v njeno zasebnost (po Kovačiču, 2010, str. 59). *»Evropsko sodišče za človekove pravice* je v primeru presodilo, da varstvo zasebnosti velja tako za telefonske komunikacije, kot tudi za elektronsko pošto in uporabo interneta, in da je s stališča varstva zasebnosti irelevantno, ali gre za zasebno ali za službeno komunikacijsko sredstvo. Prav tako so presodili, da kršitev predstavlja že samo zbiranje in obdelava prometnih podatkov in s tem potrdili, da so prometni podatki integralni element komunikacij. Kršitev zasebnosti torej ni "le" vpogled v vsebino komunikacij, pač pa tudi vpogled v prometne podatke. Nadalje so v razsodbi zapisali, da je s stališča varstva zasebnosti irelevantno, ali so bili podatki "zgolj" zbrani ali pa so bili tudi razkriti tretjim osebam oziroma uporabljeni proti pritožnici. S tem so se postavili na stališče, da je sporen že sam akt posega, ne pa šele morebitni kasnejši pregled oziroma obdelava prestreženih podatkov in komunikacij s strani tretje osebe. Pomemben element sodbe je bilo tudi dejstvo, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira elektronsko pošto zaposlenih, in je zato po mnenju sodišča lahko upravičeno pričakovala zasebnost na svojih službenih komunikacijskih sredstvih«
(Kovačič, 2010, str. 60).

Odločitev Kasacijskega sodišče v primeru Society Nikon France – delodajalec je preiskal računalnik zaposlenega in ugotovil, da je zaposleni uporabljal računalnik za neslužbene namene in ga odpustil. Kasacijsko sodišče pa je odločilo, da ima zaposleni pravico do zasebnosti in tajnosti komunikacij na delovnem mestu (po Kovačiču, 2010, str. 59).
V sodbi so zapisali:

" … delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah … To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene … Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave … Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti" (Klemenčič v : Kovačič 2010).
Zelo pomembna odločitev, ki zagotavlja zaposlenemu pravico do uporabe e-pošte v neslužbene namene tudi v primeru, kadar ga delodajalec predhodno opozori, da to ni dovoljeno.

Niemietz proti Nemčiji – v tem primeru je Evropsko sodišče za človekove pravice odločilo, da ima zaposleni pravico do vzpostavljanja osebnih in socialnih stikov, kar je tudi stališče Priporočila Sveta Evrope, št. R(89) 2 (po Kovačiču, 2010, str. 61).

Okrožno sodišče Wesel - Zanimiva je odločitev tega sodišča, ki je odločilo, da je delodajalec vsekakor upravičen do takojšne prekinitve oz. odpustitve delavca, če rok njegove zasebne uporabe interneta na delovnem mestu presega 100 ur letno. Odpustitev pa tvega tudi vsakdo, ki zaradi zasebne uporabe interneta zanemarja svoje delo (123recht.net, 2001).

6 NADZOR ELEKTRONSKE POŠTE NA SLUŽBENEM RAČUNALNIKU

Vprašanje zasebnosti e-pošte v odnosu delodajalec-delojemalec je še posebej občutljivo, ker še vedno ni znano, kakšno stopnjo zasebnosti lahko zaposleni na delovnem mestu pričakuje. Praviloma je računalnik, ki ga zaposleni uporablja, v lasti delodajalca, prav tako je elektronski naslov delojemalcu dodeljen le za opravljanje službenih zadev.
Prisoten je namreč:

- **interes delodajalca**, ki ima pravico do oblasti nad opremo in predvsem pravico, da nadzira, v kakšne namene je ta oprema uporabljena. Ima tudi interes, da odkriva, preprečuje in preganja disciplinske prekrške zaposlenih, predvsem zlorabo službene opreme v zasebne namene ali druge sporne namene;
- **interes zaposlenih**, ki pričakuje določeno stopnjo zasebnosti, delno samostojnost in zaupnost tudi na delovnem mestu;
- **interes tretjih oseb**, ki delavcu pošiljajo e-sporočila na službeni e-naslov, pri čemer ni nujno, da so seznanjeni s tem, da je e-naslov služben *(Makarovič in dr., 2001, stran* 187,188).

Glede na to, da komuniciranje prek e-pošte nedvomno spada pod ustavno zavarovano pravico, je nadzor tovrstnega komuniciranja s strani delodajalca dopusten zgolj ob izrecni zakonski podlagi, ob vednosti in vnaprejšnjem soglasju delavca.
Zato je izrednega pomena, da podjetje oziroma ustanova sprejme interna pravila nadzora, ki morajo vnaprej določiti, kdo, kdaj, kako in pod kakšnimi pogoji lahko spremlja delavčevo e-pošto, zaposleni pa morajo biti s temi pravili vnaprej seznanjeni.

6.1 ODLOČBE IN MNENJA INFORMACIJSKEGA POOBLAŠČENCA

Informacijski pooblaščenec je samostojen in neodvisen državni organ. Ustanovljen je bil 1. 9. 2003 z Zakonom o dostopu do informacij javnega značaja - ZDIJZ (Ur. l. RS, št. 24/2003). Pristojnosti Informacijskega pooblaščenca na podlagi Zakona o varstvu osebnih podatkov (ZVOP-1) je več, med njimi pa tudi naslednja:

- daje in objavlja neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojih poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;
- pripravlja, daje in objavlja neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju;
- na spletni strani in na drug ustrezen način objavlja predhodna mnenja o usklajenosti predlogov zakonov in drugih predpisov z zakonom in drugimi predpisi s področja varstva osebnih podatkov ter zahtev za oceno ustavnosti predpisov, izdaja notranje glasilo ter strokovno literaturo, objavlja odločbe in sklepe sodišč, ki se nanašajo na varstvo osebnih podatkov ter neobvezna mnenja, pojasnila, stališča in priporočila glede varstva osebnih podatkov na posameznem področju (Informacijski pooblaščenec, 2011).

Z namenom informiranja javnosti je Informacijski pooblaščenec izdal več priročnikov, ki so dosegljivi na njihovi spletni strani. Med njimi lahko zasledimo priročnik z naslovom: Zlata pravila zasebnosti na delovnem mestu. Omenja 5 zlatih pravil zasebnosti. Drugo pravilo po vrsti je pravilo, ki govori, da ima delavec pravico do zasebnosti na delovnem mestu, sorazmerno z zakonitim ciljem, ki mu delodajalec sledi. Med 10 najpomembnejših kršitev zasebnosti na delovnem mestu je prav na prvem mestu - vpogled v elektronsko pošto zaposlenih in nadzor nad uporabo interneta.

Na spletni strani Informacijskega pooblaščenca v rubriki Odločbe in mnenja informacijskega pooblaščenca zasledimo kar nekaj vprašanj v zvezi z zasebnostjo elektronske pošte na delovnem mestu. Nekaj najbolj zanimivih vprašanj in odgovorov:

1. *Vprašanje: Informacijski pooblaščenec je 9. 3. 2010 prejel vaše elektronsko sporočilo, v katerem navajate, da imate v pogodbi o zaposlitvi določilo, da lahko delodajalec pogleduje tudi v vašo elektronsko pošto. Zanima vas, ali je takšno določilo skladno z vidika Zakona o varstvu osebnih podatkov.*

Odgovor pooblaščenca: Po mnenju Pooblaščenca je treba izhajati iz dejstva, da lahko zaposleni na naslov delodajalca prejme tudi povsem zasebno pisanje – tako po navadni kot tudi po elektronski pošti. Za zasebno pisanje, ki pride potom navadne pošte, štejemo pošiljke, ki so naslovljene na zaposlenega (njegovo osebno ime), ne na delodajalca in poslane na naslov delodajalca. Pošiljk, ki prispejo v elektronski predal, na ta način ni mogoče ločevati, saj so vse naslovljene na elektronski naslov delavca, njihova vsebina pa je lahko službena ali zasebna. To dejstvo je dolžan spoštovati tudi delodajalec. Tako določilo v pogodbi o zaposlitvi, da delodajalec lahko pregleduje vašo elektronsko pošto, ne sme pomeniti generalnega pooblastila za delodajalca, da lahko kadarkoli in brez vaše vednosti pregleduje vašo elektronsko pošto. Določilo lahko pomeni le seznanitev delavca z možnostjo pregleda elektronske pošte v primerih vnaprej določenih s strani delodajalca (za katere namene, ob katerih okoliščinah …) – v internem aktu. Seveda morajo biti takšni razlogi taksativno navedeni in izjemni.

2. *Vprašanje: Prejeli smo vašo elektronsko pošto, v kateri navajate, da si dopisujete z neko osebo v drugem podjetju preko službene elektronske pošte in dnevno prejmete in pošljete v povprečju 3 zasebna sporočila. Od administratorja nasprotnega podjetja naj bi zdaj prejeli obvestilo, da je zaradi prevelike količine neposlovne pošte vaš e-naslov blokiran. Menite, da so v »nasprotnem« podjetju pregledovali vašo elektronsko pošto in vas zanima, kakšne so vaše pravice.*

Odgovor pooblaščenca: Če menite, da so v »nasprotni« družbi prebirali vašo pošto, so lahko osebe, ki so prebirale elektronska sporočila, posegle tako v pravico do zasebnosti delavke, ki je zaposlena v »nasprotni« družbi, kakor tudi v vašo pravico do zasebnosti, torej pravico do varstva tajnosti pisem in drugih občil. Če torej menite, da vam je bila kršena pravica do zasebnosti (torej prebiranje vsebine elektronske pošte), lahko zoper »nasprotno« družbo vložite odškodninsko tožbo. Enako lahko stori delavka, ki je zaposlena v tej družbi. Če pa menite, da so vam osebe v »nasprotni« družbi pogledale zgolj v prometne podatke (torej v podatke kot so podatki o pošiljatelju, naslovniku ipd.), lahko na Informacijskega pooblaščenca naslovite prijavo.

3. *Vprašanje: Ali se lahko naslov elektronske pošte, ki se glasi na vaše ime, še vedno uporablja v podjetju, kjer ste bili zaposleni do odpovedi pogodbe o zaposlitvi iz poslovnih razlogov?*

Odgovor pooblaščenca: S prenehanjem vašega delovnega razmerja pri tem delodajalcu je torej prenehala tudi pravna podlaga za obstoj vašega elektronskega naslova, ko in če ta predstavlja osebni podatek. Takšno mnenje je Pooblaščenec sprejel tudi ob upoštevanju 18. člena ZVOP-1, ki v 1. odst. določa, da morajo biti osebni podatki, ki se obdelujejo, točni in ažurni. Če je torej v vašem nekdanjem elektronskem naslovu izpisano tudi ime podjetja, takšen elektronski naslov ni več ažuren, niti točen, saj niste več zaposleni pri nekdanjem delodajalcu. Pooblaščenec meni, da vaš nekdanji delodajalec obdeluje vaš elektronski naslov brez pravne podlage. Ob zaključku delovnega razmerja bi namreč moral

elektronski naslov z zgoraj navedenimi atributi, ukiniti. Če bi vendarle nanj še vedno lahko dobival pomembno pošto, bi moral prihodnje pošiljanje urediti na način, da se vaš elektronski naslov ne bi več neposredno obdeloval, npr. z avtomatskim odzivnikom (povratno elektronsko pošto), ki bi pošiljateljem sporočala, da ta elektronski naslov ne obstaja več, zraven pa bi npr. pripisal, na kateri naslov se lahko pošiljatelj obrne. Glede na navedeno vam 32. člen ZVOP-1 omogoča, da od podjetja, kjer ste bili včasih zaposleni, zahtevate izbris osebnega podatka, t.j. vašega nekdanjega elektronskega naslova, če je ta seveda v takšni obliki, kot je opisano zgoraj (Informacijski pooblaščenec, 2011).

7 PRAVILNIK O UPORABI ELEKTRONSKE POŠTE NA DELOVNEM MESTU

Ker še vedno najpogosteje vstopamo do interneta prek službenih računalnikov in službenih povezav, je pomembno, da se vse bolj zavedamo, še zlasti ob vstopu v EU, osnovnega pravila, naj bi se e-komunikacija prek službenega računalnika s službenim e-naslovom nanašala predvsem na poslovno e-komunikacijo določenega podjetja.
Da bi v podjetju preprečili preveliko zmanjšanje storilnosti zaposlenih, ki se vse preveč ukvarjajo s pošiljanjem zasebne pošte in razpošiljanjem zabavnih datotek med delovnim časom, je koristno, da podjetja sestavijo pravilnik o uporabi e-pošte, ki lahko obvaruje tudi pred marsikatero težavo zaradi nepravilne uporabe e-pošte.
V pravilniku naj se točno zapiše, kako in kdaj morajo zaposleni odgovoriti na sporočila strank in partnerjev, kakšne nevarnosti pretijo zaradi uporabe e-pošte in kako se jim izogniti, katere vsebine se ne smejo razpošiljati, kako se bodo obravnavale zaupne vsebine, v kolikšni meri je dovoljena uporaba e-pošte v osebne namene in podobno. Vsako podjetje bi moralo seznaniti vse zaposlene, ki uporabljajo e-pošto z bontonom uporabe e-pošte, saj bo lahko le tako doseglo ustrezno raven komunikacije s poslovnimi partnerji in strankami, kar bo seveda tudi vplivalo na ugled podjetja v javnosti (Radoš, 2005).

Ministrstvo za javno upravo je na podlagi 80. čl. Uredbe o upravnem poslovanju 2.11.2010 izdalo Priporočila informacijske varnostne politike javne uprave. Priporočila so dolžni upoštevati vsi organi javne uprave, kar pa ne velja za celoten javni sektor.
»Namen IVPJU je postaviti osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi. Izvajanje te politike je pomembno za zagotavljanje informacijske varnosti.« (MJU, 2010).
Priporočila vsebujejo tudi napotke v zvezi z uporabo elektronske pošte na delovnem mestu. Čeprav prav vsi členi vsebujejo pomembna navodila za zaposlene v javni upravi, bom navedla le nekaj najpomembnejših s področja varnosti in zasebnosti in uporabe elektronske pošte v zasebne namene.

Uporaba elektronske pošte

60. člen

Zaposleni v javni upravi kot orodje za komunikacijo z državljani, strankami, zaposlenimi in zunanjimi izvajalci uporabljajo tudi elektronsko pošto. Pri tem se morajo držati ne le etičnih in moralnih norm, temveč tudi bontona. Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje organa, v katerem je pošiljatelj zaposlen.

61. člen

Sistem elektronske pošte se praviloma uporablja samo v službene namene. Uporaba v druge namene je dopustna le izjemoma, če ne moti delovnega procesa in varnosti (zaupnost, celovitost in razpoložljivost) informacijskega sistema.

64. člen

Uporabniki morajo biti previdni pri odpiranju pošte s priponkami neznanih pošiljateljev. Če sumijo, da gre za nezaželeno pošto, ki bi bila lahko škodljiva, naj je ne odpirajo, temveč naj o tem obvestijo skrbnika poštnega sistema na naslov cert@gov.si ali po telefonu (EVT) št. (01) 478 8778 ali pa naj obvestijo službo za pomoč uporabnikom pri organu javne uprave.

65. člen

Uporabniki nikakor ne smejo pošiljati občutljivih podatkov ali gesel po elektronski pošti razen v ustrezno akreditiranih sistemih.

67. člen

Vse pravice na sistemu elektronske pošte in vseh elektronskih sporočilih, ki niso zasebna, pripadajo organu javne uprave. Uporabniki se morajo zavedati, da se elektronska sporočila v sistemu elektronske pošte varnostno shranjujejo in bodo ostala shranjena tudi, če jih izbrišejo iz svojega elektronskega poštnega predala.

68. člen

Uporabnik ne sme uporabljati elektronskega poštnega naslova, ki je bil dodeljen drugemu uporabniku.

69. člen

V primeru ukinitve elektronskega poštnega naslova se pošiljateljem elektronskih sporočil na ukinjeni elektronski poštni naslov, pošlje sporočilo o nedostopnosti elektronskega poštnega naslova in po možnosti obvestilo o nadomestnem naslovu. Sprejemanje elektronskih sporočil na ukinjeni elektronski poštni naslov se onemogoči. Vsebina poštnega predala do ukinitve elektronskega poštnega naslova se arhivira skladno z relevantno zakonodajo. Preusmeritev elektronske pošte v drug predal uporabnika ni dovoljena.

70. člen

Elektronska sporočila, ki jih sprejme uporabnik na svoj elektronski poštni naslov, sme odpirati samo ta uporabnik, ali s strani uporabnika pooblaščena oseba, drug uporabnik pa samo na podlagi odredbe pristojnega državnega organa ali v izjemnih primerih posebnega pisnega pooblastila predstojnika organa javne uprave. Pri tem se morajo upoštevati določila relevantne zakonodaje in vsa pravila, ki v takšnih primerih veljajo za ravnanje z gesli.

74. člen

Če uporabnik prejme elektronsko sporočilo, ki ni namenjeno njemu, vsebine tega sporočila ne sme nemudoma izbrisati ali kako drugače uničiti. Pred uničenjem ga lahko pošlje pravemu naslovniku, če je iz sporočila nedvoumno razvidna njegova identiteta.

75. člen

Čeprav upravitelj zagotavlja zaupnost, se mora vsak zaposleni zavedati, da elektronsko pošto lahko, odvisno od tehnologije, prestrežejo in obdelujejo nepooblaščene osebe.

82. člen

Ob sumu storitve kaznivega dejanja z uporabo elektronskih sporočil, se opravijo postopki skladno z relevantno zakonodajo po odredbi pristojnega državnega organa. Pregledovanje elektronskih sporočil upravljavcev elektronske pošte iz radovednosti ali po nalogu nepooblaščenih posameznikov ni dovoljeno. (MJU, 2010)

Navodila zaposlenim v javni upravi so natančna in se dotikajo prav vseh področij. Zanimivo bi bilo vedeti, v kolikšni meri so zaposleni seznanjeni s temi priporočili. Še vedno pa veljajo le za zaposlene v javni upravi in upravičeno se vprašamo, zakaj ne za celoten javni sektor.

8 ANALIZA POZNAVANJA PRAVIC DO ZASEBNOSTI ZAPOSLENIH V JAVNI UPRAVI S POMOČJO ANKETNEGA VPRAŠALNIKA

8.1 INFORMACIJSKA ZASEBNOST ZAPOSLENIH V JAVNI UPRAVI

Informacijska zasebnost zaposlenih v javni upravi je precej natančno zapisana v Uredbi o upravnem poslovanju v 100. členu, kjer je zapisano, da pošto, ki jo prejme javni uslužbenec na svoj uradni elektronski naslov, odpira ta javni uslužbenec. Drug javni uslužbenec tega organa lahko odpira elektronsko sporočilo, iz katerega je razvidno, da ne gre za osebno sporočilo naslovniku samo na podlagi posebnega pisnega pooblastila predstojnika ali vodje organizacijske enote (100. čl. Uredbe o upravnem poslovanju).
Mnogokrat je že pri pregledovanju seznama e-pošte možno priti do nedovoljenih osebnih podatkov. Pomembno je, da delodajalec že v naprej pripravi ustrezna pooblastila oziroma privolitve v primeru, da je zaposleni odsoten, je pa nujno, da nekdo pregleda prejeto e-pošto. Brez takšne privolitve namreč ni dovoljeno pregledovanje pošte sodelavca, razen v primerih, ki jih navaja informacijska pooblaščenka: če zaposleni umre ali nenadoma odpove delovno razmerje. V vseh drugih primerih je za takšne posege potrebna odredba sodišča.
V 71. čl. Uredbe o upravnem poslovanju je prav tako zapisano, da imajo zaposleni v javnem sektorju pravico do uporabe interneta v zasebne namene, vendar uporaba ne sme povzročati informacijskih tveganj in je dovoljena samo v zmernem obsegu, ki ne ovira ali ogroža normalnega delovnega procesa.
Slovenija je razmeroma dobro razvita informacijska družba. Predvsem na področju javne uprave je porast uporabe interneta, elektronske pošte in drugih možnosti elektronskega poslovanja in komuniciranja zelo velika. Pojavi pa se seveda dilema, ali imajo zaposleni dovolj znanja in spretnosti, ki sta nujno potrebni pri tovrstnem komuniciranju ali je njihovo vedenje primerno, kakšno je njihovo jezikovno znanje, kako so seznanjeni z nevarnostmi, z zasebnostjo…
Odločila sem se, da s pomočjo vprašalnika poiščem odgovore na ta vprašanja in ugotovim, kako dejansko poteka poslovna komunikacija na področju javnega sektorja.

8.2 REZULTATI IN ANALIZA ANKETE

8.2.1 METODOLOGIJA RAZISKAVE

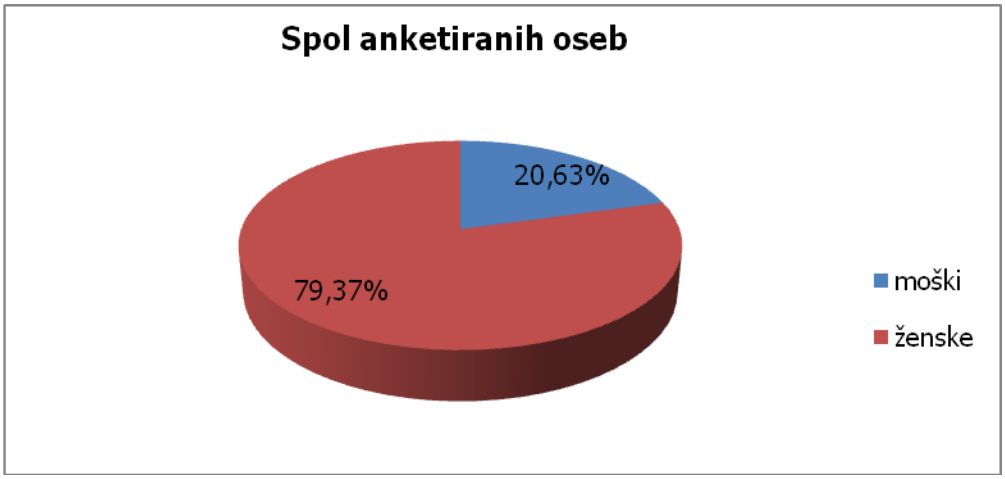
Naslov anketnega vprašalnika je bil VARNOST IN ZASEBNOST ELEKTRONSKIH SPOROČIL NA DELOVNEM MESTU. Pri tem sem uporabila deskriptivno metodo raziskovanja. Anketni vprašalnik je bil anonimen, vseboval je 22 vprašanj. Uporabila sem kvantitativno tehniko zbiranja podatkov. Vsa vprašanja so bila zaprtega tipa, to pomeni, da so bili možni odgovori že dani, anketiranec se je moral odločiti za enega ali več izmed njih.
Odločila sem se za individualno obliko anketiranja. Raziskava je potekala na konkretnem vzorcu populacije. Izvedbo ankete sem omejila na zaposlene v javnem sektorju, in sicer v več različnih delovnih organizacijah javnega sektorja: v socialnem varstvu, zdravstvu, carini, šolstvu in v občinski upravi. Cilj ankete je bil ugotoviti, kakšno je obstoječe stanje v vrstah javnih uslužbencev, v kolikšni meri so seznanjeni z zasebnostjo elektronske pošte, kakšna je stopnja varnosti njihovih sporočil, kako pogosto uporabljajo ta medij, kakšna je urejenost na področju pravil uporabe itd.

Anketne odgovore sem preračunala v odstotke in na osnovi poznavanja stanja, opazovanja in stališč prišla do samostojnih sklepov. Namen empiričnega raziskovanja je bilo zbiranje, obdelava podatkov in na koncu interpretacija dobljenih rezultatov.

8.2.2 REZULTATI ANKETE

Glede na dejstvo, da je trenutno v Sloveniji zaposlenih približno 160.000 javnih uslužbencev, rezultatov ankete ne moremo posploševati na celoten javni sektor, saj je anketirani vzorec premajhen, pa vendarle sem mnenja, da izraža trenutno realno stanje.
Na vprašalnik je odgovorilo 63 anketirancev iz različnih vrst javnega sektorja. Vsi anketiranci so odgovorili na vseh 22 vprašanj v anketi. Največji delež anketiranih oseb je zaposlenih v socialnem varstvu, zdravstvu in carinski upravi, manjši delež pa v šolstvu in občinski upravi. 50 anketiranih oseb je bilo predstavnikov ženskega spola in 13 moških, kar pomeni, da je pri anketi sodelovalo 79,37 % žensk in 20,63 % moških.

Graf 1: Delež moških in žensk vseh anketiranih oseb



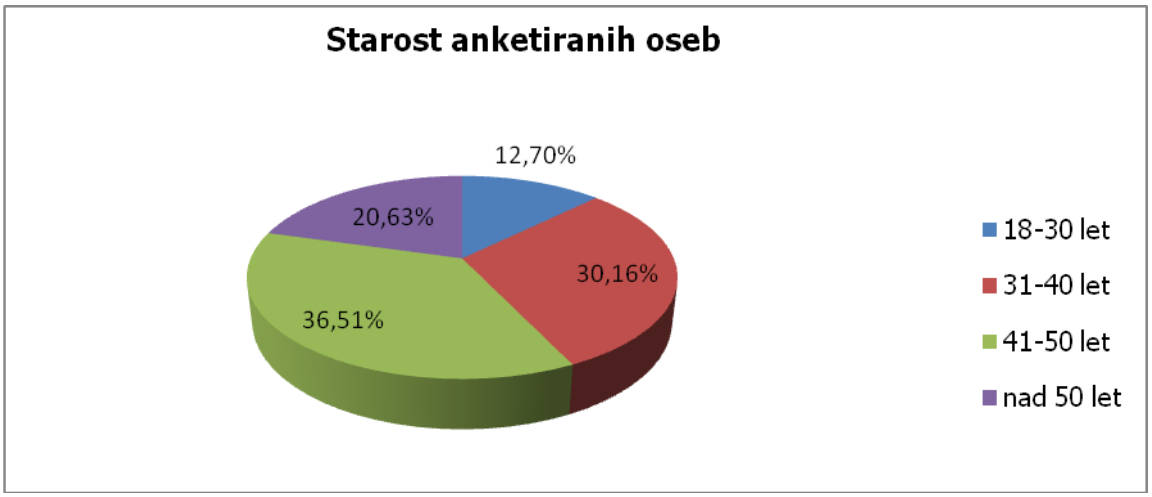
Vir: lasten

Povprečna starost anketiranih je bila 42,55 let. Rezultati so pokazali, da je bila starost anketiranih naslednja:

- od 18–30 let: 8 oseb
- od 31–40 let: 19 oseb
- od 41–50 let: 23 oseb
- nad 50 let: 13 oseb

Posamezne odgovore na vprašanja sem preverila tudi glede na starostne skupine anketiranih oseb. Večjih odstopanj nisem zasledila. Pri odgovorih, kjer pa so se odstopanja pojavila, sem to posebej zapisala. Najmanj odstopanj glede na odgovore ne glede na starost anketiranih oseb, sem zasledila pri starostni skupini od 41-50 oseb, največ odstopanj pa pri starostni skupini od 18-30 let.

Graf 2: Starost anketiranih oseb



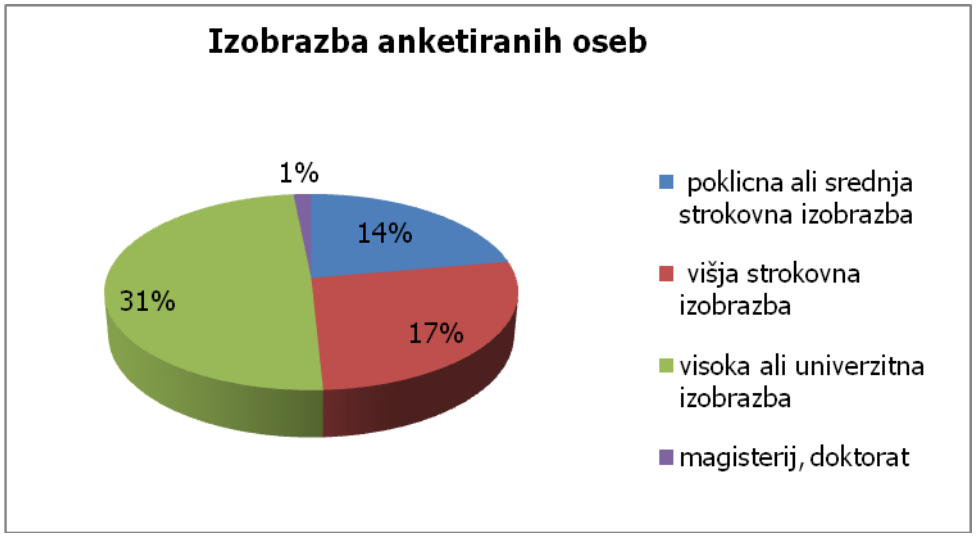
Vir: lasten

Vprašanje št. 1:

Izobrazba anketiranih oseb

Pri prvem vprašanju so anketirane osebe navedle svojo dokončano stopnjo izobrazbe. Rezultati so sledeči:

Graf 3: Izobrazba anketiranih oseb



Vir: lasten

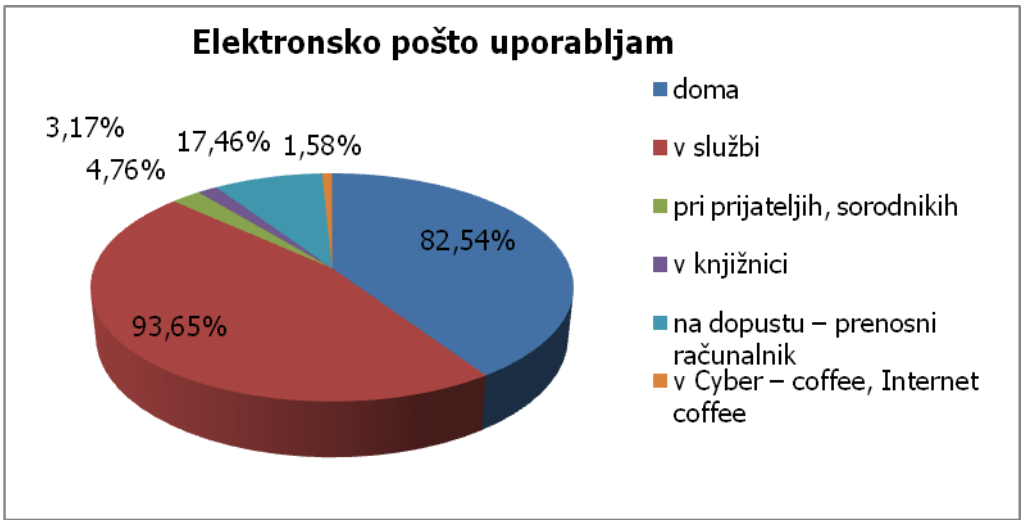
Skoraj polovica anketiranih oseb ima dokončano visoko ali univerzitetno izobrazbo, kar pomeni, da je izobrazbeni nivo anketirancev dokaj visok in ustreza zaposlitveni strukturi zaposlenih v javnem sektorju.

Vprašanje št. 2:

Elektronsko pošto uporabljam:

Elektronsko pošto imamo priložnost možnost uporabljati na več različnih mestih. Namen prvega vprašanja je bil ugotoviti, kakšne so navade anketiranih oseb pri uporabi elektronske pošte. Rezultati so povsem realni, največji odstotek je tistih, ki uporabljajo elektronsko pošto v službi kar 93,65 %, 82,54 % anketiranih jo uporablja tudi doma, razmeroma nizek odstotek pa je tistih, ki uporabljajo elektronsko pošto tudi v knjižnici in Cyber - coffee, kar je dokaj logično, saj je slednjih v Sloveniji še razmeroma malo v primerjavi s tujino.

Graf 4: Uporaba elektronske pošte



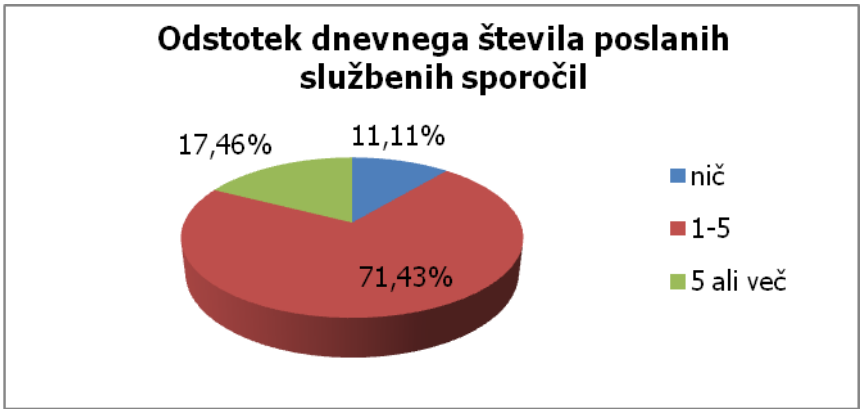
Vir: lasten

Vprašanje št. 3:

Koliko službenih elektronskih sporočil pošljete v povprečju na dan?

Kar 71,43 % vseh anketiranih oseb pošlje v povprečju na dan 1 – 5 sporočil in 17,46 % takšnih, ki dnevno pošljejo 5 ali več elektronskih sporočil. Zanimivo pri tem vprašanju je to, da v današnjem času še vedno 11,11 % vprašanih v službi ne komunicira s pomočjo e-pošte.

Graf 5: Odstotek dnevnega števila poslanih službenih sporočil



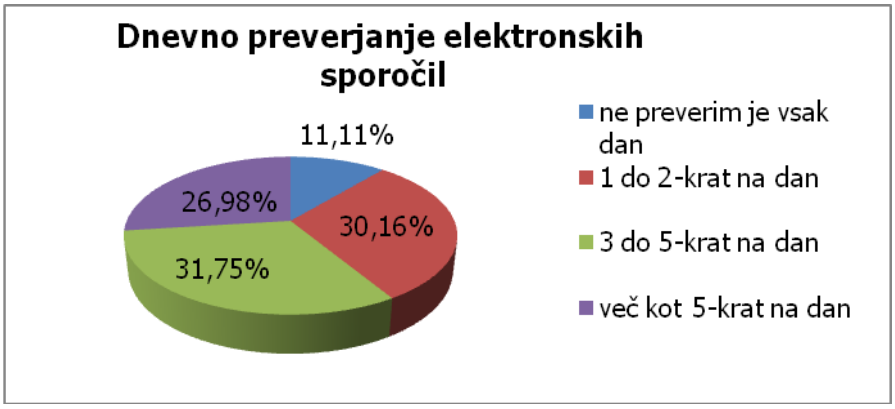
Vir: lasten

Vprašanje št. 4:

Kako pogosto v povprečju na dan preverite elektronsko pošto na vašem službenem računalniku?

Ljudje se vedno pogosteje obračajo na zaposlene v javnem sektorju s vprašanji tudi preko e-pošte. Zato je pomembno, da vsaj enkrat na dan preverimo naš poštni predal in ljudem ponudimo odgovor na njihova vprašanja. Zato se mi zdi, da je odstotek tistih, ki tega ne počno vsak dan dokaj visok (11,11 %). V starosti skupini od 31-40 let ni nikogar, ki ne bi dnevno preveril svoje elektronske pošte in visok odstotek (47 %) takšnih, ki jo preverijo kar 3–5 krat na dan.

Graf 6: Dnevno preverjanje elektronskih sporočil



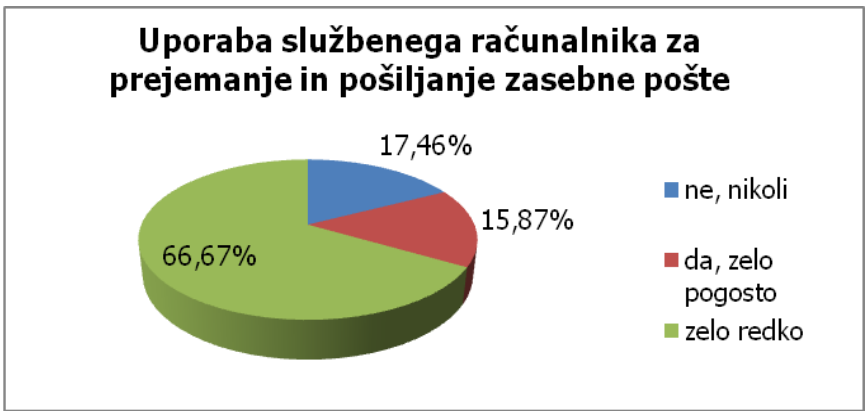
Vir: lasten

Vprašanje št. 5:

Ali uporabljate službeni računalnik tudi za prejemanje in pošiljanje zasebne pošte?

Čeprav je trend pošiljanja zasebne pošte iz službenega računalnika vedno večji, presenetljivih 66,67 % anketiranih oseb počne to zelo redko, 17,46 % ne počne tega nikoli, kar je skoraj malo verjetno. Pri analizi odgovorov glede na starost, sem ugotovila, da med anketiranci nad 50 let ni bilo nikogar, ki bi službeni računalnik zelo pogosto uporabljal tudi v zasebne namene.

Graf 7: Pošiljanje zasebne pošte iz službenega računalnika



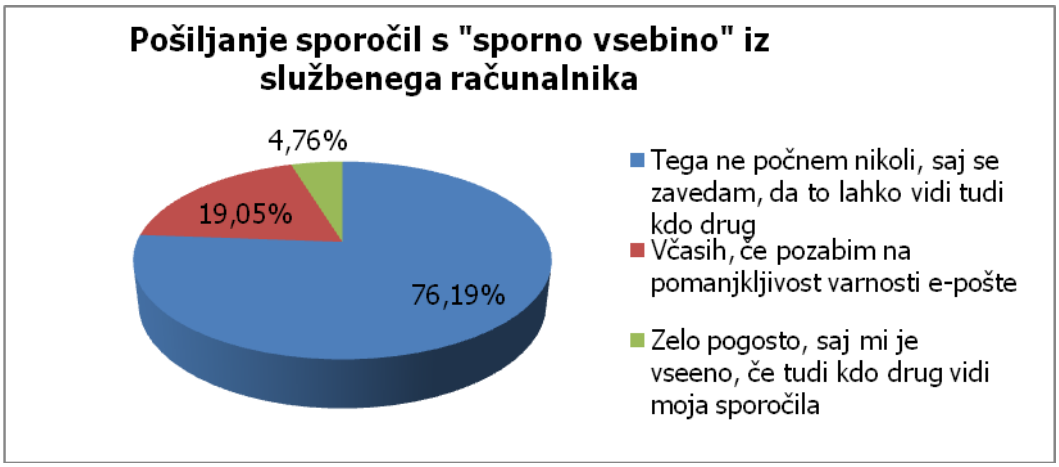
Vir: lasten

Vprašanje št. 6:

Pri pošiljanju privatnih sporočil iz službenega računalnika včasih pošljem tudi takšna s »sporno vsebino«

Verjetno je že vsak od nas prejel na službeni računalnik tudi takšno elektronsko sporočilo, katerega vsebina je nemoralna, »sporna«. Vprašanje je, če se zaposleni zavedajo, da takšna sporočila lahko vidijo tudi drugi. Anketa je pokazala, da velik odstotek zaposlenih v javnem sektorju tega ne počne, saj se zavedajo pomanjkljivosti e-pošte. Le 4,76 % je takšnih, ki to počnejo pogosto in jim je vseeno, če tudi kdo drug vidi ta sporočila.

Graf 8: Pošiljanje pošte s »sporno vsebino«



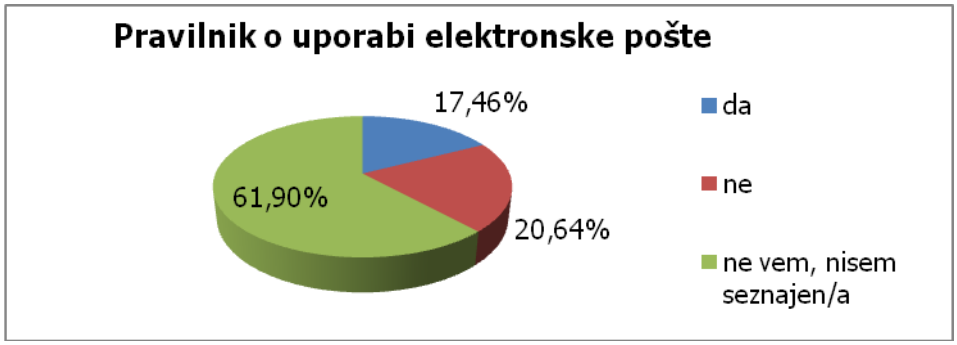
Vir: lasten

Vprašanje št. 7:

V službi imamo sprejet Pravilnik o uporabi elektronske pošte na delovnem mestu.

Glede na dejstvo, da je elektronska pošta postala zelo pogost medij pri poslovnem komuniciranju, je zelo pomembno, da zaposleni poznajo pravila takšnega komuniciranja. Iz rezultatov ankete je razvidno, da so le redki primeri (17,46 %), kjer je bil že sprejet Pravilnik o uporabi elektronske pošte. Kar 20,64 % je primerov, kjer pravilnik zaposlenim še ni na voljo in zelo visok odstotek (61,90 %) je takšnih, ki pravzaprav niso seznanjeni oziroma ne vedo, ali imajo sprejet takšen pravilnik.

Graf 9: Pravilnik o uporabi elektronske pošte

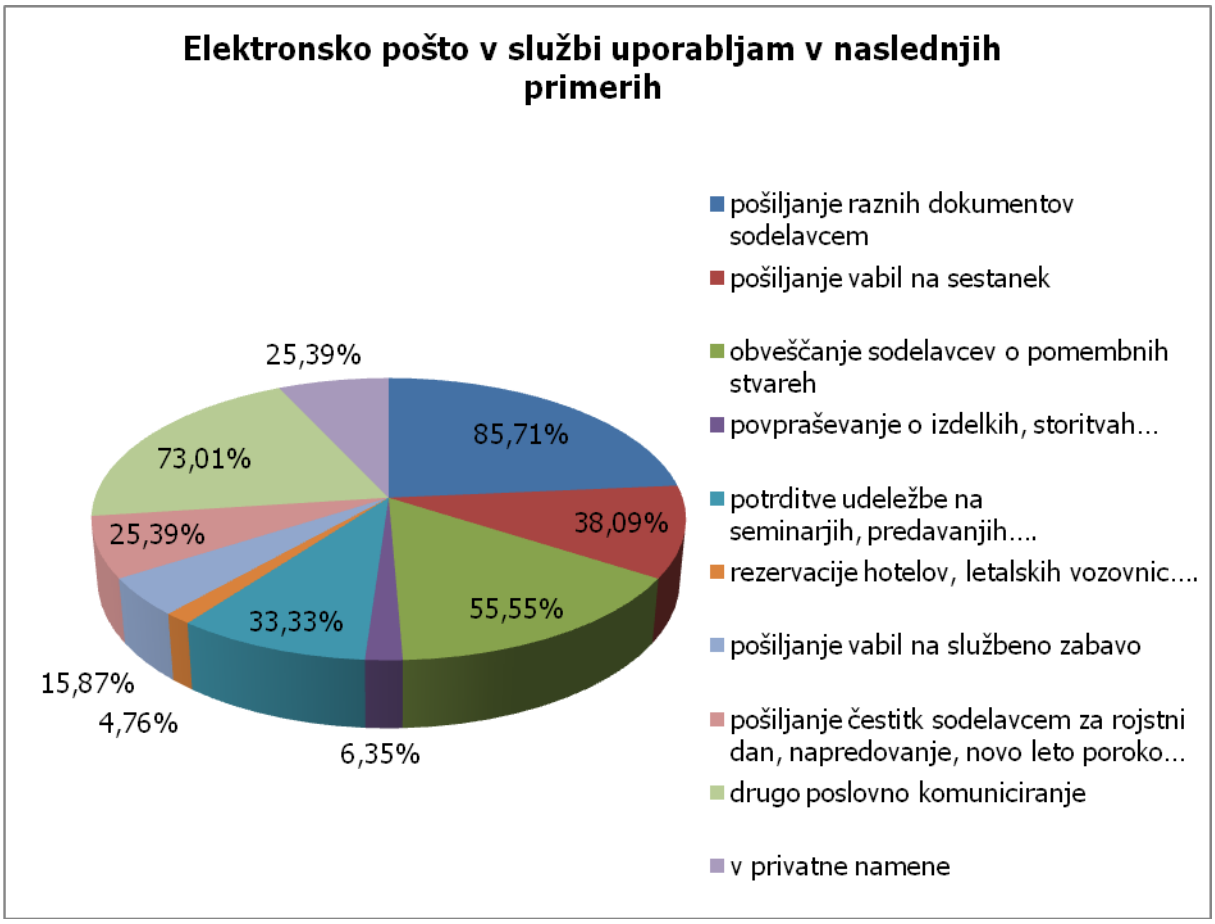


Vir: lasten

Vprašanje št. 8:

Elektronsko pošto v službi uporabljam v naslednjih primerih:
Elektronska pošta je postala vsestransko uporaben medij pri poslovnem komuniciranju. Anketa je pokazala, da je uporaba elektronske pošte v službi najbolj pogosta v naslednji primerih: pošiljanje raznih dokumentov sodelavcem (85,71 %), drugo poslovno komuniciranje (73,01 %) ter obveščanje sodelavcev o pomembnih stvareh (55,55 %). V privatne namene uporablja elektronsko pošto le 25,39 % vseh anketiranih oseb.

Graf 10: Primeri uporabe elektronske pošte

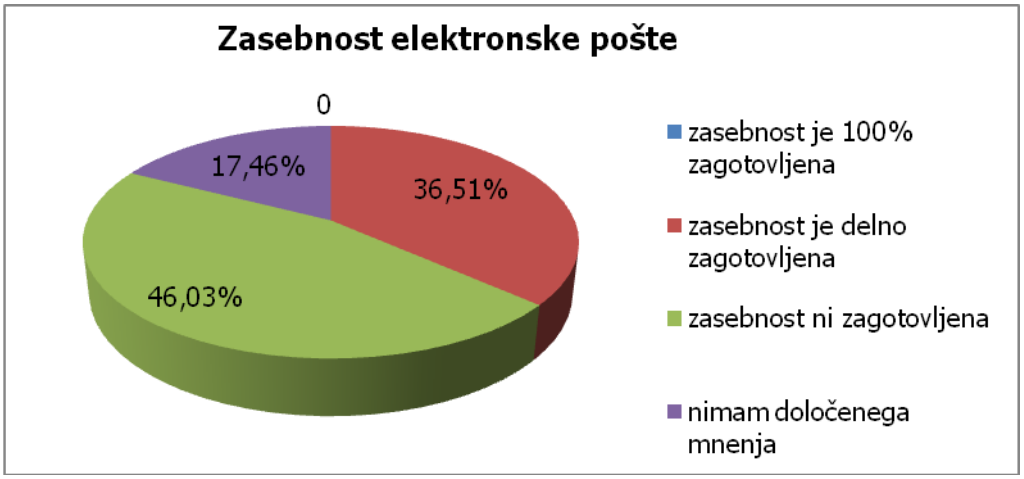


Vir: lasten

Vprašanje št. 9:

Kaj menite o zasebnosti elektronske pošte?
Pri vprašanju zasebnosti elektronske pošte sem naletela na precej negativen odziv, ljudje so na splošno mnenja, da prave zasebnosti skoraj ni. Kar 36,51 % vseh anketiranih oseb je prepričanih, da je zasebnost le delno zagotovljena, 46,03 % vseh je mnenja, da ni nikoli zagotovljena in nihče od anketiranih ni mnenja, da je zasebnost 100 % zagotovljena.

Graf 11: Zasebnost elektronske pošte



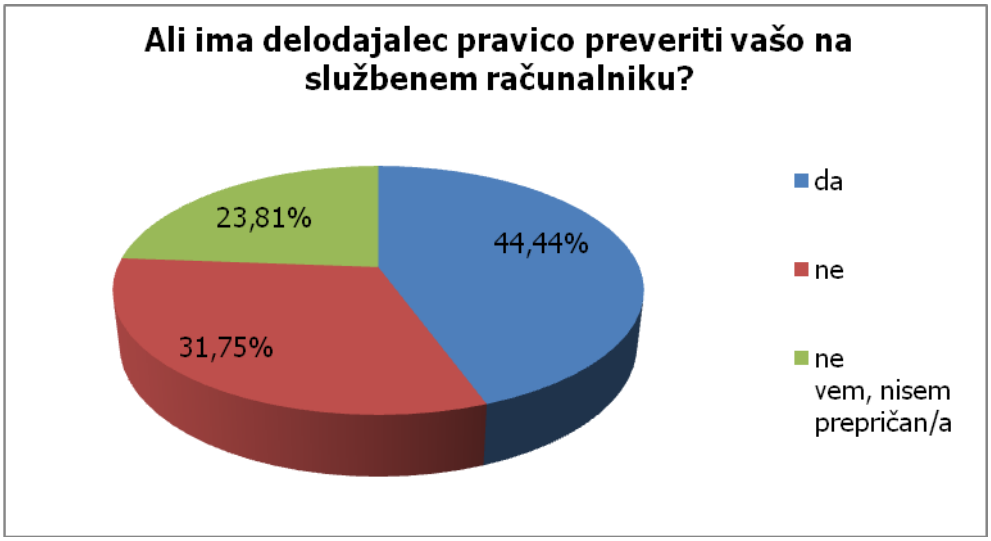
Vir: lasten

Vprašanje št. 10:

Ali menite, da ima delodajalec pravico preverit vašo elektronsko pošto na službenem računalniku?

Področje nadzora elektronske pošte je precej nedorečeno in zapleteno. Prav nepoznavanje zakonov in dejstvo, da delodajalec ne poskrbi za sprejetje pravilnika privede ljudi do mnenja, da ima delodajalec vsekakor pravico preveriti našo elektronsko pošto. Tudi anketa je potrdila moje trditve, saj je kar 44,44 % vseh odgovorilo na omenjeno vprašanje pritrdilno, kar pomeni, da zaposleni niso dovolj informirani o svojih pravicah na delovnem mestu. Pri tem vprašanju posebej izstopajo odgovori anketiranih oseb v starosti od 18-30 let. Kar 75 % teh je mnenja, da delodajalec sme preveriti njihovo elektronsko pošto na službenem računalniku.

Graf 12: Pravica delodajalca preveriti elektronsko pošto zaposlenih

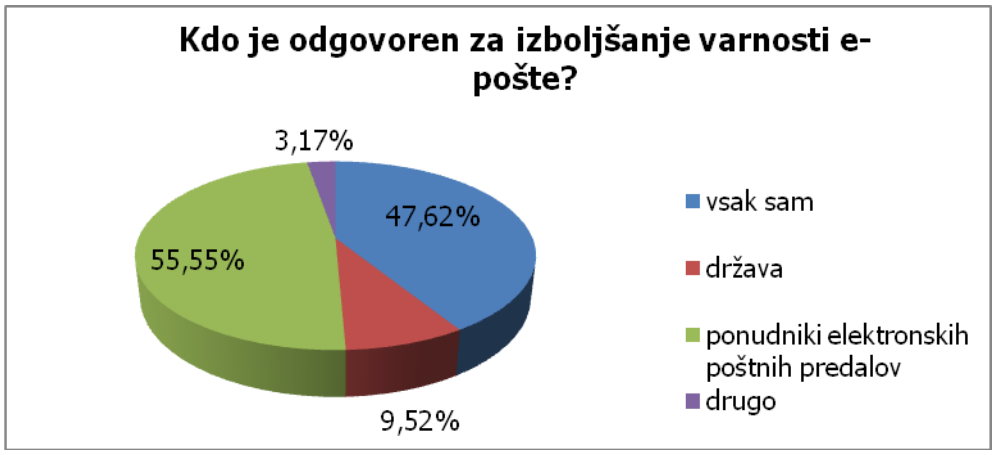


Vir: lasten

Vprašanje št. 11:

Kdo je odgovoren za izboljšanje varnosti e-pošte?
Moje mnenje je, da varnost elektronskih sporočil ni nikoli 100 %. Seveda e vprašamo, kdo je zato odgovoren oziroma, kdo je odgovoren za izboljšanje stanja na tem področju. V prvi vrsti so po mojem mnenju to ponudniki elektronskih poštnih predalov, za kar pa je v našem primeru pristojna država. Seveda tudi vsak sam v primeru, da se zaveda, kako najbolj varno komunicirati na ta način. Tudi odgovori na to vprašanje so bili podobni mojemu razmišljanju.

Graf 13: Kdo je odgovoren za izboljšanje varnosti e-pošte

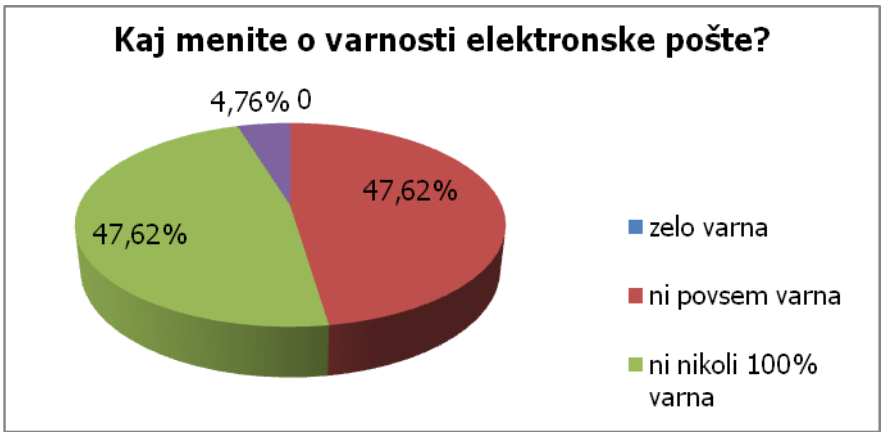


Vir: lasten

Vprašanje št. 12:

Kaj menite o varnosti elektronske pošte?
Pri vprašanju varnosti sem opazila podoben rezultat, kot pri vprašanju zasebnosti, kar je logično, saj sta pojma varnosti in zasebnosti zelo povezana. Nihče od anketiranih ni mnenja, da je zelo varna, 47,62 % je mnenja, da ni povsem varna, in enak procent anketiranih misli, da ni nikoli 100 % varna. Skoraj 5 % pa je takšnih, ki ne vedo, ali je varna.

Graf 14: Varnost elektronske pošte



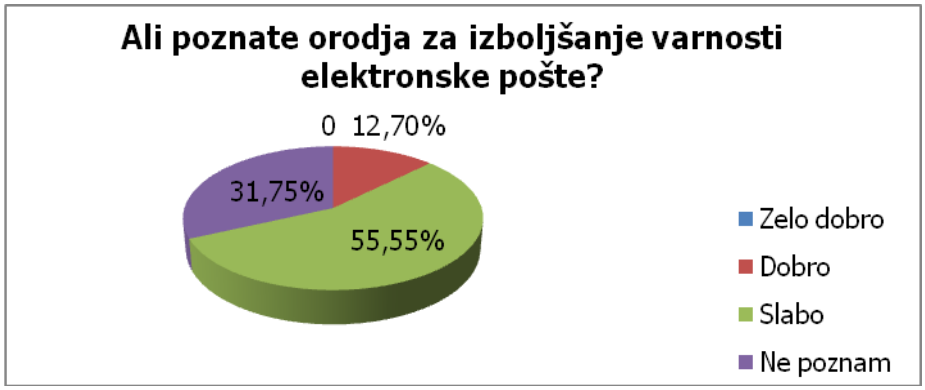
Vir: lasten

Vprašanje št.13:

Ali poznate orodja za izboljšanje varnosti elektronske pošte?

Le redko kdo pomisli na nevarnosti, ki nam prežijo na internetu, ko pošlje elektronsko sporočilo s svojega računalnika. Zaposleni se ne ukvarjajo s vprašanjem, ali je poskrbljeno za varnost elektronskih sporočil, saj jim je to dokaj samoumevno. Nihče od anketiranih ne pozno zelo dobro orodij za izboljšanje varnosti e-pošte in le malo je takšnih (12,7 %), ki ji pozna kar dobro. Odstopanja so se pokazala v starostni skupini oseb starosti nad 50 let. 54 % je takšnih, ki orodij za izboljšanje e-pošte ne poznajo, in 46 % takšnih, ki tovrstna orodja poznajo le slabo.

Graf 15: Poznavanje orodij za izboljšanje varnosti elektronske pošte



Vir: lasten

Vprašanje št. 14:

Ali je v vaši delovni organizaciji dobro poskrbljeno za zaščito in varnost elektronskih sporočil?

Moje mnenje je, da je za zaščito in varnost elektronskih sporočil pri delu javnih uslužbencev zelo dobro poskrbljeno in kar 50 % vseh anketiranih se z menoj strinja, kar 42 % je takšnih, ki z zaščito in varnostjo niso seznanjeni, le 8 % pa je takšnih, ki moji trditvi nasprotujejo.

Graf 16: Zaščita in varnost el. sporočil v delovni organizaciji

Vir: lasten

Vprašanje št. 15:

V času vaše odsotnosti je vaš nadrejeni pregledoval vaš računalnik in vaša privatna elektronska sporočila. Kako bi ukrepali?

Delodajalec ali vaš nadrejeni nima pravice preverjati elektronske pošte zaposlenih brez privolitve, saj zato nima zakonske podlage. Zaposleni imajo tudi na delovnem mestu pravico do zasebnosti, kar jim zagotavlja ustava in drugi zakoni. Presenetljivo je, da velik odstotek vprašanih ne bi ukrepal v primeru kršenja zasebnosti, pravzaprav bi veliki večini bilo vseeno, če bi njihov nadrejeni to počel (58,73 %). Pri odgovorih na to vprašanje je bilo največ odstopanj glede na starost anketiranih oseb. Izstopajo odgovori starostne skupine od 18-30 let. Visok odstotek, kar 62 %, je odgovoril, da bi nadrejenemu povedalo, da tega v prihodnosti ne dovolijo, in mnogo manj (37 %) je takšnih, ki bi jim bilo vseeno. V starostni skupini nad 50 let se nihče ni odločil za odgovor, da bi delodajalca v primeru kršitve varstva pravic zasebnosti in tajnosti pisem tudi prijavil.

Graf 17: Pregled računalnika in privatnih e-sporočil v času odsotnosti

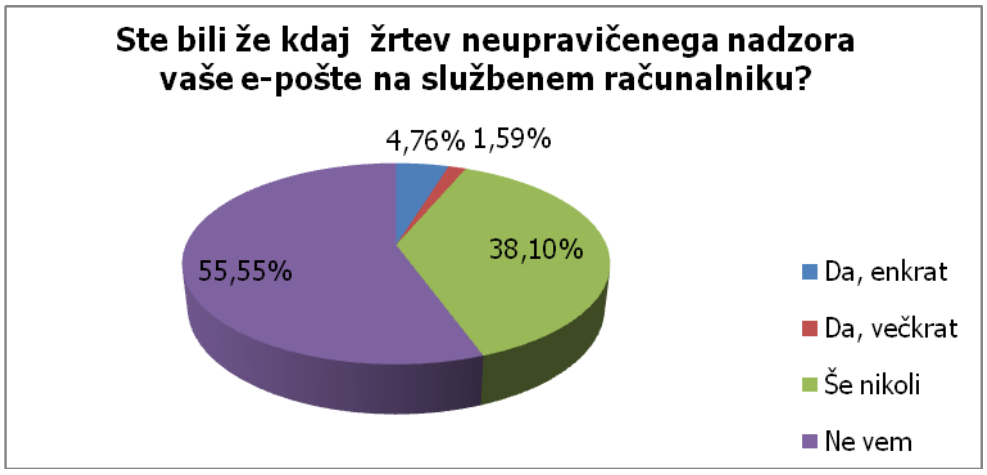
Vir: lasten

Vprašanje št. 16:

Ste bili že kdaj žrtev neupravičenega nadzora vaše e-pošte na službenem računalniku?

Verjetno je zelo težko ugotoviti, ali je nekdo neupravičeno pregledoval vašo e-pošto, zato so odgovori na to vprašanje dokaj realni. Zaposleni ne vedo, ali se je to že kadarkoli zgodilo (55,55 %), kar nekaj pa je takih, ki so prepričani, da še niso bili žrtev neupravičenega nadzora e-pošte (38,10 %). V starostni skupini anketiranih oseb od 31- 40 let je veliko takšnih (79 %), ki ne vedo, ali so bili že kdaj žrtev neupravičenega nadzora, 21 % pa je prepričanih, da se to še ni zgodilo.

Graf 18: Neupravičen nadzor e-pošte na službenem računalniku



Vir: lasten

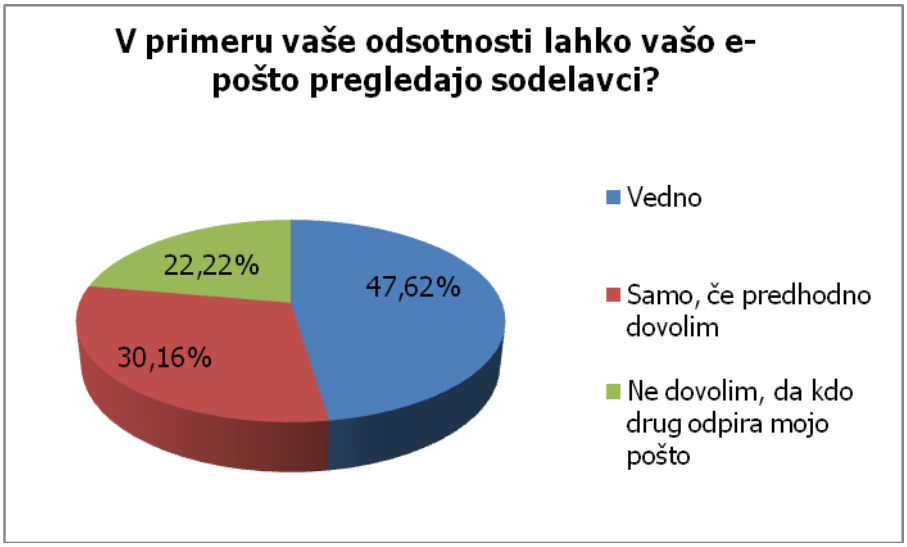
*Vpra*šanje št. 17:

V primeru vaše odsotnosti lahko vašo e-pošto pregledajo sodelavci?

Namen vprašanja je bil ugotoviti, kako je urejeno pregledovanje službenega poštnega naslova v primeru naše daljše odsotnosti na delovnem mestu. Če smo odsotni dalj časa, je potrebno e-pošto pregledati in pošiljateljem po potrebi odgovoriti. Če to stori zaposleni, ki nas uradno nadomešča, mu to lahko predhodno dovolimo pisno ali pa samo ustno. Zanimivo je, da je kar 22,22 % vseh anketiranih oseb tega striktno ne dovoli. Vprašanje je le, kaj se zgodi s prejeto pošto, kadar je ta delavec odsoten več mesecev.

Pri analizi odgovorov glede na starost pri tem vprašanju najbolj izstopajo odgovori v starostni skupini od 18-30 let. Kar 62 % anketirancev je odgovorilo, da bi sodelavcem vedno dovolilo pregledati njihovo elektronsko pošto, in nihče od vprašanih (0 %) tega ne bi nikakor dovolil.

Graf 19: Pregled e-pošte s strani sodelavcev v primeru odsotnosti



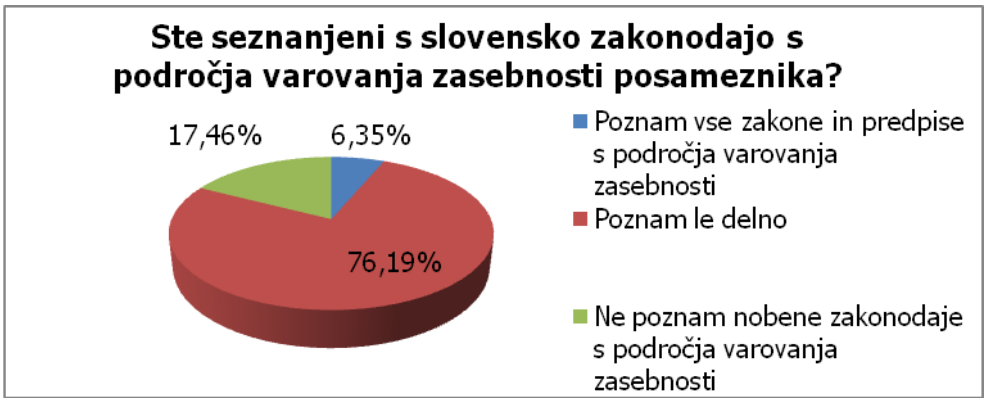
Vir: lasten

Vprašanje št. 18:

Ste seznanjeni s slovensko zakonodajo s področja varovanja zasebnosti posameznika?

Slovenska ustava obravnava omenjene pravice v treh členih, in sicer v 35.,37. in 38. členu. Verjamem, da zaposleni v javnem sektorju dobro poznajo Ustavo Republike Slovenije, zato je le malo takšnih, ki ne poznajo zakonodaje s področja varovanja zasebnosti.

Graf 20: Poznavanje slovenske zakonodaje s področja varovanja zasebnosti posameznika



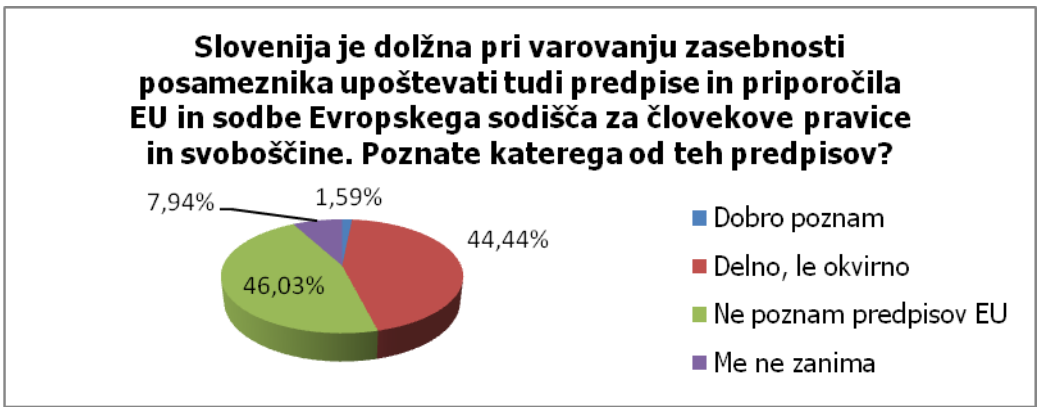
Vir: lasten

Vprašanje št. 19:

Slovenija je dolžna pri varovanju zasebnosti posameznika upoštevati tudi predpise in priporočila EU in sodbe Evropskega sodišča za človekove pravice in svoboščine. Poznate katerega od teh predpisov?

Predpisi in priporočila EU ter sodbe Evropskega sodišča za človekove pravice in svoboščine so nam manj blizu in manj poznana kot naša zakonodaja. Zato tudi odgovori na to vprašanja niso nikakršno presenečenje. Skoraj polovica anketiranih ne pozna predpisov EU in le majhen odstotek (1,59 %) jih pozna zelo dobro.

Graf 21: Poznavanje predpisov EU s področja varovanja zasebnosti posameznika



Vir: lasten

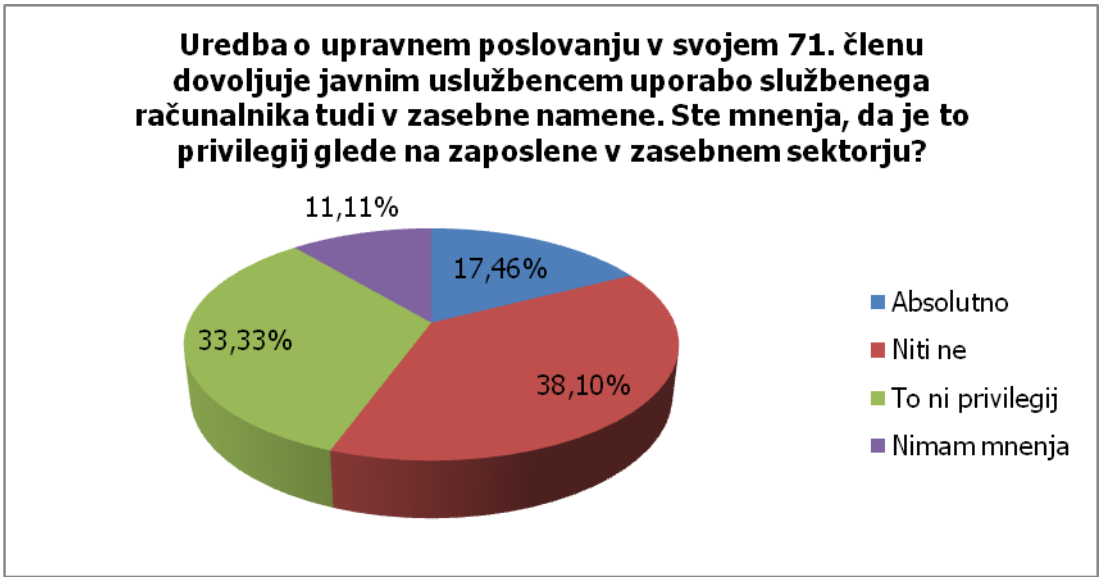
Vprašanje št. 20:

Uredba o upravnem poslovanju v svojem 71. členu dovoljuje javnim uslužbencem uporabo službenega računalnika tudi v zasebne namene. Ste mnenja, da je to privilegij glede na zaposlene v zasebnem sektorju?

Na splošno je mnenje ljudi v Sloveniji, da smo zaposleni v javnem sektorju v privilegiranem položaju glede na zaposlene v zasebnem sektorju. Eden takšnih, po mojem mnenju privilegijev pa je 71. člen Uredbe o upravnem poslovanju. Kljub temu se večina anketiranih ne strinja z menoj, da je to prednost oz. privilegij.

Opazila sem nekaj odstopanj glede na starost anketiranih oseb. V skupini od 18-30 let nihče ni mnenja, da je to privilegij, 62 % vprašanih se je na to vprašanje odločilo za odgovor, da to glede na zaposlene v zasebnem sektorju niti ni privilegij. V starostni skupini nad 50 let pa so se odgovori dokaj razlikovali, saj je kar 38 % vprašanih prepričanih, da to je privilegij.

Graf 22: Privilegij javnih uslužbencev pri uporabi službenega računalnika



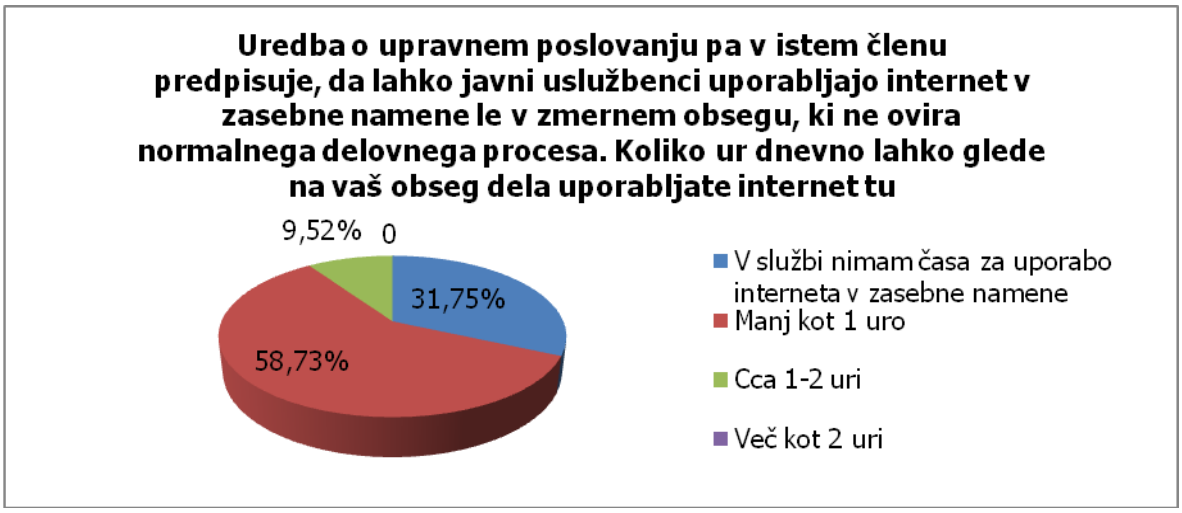
Vir: lasten

Vprašanje št. 21:

Uredba o upravnem poslovanju pa v istem členu predpisuje, da lahko javni uslužbenci uporabljajo internet v zasebne namene le v zmernem obsegu, ki ne ovira normalnega delovnega procesa. Koliko ur dnevno lahko glede na vaš obseg dela uporabljate internet tudi v zasebne namene?

Zelo zanimivi so bili odgovori na to vprašanje. Po mojem mnenju ne odražajo dejanskega stanja in so bili v kar nekaj primerih neiskreni. Enostavno ne morem verjeti, da ima nekdo vsak dan v službi takšen obseg dela, da nima niti minute časa za kakšen oseben opravek na internetu oz. pošiljanje tudi kakšne zasebne elektronske pošte. Mogoče pa se motim?

Graf 23: Dnevna uporaba službenega računalnika v zasebne namene



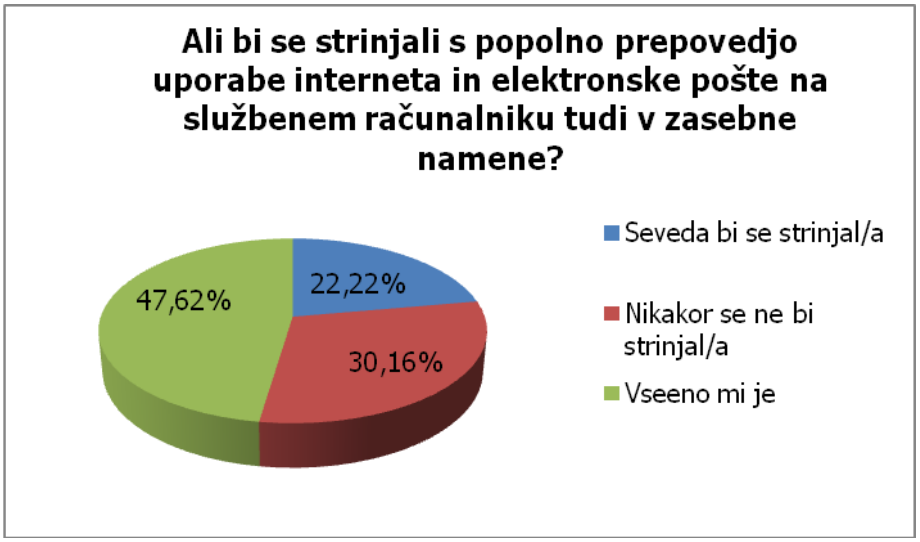
Vir: lasten

Vprašanje št. 22:

Ali bi se strinjali s popolno prepovedjo uporabe interneta in elektronske pošte na službenem računalniku tudi v zasebne namene?

Takšna popolna prepoved bi bila seveda skoraj nerealna in bi pomenila stalen nadzor nad početjem zaposlenih, kar pa je nedopustno in v nasprotju z našo ustavo in zakoni. Kar 47,62 % anketiranim bi bilo vseeno, če bi se to resnično zgodilo, kar je presenetljivo veliko. Zanimivo je, da je kar 50 % vseh anketiranih oseb v starostni skupini od 18-30 let odgovorilo, da bi se strinjalo s popolno prepovedjo uporabe e-pošte in interneta na službenem računalniku tudi v zasebne namene.

Graf 24: Možnost prepovedi uporabe interneta in e-pošte na službenem računalniku tudi v zasebne namene



Vir: lasten

8.2.3 ANALIZA ANKETE

S pomočjo ankete sem ugotovila naslednje:

- v vrstah javnih uslužbencev je uporaba elektronske pošte postala del delovnega procesa in težko najdemo še nekoga, ki je ne bi uporabljal;
- velik problem še vedno predstavlja nepoznavanje zakonov glede zasebnosti in varnosti elektronske pošte, saj pravilnika o uporabi elektronske pošte še marsikje nimajo;
- zaposleni niso seznanjeni s svojimi pravicami glede zasebnosti na delovnem mestu na področju elektronskega komuniciranja, kar je posledica nepoznavanja slovenskih in EU predpisov;
- veliki večini se ne zdi sporno oz. so mnenja, da ima njihov predpostavljeni pravico pregledovati njihovo e-pošto na službenem računalniku;
- prav tako se večini ne zdi sporno, če sodelavci pregledajo njihovo e-pošto v času odsotnosti;
- zaposleni v javnem sektorju so mnenja, da e-pošta ni povsem varna;
- zaposleni v javnem sektorju so prepričani, da ni zagotovljene zasebnosti pri elektronskem komuniciranju;
- še vedno je nekaj takšnih, ki ne preverjajo svojih službenih e-predalov vsaj 1-krat na dan;
- le redki zaposleni v javnem sektorju ne uporabljajo službenega računalnika tudi v zasebne namene.

Rezultati ankete so potrdili moje hipoteze o elektronskem poslovnem komuniciranju v javnem sektorju. Večina zaposlenih v javnem sektorju se zaveda nevarnosti in pomanjkljivosti glede zagotavljanja zasebnosti, ki jih prinaša tovrstno komuniciranje, pa vendarle ne poznajo dovolj dobro svojih pravic, ki jim jih zagotavlja Ustava Republike Slovenije in drugi zakoni s področja varovanja zasebnosti posameznika.

9 PREDLOG UREDITVE KOMUNICIRANJA Z E-POŠTO V ORGANU JAVNE UPRAVE

Zanimivo je, da je postala uporaba elektronske pošte tako pomembna in skoraj nenadomestljiva, še vedno pa nimamo sprejetega enotnega zakona, uredbe, ki bi do potankosti urejala to področje. Tudi sama sem zaposlena v javnem sektorju in pri nas prav tako še nimamo sprejetega Pravilnika o uporabi elektronske pošte na delovnem mestu, kar predstavlja po mojem mnenju veliko pomanjkljivost. Zaposleni ne vemo, kakšne so naše pravice in dolžnosti pri elektronskem poslovnem komuniciranju. Nismo seznanjeni s stvarmi, ki se nam trenutno zdijo še samoumevne. Ko bomo prvič soočeni z večjim problemom na tem področju, t se bomo verjetno vprašali, v kolikšni meri smo bili seznanjeni s pravili. Vsekakor je to področje mnogo bolje urejeno v javni upravi. Kot vemo, je Ministrstvo za javno upravo sprejelo priporočila, ki urejajo tudi področje elektronskega komuniciranja zaposlenih na delovnem mestu.
Kaj pa vsi ostali zaposleni v javnem sektorju?
Za nas velja Uredba o upravnem poslovanju, ki v svojih členih sicer omenja nekaj pravil e-komuniciranja na delovnem mestu. Pa vendar sem mnenja, da temu področju ne posveča dovolj prostora in je dokaj ohlapna. Mislim, da bi morala Vlada Republike Slovenije sprejeti Uredbo o poslovnem elektronskem komuniciranju v vrstah javnega sektorja, katera bi morala vsekakor vsebovati vsa osnovna pravila tovrstnega komuniciranja na delovnem mestu. Pomemben del takšne Uredbe bi bilo določilo, ki zavezuje vsako delovno organizacijo v javnem sektorju, da sprejme svoj Pravilnik o uporabi elektronske pošte na delovnem mestu. Delavec mora biti pred nastopom dela v javnem sektorju seznanjen tudi s pravili e-komuniciranja na delovnem mestu. Doseženo mora biti pravo razmerje med stopnjo nadzora in zasebnostjo zaposlenih.

10 ZAKLJUČEK

Elektronska pošta predstavlja najpogostejšo in s stališča novih uporabnikov najhitreje rastočo storitev v internetu. Vsekakor je postala osnovno orodje komuniciranja na daljavo in pravzaprav pridobiva na premoči nad običajnimi oblikami sporočanja, kot so pisma, telefaksi in telefon. Vzrok temu je vsekakor hitrost, preprostost in poceni uporaba.
Cilj diplomske naloge je bil raziskati uporabo elektronske pošte, vse prednosti tovrstnega komuniciranja, nevarnosti, ki prežijo na nas, posredne in neposredne koristi, kakšna je varnost, kako je zagotovljena zasebnosti pri uporabi e-pošte, ter s pomočjo raziskave ugotoviti, kakšni so mišljenje, znanje, izkušnje in obstoječe stanje zaposlenih v javnem sektorju na temo uporabe e-pošte.
Ob koncu svojega raziskovanja lahko rečem, da me je najbolj pritegnila tema zasebnosti in pravice do nadzora s strani delodajalca. Delovnega mesta brez računalnika in interneta si ne znamo več predstavljati. Z njegovo uporabo smo hitrejši, učinkovitejši, postal je nepogrešljivi del našega delovnega vsakdana. Kljub obilici dela še vedno najdemo čas, da postorimo tudi kakšno malenkost iz našega privatnega življenja. In tukaj se poraja vprašanje, ali nam je to dovoljeno ali ne. V kakšnem obsegu lahko uporabljamo službeni računalnik v zasebne namene, brskamo po internetu in pošiljamo zasebno e-pošto iz službenega računalnika? Uredba o upravnem poslovanju to dovoljuje zaposlenim v javnem sektorju, drugače je seveda v zasebnem sektorju. Moje mnenje je, da je to privilegij. Pa vendarle kar velik odstotek ljudi zaposlenih v javnem sektorju ne misli tako. Velik odstotek zaposlenih v javnem sektorju sploh ne ve, da obstaja 71. člen, ki jim dovoljuje uporabo interneta na delovnem mestu tudi v zasebne namene. Ljudje niso dovolj dobro poučeni o svojih pravicah in dolžnostih na delovnem mestu. Zanimivo je, da je postala uporaba elektronske pošte tako pomembna in skoraj nenadomestljiva, še vedno pa nimamo sprejetega enotnega zakona, ki bi do potankosti urejal to področje. Rezultati ankete so pokazali precej zadovoljivo stanje poznavanja elektronske pošte javnih uslužbencev. Anketa je tako pokazala, da se večina zaposlenih zaveda vseh nevarnosti, ki prežijo na nas, predvsem tistih, ki jih srečujemo vsak dan.
Pri pisanju diplomske naloge sem osvojila nova znanja s področja elektronske pošte, znanja, ki mi bodo vsekakor v veliko pomoč pri vsakdanjem delu v prihodnje. Spoznala sem, da vedno obstaja možnost, da nas lahko nekdo opazuje, ne da bi se tega zavedali. Zato previdnost ni nikoli odveč. Moramo pa vedeti, da imamo vso pravico zaščititi svojo zasebnost. Zelo naivno pa bi bilo razmišljati, da nikomur ni mar za naše podatke oziroma vsebino naše elektronske pošte. Ali sploh pomislimo, kdo vse ima dostop in lahko prebere naše poslovno pismo, ki mogoče vsebuje podatke, ki so po predpisih tajni in lahko ogrozijo integriteto druge osebe? Mislim, da se tega premalo zavedamo. Verjetno marsikdo o tem sploh ne razmišlja, pa bi vendarle moral.
Prepričana sem, da bom v prihodnje z zanimanjem prebrala vsako novost, ki se bo kakorkoli nanašala na to temo. Verjetno bo teh še kar nekaj, pričakujem jih prav na področju zasebnosti in nadzora. Gotovo bomo priča morebitnim tožbam posameznikov proti podjetjem ali državi zaradi zlorabe osebnih podatkov.
Elektronska pošta se z veliko hitrostjo širi in že sedaj dodobra nadomešča govorno sporazumevanje. Bojim se, da bo v prihodnje popolnoma izrinila še »običajno pošto«.
Mislim, da so možnosti tega medija neskončne, zato se pustimo presenetiti.

LITERATURA IN VIRI

LITERATURA

1. ALSPACH, Ted (1996). *Elektronska pošta na internetu.* Založba Vlado Grlica, Ljubljana.

2. BOGATAJ JANČIČ, Maja, mag. KLEMENČIČ, Goran, mag. MAKAROVIČ, Boštjan, TIČAR, Klemen, mag. TOPLIŠEK, Janez (2007). *Pravni vodnik po internetu.* GV založba, Ljubljana.

3. ETAN,Mark in MAHER,Tim (2005). *Varnost informacij.* Založba Pasadena, Ljubljana.

1. HUBER, Jernej (2006). *Poslovna raba elektronske pošte.* Dosegljivo 27.12.2006 na: http://revija.mojedelo.com/karierni-razvoj/poslovna-raba-elektronske-poste-206.aspx

2. HUMAR, Gregor (2006). *Brezplačno elektronsko dopisovanje.* Dosegljivo 12.3.2011 na: http://www.monitor.si/clanek/brezplacno-elektronsko-dopisovanje/

3. HAJTNIK in STANIČ (2009). *Komunikacijska zasebnost - da ali ne?* Dosegljivo 3.5.2009 na: http://dne.enaa.com/E-svet/E-druzba/Komunikacijska-zasebnost-da-ali-ne.html

4. KOREN, Jure (2005). *Sistem elektronske pošte.* Dosegljivo 12.3.2011 na: http://www.monitor.si/clanek/sistem-elektronske-poste/

5. KOVAČIČ, Matej (2000). *Zasebnost v informacijski družbi.* Dosegljivo 14.3.2011 na: http://dk.fdv.uni-lj.si/tip/tip20006kovacic.PDF

4. KOVAČIČ, Matej (2006). *Nadzor in zasebnost v informacijski družbi.* Znanstvena knjižnica Fakultete za družbene vede, Ljubljana.

5. KOVAČIČ,Matej (2010). *Kriminaliteta in tehnologija - Komunikacijska zasebnost na delovnem mestu.* Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Ljubljana.

6. MAKAROVIČ, Boštjan, mag. KLEMENČIČ, Goran, dr. KLOBUČAR,Tomaž, mag. BOGATAJ, Maja, PAHOR, David (2001). *Internet in pravo.* Založba Pasadena, Ljubljana.

7. M.K.,(2005). *24. ur novice – Nevarna elektronska sporočila.* Dosegljivo 16.10.2005 na: http://24ur.com/novice/it/nevarna-elektronska-sporocila.html

8. OCVIRK, Vasja (2003). *Spam – Internetna kuga.* Dosegljivo 14.3.2011 na: http://www.nasvet.com/spam/

9. OCVIRK, Vasja (2003). *Zakaj klikamo na okužene priponke?* Dosegljivo 14.3.2011 na: http://www.nasvet.com/priponke/

10. RADOŠ, Škrt (2005). *Bonton uporabe e-pošte.* Dosegljivo 14.3.2011 na: http://www.nasvet.com/bonton-posta/

11. RADOŠ, Škrt (2003). *Nezaželena e-pošta in slovenska zakonodaja.* Dosegljivo 14.3.2011 na: http://www.nasvet.com/nezazelena-posta/

12. SRNOVRŠNIK, Tanja (2011). *Zaposleni imajo pravico do zasebnosti na delovnem mestu.* Dosegljivo 13.3.2011 na: http://www.pravna-varnost.si/livelawyers_news_detail.php?detail=1&newsid=26

VIRI

1. AK-Portal (2011). *Private E-Mail - Nutzung am Arbeitsplatz.* Dosegljivo 1.3.2011 na: http://www.arbeiterkammer.at/online/private-emails-im-buero-25261.html

2. ARNES – javni zavod (2006). *Pravila uporabe omrežja Arnes.* Dosegljivo 1.3.2011 na: www.arnes.si/pravila.htm

3. Der Bayerische Landesbeauftragte für den Datenschutz (2011). *Private Internet- und E-Mail – nutzung.* Dosegljivo 1.3.2011 na: http://www.datenschutz-bayern.de/technik/orient/privmail.html

4. EUR-Lex (2002). *Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij.* Dosegljivo 31.7.2002 na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:01:SL:HTML

5. Informacijski pooblaščenec (2011). Dosegljivo 10.8.2011 na: http://www.ip-rs.si

6. Ministrstvo za javno upravo (2010). *Priporočila informacijske varnostne politike Javne uprave.* Dosegljivo 10.8.2011 na: http://www.mju.gov.si/fileadmin/mju.gov.si/-pageuploads/DEUP/IVPJU.doc_01.pdf

7. Ministrstvo za šolstvo in šport in Zavod Republike Slovenije za šolstvo (2011). *Računalniški virusi.* Dosegljivo 10.8.2011 na: http://ro.zrsss.si/projekti/comp/racopismen/anti-virus/Anti%20virus.html

8. SERŠ Maribor (2011). *Kriptografija.* Dosegljivo 13.3.2011 na: http://www.s-sers.mb.edus.si/gradiva/w3/omrezja/63_varnost/02_kripto.html

9. Zakon o elektronski komunikacijah, (ZEKom). Uradni list RS, Št. 43/2004, 86/2004-ZV OP-1, 129/2006, 13/2007-UPB1, 102/2007- ZDRad, 110/2009, 33/2011

10. Zakon o informacijskem pooblaščencu (ZinfP). Uradni list RS št. 113/2005, 51/2007 – ZustS-A, 14/2010 Odl.US: U-I303/08-9.

11. Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, Št. 86/2004, 113/2005-ZInfP, 51/2007-ZUstS-A, 67/2007, 94/2007-UPB1

12. Uredba o upravnem poslovanju, Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 63/07, 115/07, 31/08, 35/2009, 58/10, 101/2010.

PRILOGE

Priloga 1: Anketni vprašalnik

ANKETNI VPRAŠALNIK

VARNOST IN ZASEBNOST ELEKTRONSKIH SPOROČIL NA DELOVNEM MESTU

Anketa je anonimna in je sestavni del diplomske naloge na
FAKULTETI ZA UPRAVO V Ljubljani. Naslov diplomske naloge je:

E-pošta kot komunikacijski kanal na delovnem mestu v javni upravi: vidik zasebnosti.

Prosim vas, da obkrožite črko pred pravilnim odgovorom (lahko se odločite tudi za več različnih odgovorov), ki predstavlja vaše mnenje.

Spol: M Ž (obkroži) **Starost:** ____ let

1. **Izobrazba.**

a. Poklicna ali srednja strokovna izobrazba
b. Višja strokovna izobrazba
c. Visoka ali univerzitetna izobrazba
d. Magisterij, doktorat

2. **Elektronsko pošto uporabljam:**

a. Doma
b. V službi
c. Pri prijateljih, sorodnikih
d. V knjižnici
e. Na dopustu – prenosni računalnik
f. V Cyber – coffee, Internet coffee

3. **Koliko službenih elektronskih sporočil pošljete v povprečju na dan?**

a. nič
b. 1–5
c. 10 ali več

4. Kako pogosto v povprečju na dan preverite elektronsko pošto na vašem službenem računalniku?

a. Ne preverim je vsak dan
b. 1 do 2-krat na dan
c. 3 do 5-krat na dan
d. Več kot 5-krat na dan

5. Ali uporabljate službeni računalnik tudi za prejemanje in pošiljanje zasebne pošte?

a. Ne, nikoli
b. Da, zelo pogosto
c. Zelo redko

6. Pri pošiljanju privatnih sporočil iz službenega računalnika včasih pošljem tudi takšna s sporno vsebino.

a. Tega ne počnem nikoli, saj se zavedam, da to lahko vidi tudi kdo drug
b. Včasih, če pozabim na pomanjkljivost varnosti e-pošte
c. Zelo pogosto, saj mi je vseeno, če tudi kdo drug vidi moja sporočila

7. V službi imamo sprejet Pravilnik o uporabi elektronske pošte na delovnem mestu.

a. Da
b. Ne
c. Ne vem, nisem seznanjen/-a

8. Elektronsko pošto v službi uporabljam v naslednjih primerih:

a. pošiljanje raznih dokumentov sodelavcem
b. pošiljanje vabil na sestanek
c. obveščanje sodelavcev o pomembnih stvareh
d. povpraševanje o izdelkih, storitvah …
e. potrditve udeležbe na seminarjih, predavanjih …
f. rezervacije hotelov, letalskih vozovnic …
g. pošiljanje vabil na službeno zabavo
h. pošiljanje čestitk sodelavcem za rojstni dan, napredovanje, novo leto, poroko …
i. drugo poslovno komuniciranje
j. v privatne namene

9. Kaj menite o zasebnosti elektronske pošte?

a. zasebnost je 100% zagotovljena
b. zasebnost je delno zagotovljena
c. zasebnost ni zagotovljena
d. nimam mnenja

10. Ali menite, da ima delodajalec pravico preverit vašo elektronsko pošto na službenem računalniku?

a. Da
b. Ne
c. Ne vem, nisem prepričan/-a

11. Kdo je odgovoren za izboljšanje varnosti e-pošte?

a. Vsak sam
b. Država
c. Ponudniki elektronskih poštnih predalov
d. Drugo

12. Kaj menite o varnosti elektronske pošte?

a. Zelo varna
b. Ni povsem varna
c. Ni nikoli 100 % varna
d. Ne vem

13. Ali poznate orodja za izboljšanje varnosti elektronske pošte?

a. Zelo dobro
b. Dobro
c. Slabo
d. Ne poznam

14. Ali je v vaši delovni organizaciji dobro poskrbljeno za zaščito in varnost elektronskih sporočil?

a. Prepričan/a sem, da je dobro poskrbljeno
b. Ne, nisem prepričan/-a, da je dobro poskrbljeno
c. Nisem seznanjen/-a

15. V času vaše odsotnosti je vaš nadrejeni pregledoval vaš računalnik in vaša privatna elektronska sporočila. Kako bi ukrepali?

a. Vseeno bi mi bilo
b. Povedal/a bi mu, da tega v prihodnosti ne dovolim
c. Prijavil/a bi ga zaradi kršenja varstva pravic zasebnosti in tajnosti pisem

16. Ste bili že kdaj žrtev neupravičenega nadzora vaše e-pošte na službenem računalniku?

a. Da, enkrat
b. Da, večkrat
c. Še nikoli
d. Ne vem

17. V primeru vaše odsotnosti lahko vašo e-pošto pregledajo sodelavci?

a. Vedno
b. Samo, če predhodno dovolim
c. Ne dovolim, da kdo drug odpira mojo pošto

18. Ste seznanjeni s slovensko zakonodajo s področja varovanja zasebnosti posameznika?

a. Poznam vse zakone in predpise s področja varovanja zasebnosti
b. Poznam le delno
c. Ne poznam nobene zakonodaje s področja varovanja zasebnosti

19. Slovenija je dolžna pri varovanju zasebnosti posameznika upoštevati tudi predpise in priporočila EU in sodbe Evropskega sodišča za človekove pravice in svoboščine. Poznate katerega od teh predpisov?

a. Dobro poznam
b. Delno, le okvirno
c. Ne poznam predpisov EU
d. Me ne zanima

20. Uredba o upravnem poslovanju v svojem 71. členu dovoljuje javnim uslužbencem uporabo službenega računalnika tudi v zasebne namene. Ste mnenja, da je to privilegij glede na zaposlene v zasebnem sektorju?

a. Absolutno
b. Niti ne
c. To ni privilegij
d. Nimam mnenja

21. Uredba o upravnem poslovanju pa v istem členu predpisuje, da lahko javni uslužbenci uporabljajo internet v zasebne namene le v zmernem obsegu, ki ne ovira normalnega delovnega procesa. Koliko ur dnevno lahko glede na vaš obseg dela uporabljate internet tudi v zasebne namene?

a. V službi nimam časa za uporabo interneta v zasebne namene
b. Manj kot 1 uro
c. Cca 1-2 uri
d. Več kot 2 uri

22. Ali bi se strinjali s popolno prepovedjo uporabe interneta in elektronske pošte na službenem računalniku tudi v zasebne namene?

a. Seveda bi se strinjal/-a
b. Nikakor se ne bi strinjal/-a
c. Vseeno mi je

Hvala za sodelovanje!