UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MANAGEMENT KOPER

Dodiplomski visokošolski strokovni študijski program Management

Diplomska naloga

ZAKONODAJA S PODROČJA ELEKTRONSKEGA POSLOVANJA

Mentor: prof. dr. Dušan Lesjak
Somentor:
Obravnavana organizacija:
Strokovni sodelavec iz organizacije:
Koordinator diplomskega projekta:

KOPER, 2004

MATEJ KORON

POVZETEK

Število uporabnikov elektronskega poslovanja po vsem svetu in tudi v Sloveniji še vedno hitro narašča, kar kažejo tudi zadnje raziskave v Sloveniji. S povečevanjem vloge elektronskega poslovanja v življenju naraščajo tudi možnosti za njegovo zlorabo. To predstavlja številne možnosti za razne kršitelje, ki jim dostop do podatkov v elektronski obliki predstavlja vir zaslužka. Vse to posledično vpliva na zakonodajno oblast pri usklajevanju zakonov na področju elektronskega poslovanja in nadzoru njegovih vsebin. Zakoni na področju elektronskega poslovanja so še vedno šibka točka v vseh državah sveta, celo v ZDA, ki ima največ prakse pri obravnavanju takih kršitev.

Ključne besede: elektronsko poslovanje, elektronsko sporočilo, zakonodaja, kršitev, varstvo in zaščita podatkov, zasebnost.

ABSTRACT

The number of electronic management users all over the world is increasing rapid, also in Slovenia, as it is indicated by the latest research in Slovenia. By the significance of electronic management in common life the possibility for its misuse is also increasing. That represents ideal opportunity for various trespassers; for them the access to electronic data represents income advantage. This situation consequently influence on legislative authority in harmonizing the law of electronic management domain and its supervising contents. The law of electronic management domain is still very delicate in all states of the world, also in USA, which have the most practice treating this kind of offenses.

Key words: electronic management, electronic data, legislation, offense, safeguard and protection of data, privacy.

UDK 343.7:004.738.5 (043.2)

ZAHVALA

Zahvalil bi se mentorju prof. dr. Dušanu Lesjaku in Benjaminu Lesjaku, ki sta mi pomagala pri izdelavi Diplomske naloge ter dr. Zoltanu Janu, ki je Diplomsko nalogo lektoriral.

VSEBINA

1. UVOD

Dinamičen razvoj informacijske tehnologije je v zadnjih letih povzročil družbene spremembe. Elektronsko poslovanje se danes vse več uporablja v gospodarstvu kakor tudi v negospodarstvu, v gospodinjstvih in še drugje. Globalni informacijski splet, internet, medmrežje so imena, ki označujejo v mrežo povezane strežnike, delovne postaje in osebne računalnike. Vse to nam omogoča, da lahko danes uspešno poslujemo in pošiljamo elektronska sporočila po vsem svetu. Elektronsko poslovanje je postalo ne samo ena od možnosti, temveč čedalje bolj nujnost za moderno poslovanje. Kakor je šel razvoj tehnologije skozi zgodovino in se uveljavil v vsakdanji rabi kot nujnost npr.: osebni avtomobil, televizor, telefon, v zadnjem času mobilni telefon in računalnik, tako je tudi na področju informacijskih storitev zaradi hitrosti in praktičnosti elektronsko poslovanje izpodrinilo običajne oblike poslovanja, tu je predvsem mišljeno papirno poslovanje, ki vedno bolj zgublja svoj nekdanji primat v poslovni sferi.

Elektronsko poslovanje se je s pomočjo interneta predvsem v zadnjem desetletju prejšnjega stoletja razvilo in razširilo na veliko število uporabnikov predvsem zaradi praktičnosti, hitrosti in velikega obsega podatkov, ki jih lahko prenašamo s pomočjo različnih medijev na velike razdalje. Danes se s pomočjo elektronskega poslovanja izvajajo različni posli, trženjska komunikacija, industrija idr.

Prav zaradi vseh naštetih prednosti je elektronsko poslovanje postalo tudi idealno za razne nepridiprave, ki so vedno težje obvladljivi. Ko pošiljamo elektronska sporočila preko samega spleta internetnih storitev, je seveda to idealna priložnost za razne nepridiprave bodisi za lahek zaslužek, ali zgolj za izživljanje nad uporabniki in ponudniki storitev ter kaljenje svojega računalniškega znanja.

Zaradi tega je elektronsko poslovanje vedno bolj tvegano. To zahteva uvajanje številnih etičnih načel pri njegovi uporabi, vedno večjo uporabo varnostne tehnologije, potrebno pa je bilo uvesti zakonodajo, ki regulira uporabo elektronskega poslovanja in mora zajemati izjemen obseg potencialnih kršitev ter zlorab na področju elektronskega poslovanja, če hočemo vzdrževati sorazmerno visoko varnost in zanesljivost.

Cilj diplomske naloge je predstaviti zakonodajo s področja elektronskega poslovanja, osvetliti šibke točke pri elektronskem poslovanju in opozoriti na potencialne nevarnosti, ki pri tem na nas prežijo. Največji izziv bo spremljanje razvoja splošne zakonodaje in kazenske zakonodaje na področju elektronskega poslovanja, ki je še vedno v povojih in zahteva ponovno opredelitev pristojnosti institucij, pomena terminov svoboda govora in tiska ter varnost osebnih podatkov, avtorskih pravic na področju digitalnih medijev in še vedno naraščajoč obseg različnih oblik kršitev.

Diplomska naloga je sestavljena iz petih poglavji, v katerih so razčlenjene teze, na podlagi katerih je nastala ta naloga. Na začetku so predstavljena razmišljanja o elektronskem sporočilu, sledi poglavje o zakonodaji o elektronskih naslovih, naslednje

poglavje obravnava varstvo podatkov v elektronski obliki, nato je poglavje o zasebnosti in poglavje jurisdikcija v elektronskem okolju. Namen naloge je preučiti obravnavane posamezne probleme, izločiti prednosti in slabosti s področja zakonodaje o elektronskem poslovanju ter dodati svoje mišljenje o tem.

2. ELEKTRONSKO SPOROČILO

Vsak dan se srečujemo s komuniciranjem, ki ga opravljamo na različne načine, eden od njih ima tudi elektronsko obliko. Podatki, ki se prenašajo v elektronski obliki, v obliki sporočil se imenujejo elektronska sporočila. Ta so lahko podatkovna sporočila, ki so lahko kot elektronski način prenosa podatkov, ali izmenjave podatkov. Na področju elektronskega sporočanja se uveljavlja izraz *nematerializirana oblika*, kar je s fizikalnega stališča neutemeljeno poimenovanje. Ta pojem izraža prevladovanje papirnega izražanja v papirnem prometu. Od tod poimenovanje kar ni na papirju, ni materialno. To bi pomenilo, da *dematerializirani* vrednostni papir obstaja le kot ideja, ne tudi dejansko. V posameznih primerih elektronskih sporočil bi morali iskati funkcionalen izraz, ki bi opredeljeval tehnološke in pravne okoliščine posamezne vrste sporočil – listin, ne »elektronsko« enačiti z »nematerializirano« obliko. V resnici je elektronski zapis povsem povezan s snovno podstavo (Pavliha, Jerman-Blažič 2002, 21).

2.1 Zakon o elektronskem poslovanju in elektronskem podpisu v RS

Sporočanje pravno pomembnih in zavezujočih informacij v elektronski obliki ob pomanjkanju ustrezne zakonske ureditve, lahko znatno ovira in povzroča splošno pravno negotovost. Zato je nujno potrebno zagotoviti varno pravno okolje za elektronsko poslovanje v domačem in mednarodnem poslovanju.

Prvi zakon o elektronskih podpisih je bil sprejet že leta 1995 v zvezni državi Utah v ZDA. Komisija Združenih narodov za mednarodno gospodarsko pravo (UNCITRAL) je leta 1996 sprejela Modelni zakon o elektronskem poslovanju, v pripravi so tudi enotna pravila o elektronskem podpisovanju. Tudi druge mednarodne organizacije, vključno s Svetovno trgovinsko organizacijo (WTO), se ukvarjajo s podobnimi vprašanji.

V okviru evropskih zakonodaj o elektronskem podpisu je prva zakon o elektronskih podpisih sprejela Nemčija leta 1997, sledile so ji še nekatere druge države, med njimi Avstrija in Italija. Evropska unija je zato, da bi poenotila zakonodaje članic EU in za pospeševanje elektronskega poslovanja in uporabo elektronskih podpisov leta 1999 sprejela direktivo *Okvir Unije za elektronske podpise.* Njena določila so morale države članice izvršiti na nacionalni ravni do julija 2001. Direktiva obravnava vse vrste elektronskih podpisov in izpostavlja zlasti tiste, ki imajo enako pravno veljavo kot lastnoročni podpisi pri dokumentih v papirnati obliki (Jerman-Blažič 2001, 114).

Sprejem ustrezne zakonodaje v Republiki Sloveniji je bil zato nujno potreben za vključevanje v svetovno informacijsko družbo. Tako je slovenska vlada na predlog Centra za informatiko februarja 2000 sprejela predlog zakona o elektronskem

poslovanju in elektronskem podpisu ter ga poslala v obravnavo v Državni zbor, kjer je bil sprejet 13. junija 2000.

Slovenski zakon je tehnološko nevtralen, saj se tehnologija varovanja podatkov izrazito hitro spreminja. Trenutno samo digitalni podpisi na podlagi asimetrične kriptografije izpolnjujejo zahtevane pogoje kot varni elektronski podpisi.

Z novo ureditvijo se odpravljajo ovire, ki jih elektronskemu poslovanju postavljajo pravne norme, zasnovane in sprejete v času izključno papirnega poslovanja. Vzpostavlja se tudi varno okolje za preverjanje pristnosti elektronsko oblikovanih, shranjenih, poslanih, sprejetih ali kako drugače obdelanih podatkov.

Zakon o elektronskem poslovanju in elektronskem podpisu je razdeljen v pet poglavij, ki skupaj vsebujejo 55 členov[1].

V prvem poglavju zakon opredeljuje področje, ki ga ureja: elektronsko poslovanje ter uporabo podatkov v elektronski obliki in elektronskega podpisa v pravnem prometu ter določi pomen posameznih pojmov, uporabljenih v zakonu.

V drugem poglavju zakon ureja elektronsko poslovanje. Podrobneje je urejeno poslovanje z elektronskimi sporočili. Sledijo določbe, ki urejajo uporabo podatkov v elektronski obliki oziroma njihovo veljavnost in dokazno vrednost.

V tretjem poglavju zakon širše ureja elektronski podpis in delovanje overiteljev, ki so nujen pogoj za uporabo elektronskih podpisov. Vse overitelje in njihovo ponudbo storitev naj bi nadzoroval pristojni inšpektorat.

Ker gre za pomembno področje, kjer kršitev posameznih norm lahko resneje ogrozi zanesljivost elektronskega poslovanja in poseže v pravice drugih, so v četrtem poglavju določeni prekrški in kazni zanje.

Zadnje, peto poglavje, vsebuje prehodne in končne določbe. Zakon je bil v celoti usklajen z določili primarne evropske zakonodaje. Nekaj izvlečkov iz zakona o elektronskem poslovanju in elektronskem podpisu (Pavliha, Jerman-Blažič 2002, 11):

1. zakon zagotavlja elektronski obliki in elektronskemu podpisu enake možnosti kot dosedanji papirnati obliki,
2. za hranjenje podatkov v elektronski obliki je zelo pomemben tudi časovni žig, ki potrjuje, da so elektronski podatki resnično ostali celoviti in nespremenjeni od trenutka, ko so bili shranjeni, do trenutka uporabe,
3. zakon zato omogoča enostavno medsebojno priznavanje elektronskih podpisov znotraj Evropske unije ter širše priznavanje, ob pogojih vzajemnosti oziroma s tem povezane podobnosti področne zakonodaje,
4. če ni drugače dogovorjeno, se za kraj, od koder je bilo elektronsko sporočilo poslano, štej kraj, kjer ima pošiljatelj svoj sedež oziroma stalno prebivališče v

[1] ZEPEP – Zakon o elektronskem poslovanju in elektronskem podpisu št. 043-03/00-2/1 Ljubljana, dne 13.06.2000, sprememba zakona št. 043-03/00-2/2 Ljubljana, dne 27.02.2004.

času pošiljanja, za kraj prejema elektronskega sporočila pa kraj, kjer ima prejemnik sedež oziroma stalno prebivališče v času pošiljanja,

5. varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu glede podatkov v papirni obliki ter ima zato enako veljavnost in dokazno vrednost (Župan 2002, 39).

2.2 Pravna zmogljivost elektronskega sporočila

Pravna zmogljivost kakšnega sporočila je sestavljena iz vsebinske pravne relevantnosti in nevsebinskih sestavin, ki ga spremljajo. Vsebinska pomembnost ni povezana z elektronsko ali drugačno obliko, zato je E-sporočilo obravnavano z vidika nevsebinskih okoliščin, ki opredeljujejo njegovo pravno zmogljivost. Takšne okoliščine so: oblika izjave volje, zanesljivost, prepričljivost, verodostojnost, način podpisovanja, dokazna moč, način shranjevanja in ponovna uporaba. Število sestavin, ki določajo pravno zmogljivost e-pošte, je odvisno tudi od vrste posamičnega pravnega razmerja (Toplišek 1998, 57).

2.3 Pisnost in obličnost

Pri elektronskem poslovanju, če hočemo, da je neko pravno relevantno dejanje pravno zapisano, je treba izhajati iz pisnosti. Ta namen ima splošno ozadje, morda tudi posebno, tako kot izhaja iz narave konkretnega pravnega dejanja. Splošni namen vsake predpisane pisnosti je, da je zapis v telesni, neposredno zaznavni obliki in kot dokaz obstojen. Oboje je podlaga za pravno varnost.

V elektronskem poslovanju prihaja do zapletov, saj jih povzroča samo elektronsko poslovanje: odpravlja nekatere papirnate dele poslovanja, tisto, kar je napisano na elektronskih nosilcih in nato izpisano na papir, ni enako prepričljivo kot papirni izvirnik. Po 57. členu OZ[2] je zapis , če gre za pisno obliko, lahko na kakršnem koli sredstvu, ki omogoča, da se zanesljivo ugotovi vsebina izjave in kdo jo daje. Ob papirnati listini je povezava vsebine in podpisa očitna na pogled, pri elektronskem zapisu so lahko zaradi tehnoloških značilnosti vprašljivi elementi:

1. kaj je prava vsebina (pristnost),
2. kdo je podpisnik (istovetnost podpisnika),
3. ali je podpisnik podpisal pristno vsebino (poreklo listine).

Elektronskemu zapisu je potrebno v elektronskem poslovanju zagotoviti tehnološko, organizacijsko in pravno vnaprejšnjo verodostojnost. Ker lahko funkcije strožje

[2] OZ – Obligacijski zakonik – Ljubljana: Uradni list Republike Slovenije, 2003.

obličnosti zagotovimo tudi tehnološko, bo treba nekatere splošno uporabne tehnološke rešitve elektronskega poslovanja kriti z domnevami, ki bodo izhajale iz predpisa. Digitalno podpisano sporočilo velja kot pisno, ko nosi digitalni podpis, potrjen z javnim ključem, navedenem v veljavnem digitalnem potrdilu. Je veljavno, učinkovito in pravno zadostno, kot če bi bilo zapisano na papirju.

Videti je, da sta dva načina, kako dati elektronskemu sporočilu pravno veljavo pisnosti:

1. pri določeni vrsti sporočil – zlasti, če so podpisana digitalno – je mogoče vnaprej določiti, da se štejejo kot zapisana (na papir),
2. zakonske definicije pisnosti je treba oblikovati dovolj široko, da zajamejo tudi elektronski zapis.

Če je sporočilo podpisano digitalno, je njegova pristnost tako zanesljiva kot še pri nobenem doslej splošno uporabljenem načinu sporočanja (Toplišek 1998, 57).

E-poslovanje se ne bo moglo izogniti tudi pravnem pojmu obličnosti. Vprašanje je le, kako te zahteve izpeljati na papirnih nosilcih.

Ena od oblik elektronskega poslovanja je elektronska pošta, katero uporabljajo: za predhodne stike, za predpogodbe, za pogajanja, za izmenjavo dokončnih dogovorov, kot dopolnilno komunikacijo med izvedbo posla, ipd. Vse določene oblike so lahko predmet elektronskega poslovanja. Pogodba je sklenjena, ko se pogodbeni stranki sporazumeta o njunih bistvenih sestavinah (15. člen OZ).

Kdo daje izjavo, je običajno razvidno iz podpisa, lahko tudi iz drugih okoliščin primera (glava listine, žig, način zapisa ipd.). Na papirju in podobnih listinah so ti elementi sami po sebi vidni že na pogled. Pri elektronskih zapisih te vnaprejšnje razvidnosti in zaupanja ni. Zato so pri elektronskem poslovanju dokazovanje vsebine, pristnosti, istovetnosti podpisnika ipd. zahtevna vprašanja, ne glede nato, ali je oblika posla določena vnaprej ali ne. Marsikdaj je treba ugotoviti, ali elektronsko sporočilo sploh izpolnjuje pogoj pisnosti.

Za sklenitev dvostrankarske pogodbe je dovolj, da obe stranki podpišeta eno listino, ali da vsaka stranka podpiše tisti izvod listine, ki je namenjen drugi stranki (4. odst. 57. člena OZ).

V sodni praksi, ki je zadnja desetletja veljala v Sloveniji, srečujemo pretežno odločitve, ki so povezane s strogo obličnostjo (vrednostni papirji, dedovanje), zadeve o ponarejanju listin in vprašanje pogodb, ki so bile izpolnjene brez podpisa ali kakšnega drugega obličnostnega pogoja (veljavnost poslov po teoriji realizacije). To so področja, ki so v množičnem komercialnem poslovanju razmeroma redka. Toda vsak pravni posel mora biti vnaprej pravno zadosten, sicer trpi pravna varnost, negotove razmere pa slabo vplivajo na poslovanje. Zato je treba vprašanje oblike pisnosti in podpisa že vnaprej razjasniti, tudi ko gre za elektronsko poslovanje.

Razmišljati je treba, kako v elektronskem okolju zagotoviti funkcije, kakršne ima obličnost v posameznih vrstah primerov. Ob strogi obličnosti bo treba – potem ko bo preverjeno, ali je tolikšna strogost resnično potrebna – najti ustrezno »strogo« elektronsko obliko.

V najrazvitejših državah je raba e-pošte dosegla že tolikšen obseg, da resno pretresajo, ali so predpisane zahteve glede obličnosti in podpisovanja res potrebne oz. nujne v tako »absolutnih formulacijah«. V mnogih primerili gre za zahteve, ki so nastale v času peresa in črnila. Razmišljanja o spremembah gredo v te smeri:

1. po civilno pravnih predpisih je tudi elektronsko sporočilo listina (to trditev lahko izpeljemo iz (2. odst. 57. člena OZ).
2. ločiti je treba materialnopravni učinek in dokazno zmogljivost elektronske listine, ki se presoja prosto,
3. elektronski zapis se ne sme uporabiti za dokazovanje (kar ni odvisno od mnenja o tem, kakšna je dokazna zmogljivost elektronskega zapisa),
4. pri e-pošti (ali drugem e-sporočilu) ni treba iskati oblikovno podobnih rešitev, kot jih najdemo na papirju. Izhajati je treba iz funkcij, ki jih ima obličnost/podpis v določenem primeru, in potem iskati tehnološke, organizacijske, pravne rešitve,
5. v nekaterih primerih je dovolj, če izvirnik sestavimo na papirju, naslovniku pošljemo le elektronsko kopijo listine,
6. pravna zmogljivost elektronskega sporočila je lahko večja, če je pri njenem nastajanju, pošiljanju, izročanju, ipd. sodelovala verodostojna tretja oseba (ni nujno, da je zunanja, lahko je npr. neodvisen ločen oddelek, služba) (Toplišek 1998, 59).

2.4 Izjava volje po elektronski pošti

Elektronska pošta se uveljavlja za posredovanje pravno relevantnih sporočil. Izjava volje je v teoriji in sodni praksi dokaj obdelano področje, vendar vsa ključna mnenja o njej temeljijo na sporočanju s papirnim nosilcem (pismo). Ko so nastajali prvi evropski civilni ali trgovski zakoniki, še niso poznali nekaterih sodobnih sredstev za sporočanje oziroma je bila njihova civilno pravna uporaba majhna. Francoski Code civil je iz leta 1804, električni tokograf je Morse prikazal leta 1844, današnji telefon je Bell predstavil leta 1876, teleprinter so uvedli leta 1920 (Toplišek 1998, 61).

Drugi razlog zato, da se za nove načine sporočanja niso takoj pojavila posebna pravila, je tudi dejstvo, da pravo za nove oblike želi najprej uporabiti veljavna pravila iz sveta papirnega sporočanja.

Vsebina izražene volje je pri e-pošti praviloma v obliki besedila. Po tem se to sporočanje ne razlikuje od kakšne druge pisne oblike. Težava nastane, ko gre za spor o

obstoju ali vsebini sporočila, saj zaplete lahko povzročijo tudi tehnični razlogi na napravah, prek katerih pošiljamo oziroma prejemamo e-pošto.

Izjavo volje spremljata dve najpomembnejši sestavini: volja in izjava. Problematika volje ni odvisna od oblike izjave, saj gre za človekove zavestne miselne procese, ki jih vodijo razni motivi. V povezavi z e-pošto moramo opozoriti le na povsem možen primer napake volje, ki je posledica uporabljene tehnologije e-pošte. Sporočilo za elektronsko pošto najprej napišemo in nato z ukazom odpošljemo prejemniku. Nezaželeni položaji se lahko pojavijo v zvezi z odpošiljanjem. Ukaz za odpošiljanje e-pošte je lahko udarec na tipko ali klik z miško. Prenagljeno sicer lahko odpošljemo tudi pismo, vendar se to zgodi redko. Pošiljatelj e-pošte lahko celo spregleda, da je sporočilo odposlal, in sicer, če ga je napisal, in ga ni odposlal, ker ga še ni želel poslati, ali tega ni mogel storiti zaradi tehničnih težav z računalnikom oz. zaradi slabih povezav. Ob ponovnem zagonu programa za e-pošto se lahko zgodi, da program samodejno odpošlje še pripravljeno sporočilo, ki morda niti ni dokončano. Tak spodrsljaj mora pošiljatelj že vnaprej tehnično ali kako drugače preprečiti, da se izogne neprijetnim posledicam (Toplišek 1998, 62).

2.5 Sprejem ponudbe

Ponudba je sprejeta, tudi če naslovnik pošlje stvar ali plača ceno ali če stori kaj drugega, kar na podlagi ponudbe, prakse, vzpostavljene med strankama, ali običaja lahko šteje za izjavo o sprejemu. Sprejem učinkuje v trenutku, ko je bilo dejanje storjeno, če je bilo storjeno v rokih, ko ponudba še veže (2. odst. 28. člena OZ).

Pojem navzočnosti je povezan z možnostjo, da se druga stran takoj neposredno odzove in izrazi svoje mnenje glede pravno relevantnih okoliščin. Pri neposredni govorni povezavi (telefon, radio) je to očitno, medtem ko sta pojma »takoj« in »neposredno« pri teleprinterju, telefaksu in e-pošti predmet tolmačenja okoliščin dejanskega primera, praviloma gre za »enostransko« komuniciranje, ne za dialog, ki je značilen za posle med navzočimi. Položaj bi bil izenačen s telefonsko povezavo, če bi bila elektronska povezava med udeležencema neposredna, sprotna, hkratna. Tak primer je izvedljiv zlasti v zaprtih elektronskih okoljih, kjer so udeleženci pravno, organizacijsko in tehnološko opredeljeni in so ob normalnem poteku stikov izključeni zunanji posegi. (Cigoj 1984, 155).

Cigoj opozarja na povečano možnost tehničnih motenj pri napravah za prenos. Zaradi tega se hitreje zmotimo o osebi sogovornika, ali je sporočilo nerazumljivo oz. popačeno. Na splošno nosi tveganje za tehnične motnje tisti, za katerega se šteje, da komunikacijski organ (naprava) nastopa kot njegov posrednik.

Domnevo navzočnosti je treba pri e-pošti sprejemati, upoštevajoč vse okoliščine razmerja med obema stranema. Če gre npr. za stalno povezavo, kjer obe strani sproti

odgovarjata na e-pošto, bi lahko šlo za obliko razmerja med navzočimi. Na splošno bi od prejemnika težko zahtevali, da bo sproti pregledoval množico e-sporočil in nanje tudi takoj odgovarjati. Zato se glede e-pošte bolj nagibamo k trditvi, da gre načeloma za stik med nenavzočima osebama.

Čas, v katerem naj bi prejemnik odgovoril na ponudbo, je treba ocenjevati tudi skladno z običajnim načinom rabe e-pošte: tako pošiljatelj kot tudi prejemnik se ukvarjata s pošto v elektronskem nabiralniku takrat, ko utegneta. Prav to je poleg hitrosti privlačno pri e-pošti. Tehnološki razvoj komunikacij prinaša čedalje resnejše možnosti za neposredne, hkratne in sprotne dogovore med partnerji. Možen bo resničen dialog z dodatnim dokumentiranjem, ki ga bo omogočala večpredstavnost, zato bo treba vprašanje navzočnosti, ki je pravno zelo pomembno, pri novih tehnoloških rešitvah preverjati sproti. Tehnološko je pri e-pošti zanimivo, da je možno preprosto zagotoviti ujemanje ponudbe in sprejema (Toplišek 1998, 63).

2.6 Čas in kraj dogovora

Razmerje iz dane izjave nastane po prevladujoči prejemni teoriji, ko naslovnik prejme pošto. Pri e-pošti se sprašujemo, ali je to v času, ko pošta prispe v naslovnikov elektronski poštni predal, ali takrat, ko jo dejansko odpre in ima možnost, da jo prebere. Sama po sebi se ponuja primerjava s hišnim pisemskim predalom: tam načeloma velja, da izjava preide v območje naslovnika (da jo je naslovnik prejel), ko jo vržejo v poštni nabiralnik. Če nabiralnika ni ali naslovnik uporabo svojih naprav ovira, se vročitev izjave opravi tudi na kak drug način, ki po običajni poti omogoča, da naslovnik pošiljko opazi. Pri klasični pošti je možno govoriti tudi o neprimernem času dospetja izjave (npr. dostava v poštni nabiralnik ob 23. uri).

Pri e-pošti gre za sporočila, ki lahko v trenutku preidejo tudi več časovnih pasov in so dostavljena npr. sredi noči ali v nedeljo, zato si »neprimernega« časa ne moremo predstavljati. Tehnologija e-pošte je taka, da je možna dostava v elektronski predal ob katerikoli uri ali dnevu. Glede na ustaljeni, splošni način rabe e-pošte bi lahko domnevali, da je izjava z e-pošto prišla do naslovnika v razumnem času, v katerem je mogoče pričakovati, da bo naslovnik pošto pregledal. Pojem razumnega časa bo seveda drugačen, če gre za naključne udeležence ali za takšne, ki jim je e-pošta ustaljeni način dela oz. se za e-pošto izrecno dogovorijo. Pri poslih, v katerih je redno sporočanje z e-pošto potrebno tudi po večkrat dnevno, se udeleženci dogovorijo, kolikokrat na dan ali ob katerih urah so jo dolžni pregledovati. Tako morejo domnevati, da je druga stran vsa poslana sporočila prejela (Toplišek 1998, 64).

2.7 Dokazovanje z e-sporočilom

V elektronskem poslovanju mora vsakdo pravočasno ugotoviti, kakšno dokazno breme lahko pričakuje zase. Dokazno breme se še predhodno pomakne na drugega udeleženca. To je pogosto uporabljen način, s katerim se predhodno doseže pravno jasnejše razmerje. Pomik dokaznega bremena seveda ni vedno izvedljiv. Najlepši primer daje podpis. Lastnoročni podpis mora izpodbijati tisti, ki mu ne verjame. Z »elektronskim lastnoročnim podpisom« seveda ne bi bilo tako; kdor bi imel interes, bi lahko vnaprej izpodbijal njegovo pristnost, ki bi jo moral dokazovati podpisnik. Nasprotno digitalni podpis, narejen v tehnološko in pravno urejenem okolju, ustvari domnevo, da je pristen, in kdor tega ne verjame, nosi dokazno breme.

V kazenskem ali civilnem postopku utegne biti dokazovanje različno strogo. Če sta udeležena na pogled neenakopravna partnerja (npr. monopolni dobavitelj in potrošnik), bi morala močnejša stran dodatno pretehtati zmogljivost svojega elektronskega dokaza.

Če elektronskemu sporočilu priznamo, da more biti predmet dokazovanja, se problem v naslednjem koraku preseli na področje dokazne zmogljivosti. Kot glavno merilo dokazne zmogljivosti kake listine navajajo vprašanje, kako težko jo je ponarediti. Vprašanje dokazne uporabnosti ni aktualno le zaradi morebitnega dokazovanja s pomočjo elektronskega zapisa, temveč tudi zaradi možnosti, da se bomo prej, kot si lahko predstavljamo, srečali z elektronsko organiziranim sodnim postopkom. Tehnično je tak postopek že izvedljiv, manjka mu ustrezna tehnološka, organizacijska in seveda pravna infrastruktura. Verjetno se bo elektronsko poslovanje najprej razvilo v tistih delih postopkov, ki jih je možno avtomatizirati.

Med potjo elektronskega sporočila so udeležene različne osebe, različna oprema, različne programske rešitve; vsaka od teh sestavin lahko povzroči, da bo sporočilo manj verodostojno. Zgrešeno bi bilo, če bi pričakovali, da bodo problem neenakovrednosti papirne in elektronske listine uredili (izključno) pravni predpisi. Racionalni predpisi pravne države terjajo izvedljiva razmerja, zato je treba razmišljati o pravni izvedljivosti elektronskega sporočila. Uresničijo jo lahko predvsem tehnološki, organizacijski in drugi posegi.

UNCITRAL-ov vzorčni zakon v 5. členu določa, da sporočilu ne bodo odrekali pravne zadostnosti, veljavnosti ali zmogljivosti samo zato, ker je v elektronski obliki. Člen 9 se ukvarja izključno z *dokazno dopustnostjo in dokazno težo* elektronskega sporočila:

1. v katerem koli pravnem postopku nobena pravila dokazovanja ne bodo uporabljena tako, da bi se zanikala dopustnost elektronskega sporočila kot dokaza:
   - zgolj zaradi razloga, ker gre za elektronsko sporočilo,
   - da ne gre za izvirnik, če od osebe, ki dokaz predloži, ne moremo razumno

pričakovati boljšega dokaza,

2. informaciji v obliki elektronskega sporočila bo dana ustrezna dokazna teža. Pri presojanju dokazne veljave podatkovnega sporočila bo upoštevana zanesljivost načina, na katerega je bilo sporočilo narejeno, shranjeno ali poslano, kako je bila zagotavljana celovitost informacij, način, kako je bil ugotovljen pošiljatelj, in drugi pomembni dejavniki.

V pravnih postopkih prevladuje načelo proste presoje dokazov (npr. 8. člen ZPP[3]). Katera dejstva se štejejo za dokazana, odloči sodišče po svojem prepričanju na podlagi vestne in skrbne presoje vsakega dokaza posebej in vseh dokazov skupaj ter na podlagi uspeha celotnega postopka. Elektronsko sporočilo je lahko neposredno dokazno sredstvo (kot »listina« ali z ogledom), kot posredno sredstvo šele z zaslišanjem priče, strank ali izvedenca. Neposredno dokazovanje z elektronskim sporočilom zahteva določeno tehnološko infrastrukturo in usposobljenost zaposlenih pri organih, ki vodijo postopke.

Danes v pravnih postopkih obravnavajo listino predvsem kot predmet, na katerem je človekova misel izražena s pisavo. ZPP nima neposredne določbe o tem, kako obravnavati elektronske zapise, tudi ne določil, ki bi pojasnjevala njihovo dopustnost nasploh. Angleški predpis o dokazovanju v civilnih postopkih (The Civil Evidence Act 1968 in 1972) je že pred skoraj 30 leti predvidel pogoje, kdaj se sme dokazovati z listino, izdelano z računalnikom; poudarja zlasti pogoj, da je bila izdelana med rednim obratovanjem računalnika, da je le-ta deloval v redu, da morebitno nepravilno delovanje ni moglo vplivati na natančnost dokumenta in da dokazovana trditev povzema sporočilo. Ko dokument potuje do računalnika prek rok več oseb, zakon dovoljuje tudi pričanje katere izmed njih o dejstvih v računalniškem dokumentu. Vsak dokaz, izdelan računalniško, mora spremljati potrditev odgovorne osebe, da je dokument in način njegovega računalniškega nastanka prepoznala. Kot dokaz ni dovoljeno uporabiti računalniškega zapisa, ki bi izražal mnenje.

Slovenski ZPP zamuja pri urejanju elektronsko izvedenih dokazov. Tudi za elektronska sporočila je možno uporabiti delitev na javne in zasebne listine. Položaj javne listine bo imel npr. podatek iz javnega elektronskega registra (zemljiška knjiga, register podjetij...). Z javnimi elektronskimi »listinami« ne bo težav, ker pravila za njihovo izdelavo in uporabo že vnaprej izrecno opredeljujejo njihovo pravno uporabnost. Vprašanja pravne zmogljivosti se torej pojavljajo predvsem pri zasebnih listinah.

Ugotovljeno je, da je verodostojnost elektronskega sporočila ključni dejavnik dokazne moči sporočila. Obstajajo številne možnosti za potrjevanje pristnosti sporočila,

[3] ZPP – Zakon o pravdnem postopku št. 710-01/95-4/6, Ljubljana, dne 25.03.1999, sprememba zakona št. 710-01/95-4/16 Ljubljana, dne 25.10.2002, naslednja sprememba zakona št. 710-01/95-4/28 Ljubljana, dne 19.12.2003.

ki nedvomno kažejo poreklo sporočila in namen »podpisnika«, da naj bo njegovo sporočilo v določeni obliki. Če je namen potrditve pristnosti predpisan, je to treba upoštevati, pri čemer je včasih možno s tolmačenjem omogočiti tudi način potrditve pristnosti, ki ga zakonodajalec ni imel v mislih. Pomembno je, da se doseže namen predpisane avtentikacije. Največkrat je predpisani način podpis.

Pri digitalnem podpisovanju sta vsebina sporočila in podpis neločljivo povezana, zato je elektronsko sporočilo te vrste bolj verodostojno od papirnega. Ta okoliščina daje nekaterim misliti, češ da sploh ne bi bilo treba čakati na spremembe postopkovnih predpisov o zasebnih listinah. Če je infrastruktura pri uporabi digitalnega podpisa (tukaj mislimo na postopke v zvezi z registriranjem in izdajanjem podpisnih certifikatov) premišljena, je možno podpis kadarkoli preveriti. To dejstvo lahko v elektronsko poslovanje vnese pravno varnost. Zato je možno napovedati, da bo elektronski podpis, zlasti digitalni, odigral pomembno vlogo pri utrjevanju dokazne zadostnosti elektronskega sporočila. Prav z »elektronskim« podpisom bi lahko dosegli, da bi za elektronska sporočila uporabljali pravila o listinskem dokazovanju, ne postopkovna pravila o ogledu (Koželj 1995, 49).

Ko govorimo o elektronskem sporočilu, mislimo predvsem na zakon o elektronskem poslovanju in elektronskem podpisu v RS, na pravno zmogljivost elektronskega sporočila, pisnost in obličnost, izjavo volje po elektronski pošti, sprejem ponudbe, čas in kraj dogovora in dokazovanje z e-sporočilom. Gledano s strani zakonov so ta področja dobro pokrita, tako da obstajajo minimalne možnosti, pri katerih bi lahko kdo zlorabljal zakone.

3. ELEKTRONSKI NASLOVI

Elektronski naslovi zagotavljajo, da se udeleženci najdejo, zaradi tega se ukvarjamo z mednarodno usklajenim naslavljanjem. Elektronski naslov ima predvsem tehnični pomen, zaradi katerega sporočilo doseže pravi računalnik. Zato se v pravnih razpravah pojavlja tudi mnenje, da gre za številko, ki ima podoben namen, kot ga ima telefonska številka. Toda številni spori kažejo, kako je opisna oblika elektronskega naslova povezana z imenom organizacije, podjetja, z blagovno znamko ali s kakšnim drugim pravno relevantnim izrazom.

Zaradi potreb uporabnikov se elektronski naslov izraža opisno (npr. v obliki: vis@fm-kp.si), v tem primeru gre za naslov v *Sloveniji,* in sicer na *Univerzi na Primorskem* in fakulteti z okrajšanim imenom FM. Opisna oblika ni »prevod« številk v znake, temveč je izraz, ki je določeni številki dodeljen. Preslikava med številčnimi naslovi in med uporabniško zapisanimi naslovi se izvaja sproti na domenskih (imenskih) strežnikih. Glede nato, da je zgradba naslovov drevesno hierarhična, je takšna tudi zgradba imenskih strežnikov.

Čeprav je razporejanje številčnih naslovov in opisnih (domenskih) imen povsem usklajeno in marsikdaj poteka prek istih organizacij, gre za dve razmeroma ločeni področji. Če v tej razpravi naslavljanja izrecno ne omenjamo, imamo v mislili opisno (domensko) obliko naslavljanja. Večina pravnih vprašanj je povezanih prav z njo (Toplišek 1998, 73).

3.1 Dodeljevanje-registriranje elektronskih naslovov

Za Slovenijo je kot vrhnja internet domena določena dvočrkovna oznaka *.si.* Akademska in raziskovalna mreža Slovenije – ARNES je že od leta 1992 pooblaščeni register, pri katerem lahko upravičene organizacije registrirajo domeno oblike *domena.si.* Domena je naslov vaše organizacije na internetu, bodisi na predstavitveni strani (homepage) oblike *www.domena.si* ali v elektronskem naslovu oblike *ime.priimek@domena.si*.

ARNES ne registrira domen pod drugimi vrhnjimi domenami, npr. *domena.com, domena.org, domena.info, domena.at, ...*

Šolski zavodi registrirajo domeno pod domeno *edus.si*. Pravila za registracijo domen za šolske zavode določa Ministrstvo za šolstvo, znanost in šport, izpolniti pa morajo poseben formular za registracijo poddomen oblike *poddomena.edus.si*.

Registracija domene pod .si poteka v dveh korakih. Prvi korak je administrativni postopek, v katerem prosilec pridobi enolično ime oblike *domena.si*. Da bi domeno lahko uporabljali na internetu, je treba zanjo postaviti še *primarni in sekundarni DNS strežnik*. To je drugi korak in ga imenujemo aktiviranje domene. Ta pravilnik velja za

registracijo in aktiviranje domene oblike domena.si do 31.03.2005.

Spekter pravil za registracijo domen je pester že znotraj Evrope. Če gre za nacionalne vrhnje domene (country-code oz. ccTLD), je rešitev praktično toliko, kolikor je različnih držav. Pa vendar lahko vsaj na področju Evrope in severne Amerike govorimo o nekem skupnem trendu liberalizacije pravil za registracijo domen in temu trendu sledimo tudi z vrhnjo domeno .si.

Pravila za registracijo domen pod .si so bila na začetku izjemno stroga. Domeno je lahko registriral le slovenski poslovni subjekt, ime pa je moralo biti enako firmi oz. registriranemu imenu subjekta. Stroga pravila imajo kar nekaj prednosti: sama po sebi preprečujejo morebitne spore zaradi upravičenosti do domene kakor tudi spore v povezavi z blagovnimi znamkami, naslovni prostor je pregleden, domena pa »čaka« tudi na organizacije, ki bodo prednosti interneta odkrile kasneje. Večina evropskih registrov je na začetku delovanja dodeljevala domene pod svojimi nacionalnimi domenami po podobnih pravilih.

Z razširjenostjo interneta raste tudi potreba po večji fleksibilnosti pri registraciji domen. Stroga pravila imajo namreč slabost, da ne more vsakdo registrirati domene, ki so jo želi. Zato so že okrog leta 2000 posamezni uporabniki interneta v Sloveniji izrazili željo po sprostitvi pravil za registracijo domen. Arnes je odprl elektronski forum, na katerem so se zbirali predlogi in želje lokalne internetne skupnosti. Obenem se je posvetoval z zainteresirano strokovno in laično javnostjo, pravniki, strokovnjaki za intelektualno lastnino, Gospodarsko zbornico, Združenjem slovenskih ponudnikov internet storitev SISPA ter mednarodnim združenjem evropskih nacionalnih registrov CENTR. Na številnih predavanjih je predstavil možne sisteme za registracijo domen in zbiral mnenja. Rezultat posvetovanj je bil, da si večina želi, da bi bila pravila za registracijo domen pod .si bolj liberalna.

Konec leta 2001 je tako Arnes s sprejemom novih splošnih pogojev za registracijo domen pod .si naredil prvi korak proti liberalizaciji - sproščanju pravil. Upravičenci so lahko registrirali tudi domene za svoje blagovne znamke, maksimalna dolžina domen se je s 24 povečala na 63 znakov. V letu 2002 se je krog upravičencev razširil z mednarodnimi organizacijami, uvedena je bila tudi možnost začasne domene za projekt ali konferenco. Med uvajanjem postopnih sprememb je Arnes pripravljal celotno prenovo sistema za registracijo domen. Projekt je obsežen in zahteven, tako s stališča programskih rešitev kakor tudi s pravnega in administrativnega stališča. Proces liberalizacije je namreč enosmeren – ko enkrat narediš korak naprej, »poostritev« oz. vračanje na staro stanje ni več mogoče. Celotni proces liberalizacije kakor tudi novi sistem za registracijo domen je Arnes predstavil tudi na regionalnem forumu svetovalnega telesa mednarodne organizacije ICANN, ki ga sestavljajo vladni predstavniki posameznih držav (Governmental Advisory Commitee - GAC), ki je potekal v okviru srečanja ICANN od 2. do 6.marca 2004 v Rimu.

Po 4 letih priprav je Arnes novi sistem na srečanju 15.12.2004 predstavil tistim, ki so že doslej pomagali upravičencem v postopku registraciji in upravljali z imenskimi strežniki v imenu posameznih nosilcev domen. Arnes je prisotnim predstavil tako nova pravila kakor tudi tehnično izvedbo ter pojasnil način komunikacije med Arnesom in bodočimi registrarji. Prisotni so predlagane spremembe pozdravili in Arnesu posredovali tudi nekaj predlogov.

Novi sistem za registracijo domen pod .si bo stopil v veljavo 04.04.2005 ob 10:00, ki prinaša bistvene novosti:

1. Poljubne domene po principu »first come first served«, ki bodo (zaenkrat) obdržala enak krog upravičencev; domeno pod .si bodo torej še vedno lahko registrirali le slovenski poslovni subjekti in mednarodne organizacije kot doslej. Vendar pa ni več omejitev in zahtev glede same domene, ustrezati morajo le sintaktičnim pravilom, ki so v novih pravilih ostala nespremenjena. Vsak upravičenec bo torej od 04.04.2005 po načelu »first come first served« lahko registriral poljubno domeno, omejeno bo le maksimalno možno število domen na nosilca (20).
2. Druga bistvena novost je, da se s 04.04.2005 po priporočilu mednarodne organizacije ICANN ter po zgledu drugih nacionalnih registrov tudi v Sloveniji vzpostavlja sistem registrarjev. Doslej so nosilci domen domeno registrirali neposredno pri Arnesu. Arnes bo v novem sistemu obdržal le osnovne funkcije, ki jih mora opravljati register, vse ostale pa bodo prevzeli t.i. registrarji. Ti bodo dejansko posredniki med Arnesom kot registrom in nosilci domen (registranti). Kakšna bo vloga registrarjev? Registrarji bodo svetovali prosilcem v postopku registracije in jih seznanili s Splošnimi pogoji za registracijo, nato pa bodo v imenu stranke Arnesu na predpisan način posredovali vloge za registracijo in podaljševanje. Vsa komunikacija med Arnesom in nosilci bo, razen v izjemnih primerih, potekala izključno preko registrarjev.
3. Plačilo registracije domen in podaljšanje registracije je tretja večja novost, ki jo bo prinesel novi sistem. Doslej je bila ta storitev Arnesa brezplačna, kar v Evropi nikakor ni več običajno. Za domeno pod vrhnjo nacionalno domeno morajo plačevati nosilci po vsej Evropi in ostalem razvitem svetu, cene pa se gibljejo od nekaj evrov do par sto evrov letno.

   Po novih pravilih bodo nosilci registrirali domeno za eno leto, proti plačilu se bo registracija domen lahko letno podaljševala. Tudi plačila bodo potekala preko registrarjev: Arnes bo po enotni tarifi (ki bo določena po stroškovnem principu) transakcije zaračunaval registrarjem, stranke pa bodo plačevale registrarjem. Cene storitev registrarjev se bodo oblikovale prosto.
4. Arnes se je za razliko od nekaterih drugih registrov, ki so vpeljali sistem registrarjev, odločil, da ne bo postavljal visokih kriterijev za izbor registrarjev,

saj menimo, da bodo končni uporabniki oz. nosilci tisti, ki bodo potrdili in izbrali tiste,ki bodo najboljši oz. najbolj konkurenčni. Registrar bo tako lahko postal vsak slovenski poslovni subjekt, ki je nosilec domene pod .si in ima tehnično znanje in možnosti za komunikacijo (torej dostop do interneta) z Arnesom preko novega sistema. Z Arnesom bo podpisal pogodbo o sodelovanju za obdobje enega leta, ki jo bo lahko podaljšal, če bo v tem letu registriral oz. podaljšal registracijo vsaj 100-tih domen. Ker bodo plačila potekala preko registrarjev in bi Arnes v primeru neplačil moral oškodovati nosilce domen, bo sistem temeljil na predplačilih: vsak registrar bo na Arnesov račun nakazal avans. Opravljene transakcije se bodo odštevale, registrar pa bo svoje "stanje" lahko redno spremljal in po potrebi »račun napolnil«. Transakcije namreč ne bo mogel opraviti, če njegovo stanje na računu tega ne bo več dopuščalo.

5. Stroga pravila že sama po sebi v veliki meri preprečujejo spore zaradi domen. Z liberalizacijo pa se možnost sporov precej poveča, zato je Arnes v sodelovanju s pravnimi strokovnjaki razvil Postopek za alternativno reševanje domenskih sporov (ARDS). Postopek ARDS, h kateremu bodo zavezani vsi nosilci, registrarji in Arnes kot register, predstavlja hiter in poceni način reševanja domenskih sporov, ne izključuje pa možnosti, da se spori rešujejo preko sodnih postopkov.

   Za sprožitev postopka ARDS bodo morali biti izpolnjeni trije pogoji: domena mora biti enaka ali zamenljivo podobna znamki, nosilec domene nima pravice do te domene in domena je registrirana ali se uporablja v slabi veri. O sporih bodo odločali neodvisni razsodniki, Arnes pa bo zavezan, da odločitev izvrši.

Pred 04.04.2005 bodo seveda potekale pospešene priprave na vzpostavitev novega sistema.

Vloge po starih pravilih bo Arnes sprejemal do vključno 31.03.2005 do 12:00. Obravnavane bodo le popolne vloge, ki bodo do tega trenutka prispele na Arnes, vse ostale bodo zavržene. Zakaj je to pomembno? Vsi poslovni subjekti, ki še niso registrirali domen, ki so enake njihovemu registriranemu imenu ali njihovim blagovnim znamkam, vse občine in krajevne skupnosti, ki še niso registrirale domene za svoj kraj imajo do 31.03.2005 čas, da to storijo, saj jih »njihova« domena »čaka«. Po 04.04.2005 bo vsak upravičenec lahko registriral poljubno domeno, torej tudi domeno, ki bo blagovna znamka nekoga drugega ali domeno, ki bo enaka imenu kraja.

Sprememba sistema registracije bo vplivala tudi na nosilce domen, ki so bile (ali bodo) registrirane pred 04.04.2005. Vsi nosilci si bodo morali v določenem roku, ki bo objavljen, poiskati registrarja, ki bo Arnesu v bodoče sporočal vse spremembe v zvezi z njihovo domeno in v njihovem imenu tudi podaljšal registracijo njihove domene. Spisek registrarjev bo javno dostopen na Arnesovih domačih straneh brž, ko bodo podpisane pogodbe med Arnesom in registrarji.

Vse je pripravljeno tudi za naslednje spremembe pravil. Predvidoma v septembru 2005 se bo krog upravičencev do domene pod .si razširil s slovenskimi fizičnimi osebami, opuščeno pa bo tudi maksimalno število domen na upravičenca. Vse slovenske pravne in fizične osebe bodo torej lahko registrirale poljubno domeno. V prvi polovici leta 2006 pa bo domena .si na voljo vsakomur, torej tudi tujim pravnim in fizičnim osebam [URL: http://www.arnes.si/domene], 03.03.2005).

Iznajdljivi uporabniki so si registrirali domene z imeni zelo slavnih in priznanih podjetij, kot je npr. McDonald's, in nato izsiljevali nosilce le-teh, ki so bili za odkup te domene pripravljeni plačati tudi več deset tisoč dolarjev, kar je postalo znano pod angleškim izrazom »domain name grabbing«. Zlorabe so se vršile tudi med konkurenčnimi tekmeci, ko so podjetja registrirala domeno z imenom konkurenčnega podjetja in na takem strežniku objavljala informacije, ki so kvarile ugled konkurenčnemu podjetju. V takem primeru se je treba zateči k pravnim ukrepom, ki so včasih zapleteni in dragi, stranka v postopku je morda celo na drugem koncu sveta. Zato je priporočljivo, da podjetja poleg svoje regionalne domene registrirajo z istim imenom vsaj še različico .com.

Z namenom pospeševanja elektronskega poslovanja v EU so telekomunikacijski ministri, pristojni za telekomunikacije v državah članicah sprejeli namero o uvedbi nadnacionalne domene .eu, ki bi omogočala medsebojno identifikacijo med poslovnim subjekti držav članic EU.

Kadar so uporabniki pri kršitvah avtorskih pravic prisiljeni uporabiti pravna sredstva, je to smotrno najprej doseči v lastni državi. Zaželeno bi bilo, da bi sodišče lahko zahtevalo od lokalnih ponudnikov internetnih storitev preprečitev vidnosti spletnih strani, ki kršijo avtorske pravice. Čeprav odločitev sodišča še ni avtomatično veljavna v drugih državah, nekatere države tako odločitev že upoštevajo (Župan 2002, 34).

3.2 Zakonodaja v zvezi z dodeljevanjem elektronskih naslovov

Položaj imena fizične ali pravne osebe ureja imensko pravo. Po njem se osebe med seboj (pravno) razlikujejo. V širši pojem imena spadajo tudi psevdonim, nekateri dodatki k imenu (npr. plemiški), družinski grb, umetniško in skrajšano ime (to še posebej primerno za domeno). Če bo akademski naziv v domenskem imenu kazal, da gre za opravljanje dejavnosti, povezane z nazivom, tudi v drugi državi, se bo pojavilo vprašanje dovoljenja/licence za delo.

Imena pravnih oseb urejajo posebni predpisi (o družbah, društvih ipd.). Ime pravne osebe pripada pravni osebi, ne morebitnim družbenikom ali članom. Firma je ime, s katerim družba posluje. V imenu firme mora biti označba, ki napotuje na dejavnost družbe. Firma lahko ima dodatne sestavine, ki jo podrobneje označujejo. Te ne smejo

biti take, da spravljajo ali utegnejo povzročiti v zmoto glede vrste ali obsega poslovanja ali da bi prišlo do zamenjave s firmo ali znakom razlikovanja druge osebe ali bi kršile pravice drugih oseb. V Sloveniji mora biti ime firme zapisano v slovenskem jeziku, kar je ena najbolj kršenih določb Zakona o gospodarskih družbah (ZGD). Zakon omenja nedovoljene sestavine firme, rabo imena tuje države, rabo besede Slovenija in rabo imena zgodovinske ali znamenite osebe. Vse to bo potrebno uveljaviti tudi pri domenskih imenih[4]. Trgovsko ime je kot varovano dobrino omenjala že Pariška konvencija za varstvo industrijske lastnine iz leta 1883 (čl. 1, 2 in 8). Ime osebe oz. njen naziv v firmi tudi v domeni lahko doda učinek »dobrega imena«. Zato bi bila vsakršna lažna ali nedobroverna raba imena v domeni protipravna ali celo kazniva.

Tudi elektronski naslov je oblika nastopanja v pravnem prometu. Iz omenjenih primerov vidimo, da tudi vključevanje imen fizičnih ali pravnih oseb v domene ne bo vedno preprosto. Pri imenih moramo upoštevati možen javnopravni vidik (s predpisom določena pravila glede nastanka, spreminjanja, prenašanja, prenehanja, morebitno posebno varstvo skupine imen[5]). Če določenega vidika imena ne varuje poseben predpis, je možna odškodninska obravnava po obligacijskih predpisih.

Elektronski naslov je pomemben zaradi pravnega razkritja pošiljatelja oz. udeleženca poslovanja. Tudi pri elektronski obliki imena gre za način nastopanja v pravnem prometu. Ponudnik elektronskih storitev mora navesti svoje ime in naslov, pri združenjih in skupinah morata biti navedena tudi ime in naslov pooblaščenega zastopnika.

Načelo izključnosti firme v globalnem poslovanju bi moralo smiselno veljati tudi pri domenah, kjer to še posebej zahteva tehnologija enoličnega naslavljanja. Obvezno razločevanje po pravu, ki velja za firme, pokriva le območje države Slovenije, tako da še ni jasno, kako se bodo uporabljala imena firm, ki se ne razlikujejo od tistih v tujini. Ime druge firme mora biti ne le drugačno, ampak tudi tako drugačno, da ga ni možno zamenjavati. V primeru dveh podobnih firm bi se morala prilagoditi tista, ki je v sodnem registru prijavljena kasneje. Slovenski domenski registrator se pri vpisu domene opira na uradno registracijsko listino pravne osebe. S tem se vzpostavlja neposredna povezanost imena oz. firme in domene. Nejasna, odprta ostaja obveznost, da mora firma vedno vključevati tudi predpisano oznako odgovornosti (27. člen ZGD zahteva npr. oznako d.o.o. ali drugo oznako vrste družbe). Če je domena identična z vsebino firme (tudi če je skrajšana oblika), je možno trditi, da gre tudi ob nastopanju pod takšno domeno za obliko uporabe firme. Po tem ZGD bi morala celo skrajšana firma vsebovati

[4] Nedovoljene sestavine (17. člen ZGD) št. 001-06/92-1/3, Ljubljana 27.05.1993 so besede oz. znaki, ki nasprotujejo zakonu ali morali, ki vsebujejo znane blagovne ali storitvene znamke drugega in ki vsebujejo ali posnemajo uradne znake.

[5] Zakon o osebnem imenu, ime kot osebnostna pravica v 35. čl. Ustave, firmske določbe v ZGD, predpisi o akademskih in strokovnih naslovih...

oznako vrste družbe (odgovornost). Oznako odgovornosti bo možno uporabljati kot domensko sestavino, zaradi katere se bosta dve podobni (ali celo enaki) firmi po domeni razlikovali (npr. d.o.o. in d.d. enakega imena). To oznako bo možno uporabiti tudi za »daljšanje« prekratkih imen firm.

Po veljavnem slovenskem ZGD je možen vpis nameravane firme. To je zanimiva možnost tudi pri domenah. Ponekod v tujini jo izpeljujejo z registrirane domene in domene »na zalogo« (bodisi zaradi morebitne lastne rabe ali zaradi kasnejše prodaje tržno zanimive domene). Pri tem ne gre za rezerviranje imena, temveč za dokončno registracijo domene, ki je morda še ne nameravajo uporabiti.

Postopka za varstvo firme (23. čl. ZGD) ni možno neposredno uporabiti pri varstvu domen, zato bo treba, dokler o tem ne bo izrecnega predpisa, uporabiti civilnopravna pravila o imenih, pravila o blagovnih znamkah, konkurenčno pravo[6] ipd. V (14., 15., 16., 17. člen ZGD) določa pravila o imenih. Firma ne sme vsebovati imen ali znakov tujih držav ali mednarodnih organizacij. Uporaba besede *Slovenija* in označb države in lokalnih skupnosti. Besedo *Slovenija* ali njene izpeljanke in kratice je dovoljeno vnesti v firmo le z dovoljenjem Vlade Republike Slovenije. Dovoljenje Vlade Republike Slovenije oziroma pristojnega organa lokalne skupnosti je potrebno tudi za to, da se v firmi uporabijo besede, ki označujejo državo ali lokalno skupnost (npr. državni, republiški, občinski). Ime ali del imena zgodovinske ali druge znamenite osebe je dovoljeno vnesti v firmo le z njenim dovoljenjem; če je že umrla, z dovoljenjem njenega zakonca in sorodnikov do tretjega kolena v ravni vrsti ter staršev, če so še živi, ter z dovoljenjem ministra, pristojnega za upravo. Firma ne sme vsebovati besed oziroma znakov:

- ki nasprotujejo zakonu ali morali,
- ki vsebujejo znane blagovne ali storitvene znake drugega upravičenca,
- ki vsebujejo ali posnemajo uradne znake.

Raba krajevnih imen v domeni povzroča veliko sporov glede domenske rabe krajevnih imen, zlasti mest. To velja tudi za razne oblike političnih, državnih, oblastnih ozemeljskih enot (npr. občin). Gre za primere, ko se ime mesta uporabi kot domena zaradi poslovnih interesov, možni so tudi spori zaradi enakih imen krajev ali zato, ker ima kaka oseba isto ime kot kraj.

Imena oseb javnega prava pri varovanju svojega imena seveda ne bodo mogle uporabiti pravil o varstvu pred nelojalno konkurenco, ampak bodo morale uporabiti splošna civilnopravne predpise (v Sloveniji splošna odškodninska pravila ali poseben

[6]Zakon o varstvu konkurence, UL RS 18/1993.

predpis, ki ureja posamezno vrsto imena – npr. za občino, državo ipd.). V Sloveniji namreč ni predpisa, ki bi civilnopravno neposredno posebej varoval ime[7].

Domeno kot obliko nelojalne konkurence je poleg splošnega civilnopravnega varstva domenskega imena možno varovati tudi po pravilih varstva pred nedovoljeno konkurenco. Takšno varstvo je možno zlasti ob neupravičeni uporabi imena, firme, znamke ali kakšne druge oznake. Ni pomembno, ali gre pri tem hkrati tudi za sestavine varstva intelektualne lastnine, dovolj je že dejstvo, da sporna raba utegne povzročiti zmedo na trgu. Zaradi takšne utemeljitve npr. v Nemčiji niso dovolili registrirati domene banhof.de (kolodvor.de). Dodatek vrhnje domene COM namreč sam po sebi ni dovolj, da bi se celotno domensko ime na trgu razlikovalo od podobnih.

Verjetno se bodo sčasoma oblikovala pravila, ki bodo varstvo imen, znamk, lojalne konkurence ipd. izrecno razširila tudi na meta – podatke v spletnih dokumentih. To ne bo preprosto in najiznajdljivejši bodo do takrat že iznašli nove načine za obvladovanje trga. Za zdaj je to vprašanje najbolje obravnavati po pravilih o nepreučevanju nelojalne konkurence, ne po pravu znamk ali po imenskem pravu.

Pri obravnavanju domenskih sporov je zanimivo tudi vprašanje krajevne pristojnosti. Poleg drugih splošnih pravil bi bilo v tem primeru možno uporabiti tudi navezno okoliščino domenskega registra. To pomeni, da bi bilo načeloma za vse spore domenskega prostora SI pristojno slovensko sodišče. Tudi nemško sodišče je izreklo, da so za vse spore v povezavi z domeno DE pristojna nemška sodišča. Možno je seveda tudi povezovanje z drugačno pristojnostjo. Berlinsko sodišče se je npr. razglasilo kot pristojno zato, ker je bilo sporno domeno možno priklicati na območju tega sodišča (navezna okoliščina je bila torej kraj storitve možnih posledic). Kadar gre za nevarnost zamenjave imen v ožjem pomenu (zamenjava identitete), ni mogoče upoštevati ugovora, da gre za različne dejavnosti strank v sporu. V omenjenem berlinskem primeru se je sodišče tudi vprašalo, ali za kršitev imena ni morda sokriv tudi registrator DE-NIC, ki je nameraval registrirati različice izpodbijanega imena. Na podlagi splošnih pogojev poslovanja te organizacije je sodišče ugotovilo, da je po pravilih DE-NIC za izbiro domenskega imena odgovoren imetnik (Toplišek 1998, 82).

3.3 Trgovanje z elektronskimi naslovi

Prenos poslovnega imena ali blagovne znamke je pravni posel, ki je bil znan že pred pojavom elektronskega poslovanja. Tako se npr. po slovenskem ZGD firma lahko prenese samo skupaj s podjetjem (24. člen). Posebnost, ki je posledica slabo usklajenega dodeljevanja domenskih imen, je da so mnoge domene registrirali iz špekulativnih

[7]Pravica do imena obravnava v članku Denarna odškodnina za negmotno škodo zaradi okrnitve osebnostne pravice, N. Betetto. PP 21/97, 25.

razlogov, da bi jih ob ugodni priložnosti (tudi z izsiljevanjem) prodali[8]. Cena je seveda višja od registracijske pristojbine. V Sloveniji taki primeri še niso znani (tudi sistem dodeljevanja domen to v veliki meri izključuje), v državah, kjer so prvi spoznali izjemne možnosti interneta, pa vlada prava registracijska mrzlica.

Tudi podjetja, ki še nimajo do popolnosti vpeljanega elektronskega poslovanja in še ne poslujejo po internetu, se bojijo, da bi kdo pred njimi registriral domensko ime, ki bi bilo podobno njihovemu. Registrirajo celo domene, katerih edini namen bi utegnil biti, da bi se prek njih bojevali proti drugi firmi/organizaciji. Razlogi so lahko politični, etični, predvsem poslovni (nezadovoljni potrošniki, nasprotniki nameravane združitve dveh podjetji, boj proti monopolu na trgu ipd.). Taka domena seveda ustrezno izziva ali celo žali, čeprav je danes takih podjetji vedno manj.

Slovenski registrator nima izrecno oblikovanih pravil za prenos domene na drugega upravičenca. Navodila nemškega DE-NIC pravijo, da dodeljena domena ni last, temveč je le dodeljena v uporabo. Z njihovim soglasjem se lahko prosto prenese na drugega imetnika. Soglasje lahko zavrnejo, če obstajajo razlogi, zaradi katerih tudi registracija ne bi bila možna (če bi bil npr. pridobitelj nekdo, ki nima sedeža/prebivališča v Nemčiji), ali zaradi kakšnega drugega pomembnega razloga. Stari in novi imetnik solidarno jamčita za morebitne obveznosti imetnika v trenutku prenosa. DE-NIC lahko brez odpovednega roka prekliče soglasje za prenos, če novi imetnik grobo krši pravila za dodeljevanje ali druge pogodbene obveznosti, ali če je na podlagi pravnomočne sodne odločitve oškodoval pravice tretjih, ali če je domeno uporabljal tako, da je znatno kršil predpise (Toplišek 1998, 98).

Kot je razvidno iz zgoraj navedenega, je zakonodaja na področju elektronskih naslovov v Sloveniji dobra. Obstajajo pravila in objektivni predpisi za dodeljevanje elektronskih naslovov. V Sloveniji je glavni upravljalec domenskega prostora vrhnje domene »SI« ARNES. Sprejeta je bila zakonodaja v zvezi z dodeljevanjem elektronskih naslovov. Imensko pravo določa položaj pravne ali fizične osebe, kar pripomore pri dodeljevanju imen. Določanje firme ali imena pravne ali fizične osebe ureja imensko pravo, ki pomaga pri dodeljevanju imen. Po ZGD je možen tudi prenos imena firme in s tem tudi domene.

V tujini se pojavlja posebnost, ki je posledica slabo usklajenega dodeljevanja domenskih imen. Prihaja do tega, da so domene registrirali iz špekulativnih razlogov le zato, da bi jih ob ugodni priložnosti (tudi z izsiljevanjem) prodali, po višji ceni. V Sloveniji taki primeri še niso znani (tudi sistem dodeljevanja domen to v veliki meri izključuje), v državah, kjer so prvi spoznali izjemne možnosti interneta, pa vlada prava

[8] V Veliki Britaniji je sodišče prepovedalo uporabljati nekaj domen, ker so pomenile ime podjetja ali blagovno znamko. Registriralo jih je podjetje, katerega osnovna dejavnost je bila registriranje in prodaja domen. V podobnem, danskem primeru, je sodišče presojalo po predpisih o nelojalni konkurenci.

registracijska mrzlica. Tako lahko trdim, da je področje v zvezi z elektronskimi naslovi v Sloveniji dobro pravno opredeljeno in z ustreznimi zakoni, zakonsko urejeno.

4. VARSTVO PODATKOV V ELEKTRONSKI OBLIKI

Nadaljnji vidik obravnave zaščite podatkov zadeva zbiranje podatkov o uporabnikih. Po slovenski ustavi ima vsakdo pravico do varstva osebnih podatkov, torej, da sam odloča, kdaj, komu in v kakšni obliki bodo sporočeni podatki, ki se nanašajo nanj. Ta pravica z vstopom na internet nekako zbledi. Seveda so podatki, zbrani v elektronski obliki, z vstopom na internet na voljo drugim brez vedenja tega, ki ima take podatke zbrane v elektronski obliki (Jerman-Blažič 2001, 182). Ob obisku spletnega mesta se avtomatično prenesejo nekateri podatki o obiskovalcu na obiskani strežnik, ki si jih v večini primerov zapiše med svoje statistične podatke. Nekatere države zakonsko regulirajo zbiranje podatkov o posameznikih in predpisujejo, da mora zbiralec svojo dejavnost prijaviti, seznaniti ljudi z vrsto podatkov in namenom njihovega zbiranja, omejene so možnosti distribucije teh podatkov, posamezniku je dana pravica, da pogleda v podatke o sebi in v nekaterih primerih lahko prepove njihovo zbiranje.

Pravna praksa na tem področju v EU in ZDA se precej razlikuje. V ZDA je skrb za podatke prepuščena posameznikom, v EU so za podatke odgovorni zbiralci. EU prepoveduje izvoz arhiva podatkov o državljanih EU v države z nižjo stopnjo zaščite, torej tudi v ZDA.

V Sloveniji nemalokrat vidimo, da se pojma varstvo in zaščita podatkov uporabljata kot sopomenki, kar je nepotrebno in zavajajoče. Iz vsebinske povezave kmalu ugotovimo, da se v teh primerih prepletata pojem pravnega varovanja in pojem tehnične/tehnološke zaščite podatkov. Čeprav zlasti raba angleških izrazov ni vedno dosledna, v tujih jezikih najdemo izraze, ki oba pojma funkcionalno razlikujejo (data protection = pravno varstvo podatkov, in na drugi strani data security = zaščita, tehnično varovanje, zavarovanje).

Če bomo v slovenščini uveljavili različna izraza za ti dve področji, lahko prispevamo k jasnejšemu obravnavanju problema in vsakemu avtorju ne bo treba vedno znova opredeljevati posameznih pojmov. Do nefunkcionalne zamenjave pojmov varstvo in zaščita prihaja tudi pri prevajanju, zlasti iz angleškega in srbskega jezika (Toplišek 1998, 101).

4.1 Pravno varstvo elektronskih vsebin

Pravno varstvo podatkov v elektronski obliki ureja drugo poglavje, predvsem pa 12. in 13. člen ZEPEP[9]. 12. člen ZEPEP določa, kateri elektronski podatki se lahko hranijo

[9] ZEPEP – Zakon o elektronskem poslovanju in elektronskem podpisu št. 043-03/00-2/1 Ljubljana, dne 13.06.2000, sprememba zakona št. 043-03/00-2/2 Ljubljana, dne 27.02.2004.

in pod kakšnimi pogoji. Različni zakoni zahtevajo hrambo dokumentov, ZEPEP razširja to možnost na podatke v elektronski obliki. V Uradnem listu RS, št. 39/00 je objavljen zakon o javnih naročilih, ki od naročnika zahteva, da mora hraniti dokumentacijo najmanj toliko časa, kolikor trajajo pogodbeni roki o izvajanju posameznega javnega naročila. Ker so danes skoraj vsa javna naročila v elektronski obliki, kar omogoča ZEPEP, bi bilo nelogično, če bi hramba potekala v pisni obliki. Zakon izenačuje obe obliki, papirno in elektronsko, in tudi določa elektronsko hrambo dokumentacije. V prvem odstavku tega člena ZEPEP določa pogoje, kdaj se lahko določeni dokumenti in zapisi hranijo v elektronski obliki. Predvsem so to tisti podatki v elektronski obliki, ki so dosegljivi in primerni za kasnejšo uporabo. Ti podatki so poslani ali sprejeti. ZEPEP dopušča, da se podatki hranijo v spremenjeni obliki. Tretja alineja prvega odstavka 12. člena se nanaša na informacije, ki jih je treba shraniti, ne glede na vsebino podatkov, ne glede na izvor, čas in kraju nastanka, ter komu so bili podatki, oziroma sporočila poslana. Najpomembnejši pogoj za hranjenje elektronskih podatkov je zapisan v četrtem odstavku tega člena, ki zahteva zanesljivo jamstvo o nespremenljivosti sporočila na podlagi uporabljene tehnologije. ZEPEP v tem členu elektronsko obliko implicitno izenači s papirno, ker pravi, da je tako hranjenje podatkov enakovredno.

13. člen eksplicitno izenačuje elektronsko obliko s papirno in določa, v katerih primerih določila tega člena in ZEPEP ne veljajo. Prvi odstavek je prepis 6. člena UNCITRAL-1, ki govori o veljavnosti podatkov v elektronski obliki. Oblika zapisa pri sklepanju poslov v pravnem prometu ponavadi ni določena z zakonom. Namen oblike je varstvo veljavnosti pogodbe, včasih zakon želi zavarovati stranko pred nepremišljenim dejanjem. V tem smislu gre verjetno obravnavati darilno pogodbo, pri kateri je oblika potrebna, če darovalec podarjeno stvar ali pravico ni takoj prenesel na obdarjenca, da z njo prosto razpolaga (538. člen OZ). ZEPEP v tem členu izenačuje papirno obliko in elektronsko, vendar postavlja dodatne pogoje. Gre za objektiven kriterij, ker morajo biti sporočila dosegljiva, da bi bila uporabna tudi kasneje. To pomeni, da morajo biti sporočila berljiva in da jih je možno interpretirati. Na drugi strani termin *dosegljiv* tudi pomeni, da je treba imeti programsko opremo, ki bo lahko prikazala takšno sporočilo. Termin *uporabna* se ne nanaša zgolj na uporabnost, temveč tudi na računalniško procesiranje. V tem členu so naštete tudi izjeme, kdaj elektronska oblika ni izenačena s papirno. Gre za pomembne pravne posle, pri katerih želi zakonodajalec zavarovati stranko in tudi pravni promet[10]. Poleg tega ZEPEP tudi zaradi tehnične plati ne dovoljuje elektronske oblike zapisa pri vseh tistih poslih, za katere je za veljavnost potreben notarski zapis (Pavliha, Jerman-Blažič 2002, 62).

[10] Stranke razpolagajo s svojim premoženjem v primeru določenega dogodka, npr. poroke, smrti.

Na področju računalniških programov je Slovenija prevzela določbe Direktive EU o pravnem varstvu računalniških programov iz leta 1991. Zaščita računalniških programov je opredeljena v členih od 111 do 117 ZASP[11]. Varujejo se algoritmi, programska dokumentacija, sestavni deli in naslov računalniškega programa.

Pogoje proste uporabe avtorskih del, ki se nanašajo predvsem na pridobivanje informacij javnega značaja, kot so obveščanje o dnevnih dogodkih, dnevne novice in vesti, ki imajo naravo tiskovnih s poročil, in izobraževanje ter zasebno razmnoževanje določajo členi 48 do 57 ZASP.

Računalniški program je zavarovan z zakonom pod pogojem, da je le-ta individualno delo v smislu intelektualne storitve. Avtor ima tako izključno pravico do razmnoževanja celotnega programa ali njegovih sestavnih delov, priredbe, predelave in posredovanja. Te pravice se z licenčno pogodbo lahko prenesejo na drugo osebo.

V 166. členu zakona (ZASP) se posebej obravnavajo kršitve avtorskih pravic, ki temeljijo na proizvodnji, uvozu, posedovanju, distribuciji, dajanju v najem kakršnihkoli sredstev, katerih namen je neupravičeno odstraniti ali obiti zakonito zaščito (računalniški program, tehnično napravo, požarni zid), ki preprečuje nepooblaščeno uporabo.

Za globalno elektronsko poslovanje je pomembno varovanje elektronskih avtorskih del v tujini in v zvezi s tem položaj tujcev pri nas. ZASP daje glede teh razmerji odgovor v osmem poglavju (čl. od 176 do 183). Na podlagi teh členov ali mednarodne pogodbe, bi lahko dokazovali, da med državama obstaja dejanska vzajemnost. Najpomembnejše je načelo nacionalnega tretmaja (5. člen Bernske konvencije), po katerem so tujci izenačeni z domačini. Ne glede na te določbe tujec uživa vse moralne pravice (zlasti imenovanje avtorja). Varstvo uživa tujec, ki svoje delo prvič objavi v Sloveniji, ali v 30 dneh od dneva, ko ga je objavili v tujini. Nasploh se za kršitve uporablja pravo države, za katero se zahteva varstvo (Jerman-Blažič 2001, 175).

4.2 Tehnično varovanje in zaščita podatkov

Osnovne zahteve za varno elektronsko poslovanje so: zaupnost, neokrnjenost, verodostojnost in avtorizacija. S pomočjo tehnologije lahko izpolnimo vse štiri zahteve, vendar je od posameznikov v procesu elektronskega poslovanja odvisno, kako se bo upoštevalo posamezno zahtevo. Pravilno in uspešno tehnično varovanje informacijskega sistema temelji na hierarhiji varnostnih sistemov in mehanizmov, ki je sestavljena iz varnostne politike, fizičnega varovanja, opredeljenih pravic dostopa, varovanja dostopa, varovanja podatkov in nadzora nad varnostnimi mehanizmi. Vsak sloj varnostne

[11] ZASP – Zakon o avtorskih in sorodnih pravicah št. 120-01/94-1/26, Ljubljana 09.04.2004.

hierarhije je odvisen od slojev pod njim. Če nižji sloji niso varnostno dovolj definirani in postavljeni, tudi gornji ni ustrezno varovan. Najnižja raven je varnostna politika, ki je temelj celovitega pristopa k varnosti informacijskega sistema. Zajema vse dejavnike, ki bi lahko kakorkoli vplivali na varno in zanesljivo delovanje celotnega računalniškega omrežja in sistema. Obsega fizično in tehnično varovanje in tudi pravila, ki določajo načine varovanja – kaj se sme in kaj ne (Štrakl 2001, 16).

Odprti sistemi in omrežja so varnostnim vprašanjem v informacijski tehnologiji dali dodatno težo. Prost pretok podatkov v infrastrukturi informacijskih sistemov, ki med seboj komunicirajo, omogoča vedno nove možnosti zlorabe (prestrezanje informacij, kraja podatkov itd.) ali manipulacije s podatki (poneverba, lažna identiteta itd.). Varnostna tehnologija poskuša škodljive posege onemogočiti in zagotoviti varno uporabo informacijskega okolja. Še posebej kritična področja, na katerih je varnostna tehnologija tudi ključna, so številni poslovni ali upravni procesi in postopki različnih varnostnih organov, ki sicer za svoje potrebe pogosto uporabljajo nestandardizirano tehnologijo in so ločeni od javnih informacijskih tokov. Varnostna tehnologija ni pomembna zgolj pri zaščiti vsebine pred vpogledom s strani nepooblaščenih. Ista tehnologija omogoča preslikati določene formalne postopke v popolno elektronsko obliko (Kuščer 2004, 60).

4.3 Varstvo in zaščita intelektualne lastnine

Pri avtorskem delu so zelo pomembne oznake avtorstva. Pri tem ne mislimo le na znak ©, temveč na tehnične rešitve, s katerimi so v elektronskem delu vneseni podatki o avtorju in vseh drugih možnih pravicah in omejitvah na tak način, da povprečen uporabnik oznak ne more odstraniti. Takšne tehnične rešitve bodo omogočile celo samodejno licenciranje. Kljub temu bo treba odgovoriti še na vrsto izvedbenih vprašanj:

1. digitalni objekti za označevanje pravic intelektualne lastnine bodo morali delovati v vseh elektronskih okoljih (standardizacija),
2. njihovi metapodatki bodo morali biti verodostojni, kar je podobno kot pri certificiranju digitalnih podpisov,
3. digitalna dela se včasih gibljivo spreminjajo, zato se postavlja vprašanje, kako bo z oznakami pri sestavljenih delih in pri tistih, ki »nastajajo« na zahtevo.

Razvijajo se tehnike digitalnega vodnega znaka (tatooing), ki lahko pomembne avtorske podatke skrijejo v sliki ali drugi vsebini. Pri tem se bo včasih pojavil interes, da bi uporabnik nekatere podatke lahko videl, druge ne. Možne so razčlenjene oznake, različne na posameznih skupinah kopij. S tem bodo lahko sledili kopijo, ki bo pri določenem uslužbencu ali kupcu (dokaz edinega možnega vira). Učinkovit vodni znak bo ostal uporaben tudi ob predelavi in ponovnem skeniranju.

Že sedaj je možno z iskalnimi sistemi po internetu izslediti marsikatero nezakonito uporabljeno delo. Če bodo ti sistemi programirani za iskanje skritih oznak v elektronskih delih, bo odkrivanje še lažje.

Za zakrivanje vsebine so najuporabnejše šifrirne tehnike. Digitalno podpisovanje je možno uporabiti, kadar je treba zavarovati celovitost vsebin ali shraniti avtorsko delo pri nepristranski osebi. Če se uporabi skupinski ključ, se določi najmanjše število oseb, ki morajo sodelovati pri razkrivanju podpisa.

Po 166. členu ZASP pomeni posebno kršitev pravic, če neka oseba krši izključne pravice po tem zakonu, kadar proizvede, uvozi, distribuira, proda, da v najem, oglaša za prodajo ali najem ali poseduje za gospodarske namene tehnologijo, napravo, proizvod, sestavni del ali računalniški program ali opravi storitve, ki:

- se promovirajo, oglašujejo ali tržijo z namenom, da se izogne dejanskim tehničnim ukrepom,
- imajo majhen gospodarski pomen ali uporabnost za druge namene.

»Tehnični ukrepi« po tem členu pomenijo vsako tehnologijo, napravo, proizvod, sestavni del ali računalniški program, ki je ob običajnem delovanju namenjen preprečevanju ali oviranju dejanj, ki jih imetnik pravic po temu zakonu ni dovolil. Ta člen se smiselno uporablja tudi za tehnologijo, napravo, proizvod, sestavni del ali računalniški program, s katerim se odstranijo ali spremenijo elektronski podatki za upravljanje pravic.

Avtorje oz. lastnike del lahko varujejo tudi sistemi za obračunavanje rabe. Nekateri menijo, da se bo v prihodnosti zaradi sprotnih sistemov obračunavanja zmanjšal pomen organizacij, ki danes skrbijo za kolektivno uveljavljanje avtorskih pravic (nem.: Verwertungsgesellschaft; gl. člen od 146. do 163. ZASP).

Očitno je torej, da bodo avtorji elektronskih del lahko izbirali med vrsto tehničnih ukrepov, ki bodo varovali njihove pravice. S skupnim imenom jih angleško imenujejo ECMS: Electronic Copyright Management Systems (Jerman Blažič 2001, 165).

4.4 Predelava javno dostopnih podatkov

S pomočjo informacijske tehnologije je možno nabirati splošno dostopne podatke, ki sami po sebi ne pomenijo osebnega podatka ali vsaj ne spadajo v skupino posebej varovanih »občutljivih podatkov«. Največ jih najdemo v javno dostopnih imenikih, seznamih, registrih ipd. Sem lahko štejemo tudi podatke, ki jih posamezniki sami, po svoji volji razkrivajo javnosti (npr. javna objava na spletni strani ipd.). Tudi pri telefonskem imeniku je videti, da gre za podatke, ki so bili brez omejitev dani na voljo javnosti, vendar tudi zanje veljajo pravila informacijske zasebnosti iz telekomunikacijskih predpisov.

Primer take sestavljene zbirke, ki je zelo razburil javnost, je *P-TRAK*, ki jo je objavil ameriški informacijski sistem Lexis-Nexis[12]. Tam je možno najti ime in priimek, telefonsko številko, sedanji in do dva prejšnja naslova, včasih so dodani tudi dekliški priimki; številko socialnega zavarovanja so umaknili po prvih protestih. V Evropi take zbirke najbrž ne bi nikjer dopustili. Pri Lexisu so se izgovarjali, češ da gre za splošno dostopne (javne) podatke in da morejo do njih le naročniki sistema, ki so večji del odvetniki in drugi pravniki, bančniki in drugi poslovneži, uradniki, policija, socialno skrbstvo ipd. Tej ugledni druščini se seveda lahko pridruži vsakdo, če plača pristopnino.

P-TRAK je primer, s kakršnim se bomo verjetno srečali tudi v Sloveniji. Do takih javno dostopnih osebnih podatkov, iz katerih bi bilo možno sestaviti novo donosno zbirko, namreč ni težko priti.

Za nabiranje osebnih podatkov so postala še posebej hvaležna odprta elektronska okolja. Tako npr. lahko kot člani e-liste prikličemo seznam elektronskih naslovov, ki jih je možno prodati ali kako drugače koristno uporabiti, saj le redke liste tega ne omogočajo.

Menimo, da je tudi takšne zbirke treba obravnavati po predpisih o varstvu osebnih podatkov (Toplišek 1998, 114).

4.5 Pravni okviri za zagotavljanje informacijske varnosti

V celostnem procesu elektronskega poslovanja posamezni udeleženci ne morejo delovati brez pravil. Uspeh njihovih dejanj je v veliki meri odvisen od globalno dogovorjenega okvira, ki je zgrajen na industrijskih standardih, v okolju javnega pravnega reda in ureditvenih predpisov. Za vzpostavitev urejenega trga brez ovir in razdrobljenosti je pomembno, da udeleženi subjekti elektronskemu poslovanju zaupajo in se nanj zanesejo. Ustrezna zakonodaja omogoča varno izvajanje elektronskega poslovanja, vendar ne samo v posamezni državi, temveč tudi preko državnih meja. Zato je nujno zagotoviti pravno varnost elektronskega poslovanja v domačem in mednarodnem poslovanju, pri čemer je potrebno upoštevati interese proizvajalcev, prodajalcev in kupcev. Zakonodaja, ki ureja področje elektronskega poslovanja, mora biti čimbolj jasna in predvidljiva, podpirati mora konkurenčnost ter jasno določati ravnotežje med svobodo izražanja, varovanjem osebnih in javnih interesov s posebnim poudarkom na varstvu potrošnika. Vzpostaviti se mora takšen pravni okvir, ki mu bo potrošnik zaupal, poslovni svet pa spodbujal k vlaganju in razvoju (Jerman Blažič 2001, 162).

[12] Podatke iz zbirke P-Trak kupujejo od bonitetne agencije Trans Union. credit reporting bureau. Gl. <http ://www. privacyrights org/ar/ptrak. html>.

Po Ustavi Republike Slovenije ima vsak pravico do varstva osebnih podatkov kar je opredeljeno v ZVOP[13] in možnost da razpolaga z njimi. Torej sam odloča kaj, komu, v kakšni obliki bodo sporočeni podatki, ki se nanašajo nanj. Ob obisku spletnega mesta se nekateri podatki o obiskovalcu avtomatično prenesejo na obiskani strežnik, ki si jih v večini primerov zapiše med svoje statistične podatke, lahko pa jih uporabi tudi za nedovoljeno ravnanje z njimi. Take kršitve je težko nadzorovati in glede na to, da je vedno več uporabnikov internetnih storitev, si lahko predstavljamo kakšno bazo osebnih podatkov si lahko nekdo ustvari.

V Sloveniji preži največja nevarnost zlasti pri zbirkah podatkov, ki jih imajo državni organi oz. javni sektor, ker je na tem področju je še danes največ možnosti za zlorabe. Glavno tveganje izhaja iz neprepričljive politične nevtralnosti tega sektorja. Po izkušnjah zahodnih držav pa bo čedalje več pozornosti treba nameniti tudi poslovni sferi, tistemu delu družbe, katerega glavni motiv je dobiček.

Ko govorimo o pravnem varstvu elektronskih vsebin, ne postavljamo vprašanje o zakonskem varstvu teh vsebin, ker so programi zavarovani z zakonom, pod pogojem, da je to individualno delo v smislu intelektualne lastnine. V takem primeru ima avtor vse pravice opravljanja z svojim programom (prodaja, razmnoževanje…). Kljub vsej zakonski in fizični zaščiti programov prihaja do zlorab. Tu gre predvsem za razbijanje zaščit, razmnoževanje in prodajo kopji programov. Tako prihaja do kršitev 166. člena zakona (ZASP).

Pri tehničnem varovanju elektronskih vsebin,ko gre za kriptografijo, simetrični in asimetrični ključ, zaščito z algoritmi, varen kanal…, je težko dešifrirati podatke pošiljatelja, zato je manjša možnost, da lahko pride do zlorabe.

Intelektualna lastnina je tehnično tako zaščitena, da je povprečen uporabnik ne more razbiti. Takšne tehnične rešitve bodo omogočile celo samodejno licenciranje. Po 166. členu ZASP pomeni kršitev avtorskih pravic, če neka oseba zlorabi izključne pravice po tem zakonu, ko proizvede, uvozi, distribuira, proda, da v najem, oglaša za prodajo, ali najem ali poseduje za gospodarske namene tehnologijo, napravo, proizvod, sestavni del ali računalniški program ali opravi storitve, ki se promovirajo, oglašajo ali tržijo z namenom, da se izogne dejanskim tehničnim ukrepom, imajo majhen gospodarski pomen ali uporabo za druge namene, kot za izognitev dejanskim tehničnim ukrepom; so načrtovani, proizvedeni, prirejeni ali izvajani predvsem z namenom omogočanja ali olajšanja izognitve dejanskim tehničnim ukrepom. Zakonodajalec je predvidel, da na tem področju obstaja možnost kršenja pravic, oziroma kraje podatkov.

[13] ZVOP – Zakon o varstvu osebnih podatkov št. 210-01/89-3/20 Ljubljana, dne 08.07 1999, sprememba zakona št. 210-01/89-3/21 Ljubljana, dne 26.06.2001 in naslednja sprememba št. 210-01/89-3/25 Ljubljana, dne 15.07.2004.

Tudi javno dostopne podatke, ki nimajo značaja avtorskega dela (npr. telefonske številke, naslove in še druge podatke) je možno zbirati. Tu gre seveda tudi za kršitve zasebnosti in obenem za predelavo javno dostopnih podatkov.

Ustrezna zakonodaja omogoča varno izvajanje elektronskega poslovanja, vendar kljub vsemu prihaja do kršitev.

5. ZASEBNOST

Pravica do zasebnosti spada med temeljne in najstarejše človekove pravice. Pravna teorija jih označuje kot absolutne pravice. Mnogokrat so označene kot univerzalne, kar pomeni, da veljajo v vsakem primeru in zoper vsakega in ne bi smele biti odvisne od zakonodajalčeve subjektivne volje, kar jim daje naravo nevtralnosti.

Sodobne družbe upoštevajo načelo, da je vsakemu posamezniku zagotovljena pravica do zasebnosti, kar pomeni, da mu je zagotovljeno spoštovanje njegovega zasebnega življenja tako doma kot v družbi. Vsaka demokratična država priznava pravico do zasebnosti v celoti, brez priziva in je pravno umeščena. Vendar imajo države različno pravno razlago teh pravic, zato jo je potrebno pravico do zasebnosti obravnavati glede na druge človekove pravice.

»Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi«, določa 12. člen splošne deklaracije človekovih pravic, ki jo je že leta 1948 sprejela in razglasila Generalna skupščina Združenih narodov. V tistem obdobju informacijska tehnologija še ni ogrožala človekove zasebnosti. V današnjem času ta določba dobiva vse večji pomen, ker je informacijska tehnologija iz dneva v dan boljša. Zato si s pojmom pravice do zasebnosti posameznik želi normalno osebno življenje in ne vmešavanje tretje osebe v njegovo življenje.

To je pravica posameznika, da v njegovo življenje ne posega ne država in ne zasebnik. Je pravica, ki jo ljudje pojmujejo kot eno največjih vrednot v življenju, saj jim predstavlja svobodo, intimnost in obvladovanje okolja.

Tudi zasebnost ima sestavine in nekateri avtorji opisujejo tri sestavine:

1. zasebnost v prostoru (želja posameznika, da je sam),
2. zasebnost osebnosti (svoboda misli, opredelitve in izražanja),
3. informacijska zasebnost (želja posameznika, da se informacije ne izvejo, ker on ne želi).

Prvi dve sestavini spadata med temeljne pravice in svoboščine. Sporna oziroma ogrožena je zadnja, tretja sestavina zasebnosti, v katero sodi tudi varstvo osebnih podatkov.

Ena prvih definicij se je pojavila na začetku 20. stoletja v ZDA. To je pravica posameznika, da se ga pusti pri miru. Vendar ta definicija v današnjem času nima pravega pomena. Zaradi razvoja informacijske tehnologije se pravica do zasebnosti opredeljuje kot pravica posameznika, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli. »Gre torej za kontrolo pretoka in posredovanja podatkov, ki se nanašajo nanj oziroma opisujejo njegove lastnosti« (Čebulj 1992, 7).

V današnjem času, ko je informacijska tehnologija iz dneva v dan bolj razvita, se najbolj ukvarjajo z informacijsko zasebnostjo. Predvsem s kontrolo in posredovanjem podatkov, ki se nanašajo na posameznika.

Poleg tega moramo upoštevati tudi zbiranje, obdelovanje in prenos podatkov, ki predstavljajo nevarnost pri kršenju teh pravic.

Pri zbiranju moramo biti pozorni predvsem na to, da posameznik ne utrpi materialne ali moralne škode. To pomeni, da moramo pri zbiranju paziti na nenatančnost, napačnost, nepopolnost in neažurnost podatkov.

Pri obdelovanju podatkov lahko hitro pride do nove vsebine podatka. »Z napačnim vrednotenjem ogromne količine podatkov in informacij, ki se zbirajo o posamezniku, lahko pridemo do novih podatkov in informacij s kvaliteto, ki je za posameznika škodljiva ali celo nevarna« (Čebulj 1992, 9).

Pri prenosu podatkov je potrebno paziti, da podatkov ne dobi oseba, ki nima pooblastil za njihovo uporabo.

Podatki se vodijo v državnih organih, v javni upravi, v podjetjih, v zasebnem sektorju in nenazadnje tudi na domu, ko posameznik opravlja delo preko računalniškega omrežja. Zaradi različnega vodenja podatkov je potrebno zagotoviti tehnične pogoje in mehanizme, ki preprečujejo nepooblaščen dostop do osebnih podatkov. Zaščita podatkov je označena v teoriji in vanjo spada varstvo osebnih podatkov oziroma varstvo posameznikove informacijske zasebnosti ter zavarovanje podatkov. V zavarovanje podatkov štejemo računalniško opremo, zbrane podatke in procesiranje.

Vprašanje pojma informacije in podatka je precej odvisno od obsega varstva posameznikove pravice do informacijske zasebnosti. Podatek je informacijsko nižja sestavina od informacije, zato je bolje govoriti o varstvu podatkov. To pomeni, da je potrebno varovati podatke, informacije in oboje.

Poznati moramo tudi pravna sredstva, ki se uporabljajo v primeru kršitve pravil varstva osebnih podatkov. Ta sredstva so v obliki preventivnih ukrepov, ki se uporabljajo v okviru pravil varstva osebnih podatkov in v obliki sredstev. Med preventivne spada predvsem pravica posameznika, da se seznani s podatki, ki so zbrani in se nanašajo nanj. Če je prišlo do kršitve, posameznik uveljavlja kazenskopravne, civilnopravne in druge sankcije zoper kršitelja.

Tudi Evropska unija opozarja na kršenje zasebnosti oziroma pravice do zasebnosti. Odbor za varstvo osebnih podatkov in zasebnosti pravi, da podatki zbrani v elektronski obliki niso zaščiteni, ko uporabnik uporablja internet, saj je javen in odprt sistem, ki ne zagotavlja tajnosti in zaupnosti informacij. Vsak posameznik, ki ima vsaj malo tehnično-informacijskega znanja lahko prestreza in razkrije informacije, ki se pretakajo po omrežju. Zato bi bilo smiselno opozarjati vse uporabnike na nevarnost kršenja zasebnosti.

Podjetja bodo težila, da bi ponudbo približala posamezniku, zato zahtevajo obdelavo osebnih podatkov. Tehnologija bo težila k lažjemu sledenju uporabnika, zato se bodo videle njegove stalne navade. Ker bodo osebni podatki vse lažje dostopni, se bodo pokazale sekundarne kršitve. Vse to bo prineslo nova tveganja s stališča varstva pravice do zasebnosti. Tudi podjetja bodo imela vse več osebnih podatkov, kar ni v interesu vsakega posameznika (Kalan 2002, 13).

5.1 Pravica do zasebnosti

Pri zasebnosti se postavlja tudi vprašanje, kaj sploh je zasebnost. Zato moramo vedeti, da pravo (ustava) ne ščiti zgolj prostorov, lastnine ali lastnikov, temveč tudi posameznike, ki v določenem prostoru (tudi virtualnem) ali pri določenem ravnanju (upravičeno) pričakujejo zasebnost.

Pravico do zasebnosti, ki spada med človekove pravice, imenujemo v elektronskem poslovanju pravico do informacijske zasebnosti. Za posameznika predstavlja interes, da se državi in nepovabljenim tretjim ne razkrije informacije in da ima posameznik nadzor nad informacijami (katere informacije in v kakšnem obsegu jih bo predstavil drugim). Je pravica, da posameznik svobodno sprejema odločitve v svojem življenju. Pri tem moramo razlikovati, da ima posameznik različne potrebe po informiranju. Informiranje družine in prijateljev ni enako kot informiranje države, delodajalca ali dajanje podatkov elektronski trgovini.

Gre za temeljno osebnostno pravico, ki je povezana s svobodo, avtonomijo in svobodno voljo posameznika in ni samo pravica posameznika. Določa, da se posameznik avtonomno odloči kdaj, kako in koliko se v to pravico lahko posega. Poseg v pravico je prepovedan, če posameznik tega ne želi. Zato se vse neutemeljene in neupravičene posege skuša preprečiti v mednarodnih dokumentih, s področja varstva pravic posameznika. Tudi v našem pravu je zagotovljeno varstvo pravic posameznika, kot ustavna kategorija.

Ustava Republike Slovenije je najpomembnejši vir ustavnega prava, ker določa pravice in svoboščine posameznika ter ureja temelje državne ureditve. Zato morajo biti z ustavo usklajeni vsi pravni akti, ki sestavljajo pravni red države.. V členih, ki se nanašajo na zasebnost, se zagotavlja varstvo zasebnosti in osebnostnih pravic 35. člen; varstvo osebnih podatkov 38. člen; svoboda izražanja 39. člen.

Pravica do zasebnosti je zapisana tudi v vseh pomembnih pravnih dokumentih, vendar zaradi razvoja tehnologije, ki omogoča vse večje kršenje zasebnosti, ni mogoče zapisati enotne definicije zasebnosti. Zasebnost se npr. pojavlja v povezavi s pravicami do zasebnosti, ki je pravica posameznika, da se ga pusti pri miru, v ta okvir spada tudi pravica do zasebnega življenja; pravica do nadzora informacij o samem sebi; pravica omejitve dostopa do osebnih podatkov; pravica nadzora dostopa do zasebnega življenja;

pravica do najmanjšega možnega posega v zasebnost; pravica do pričakovanja zaupnosti; pravica do osamljenosti; pravica do intimnosti; pravica do anonimnosti; pravica do distance; pravica do tajnosti.

Ustavno sodišče v Sloveniji je prevzelo varovanje zasebnosti v primeru Halford iz Velike Britanije. Tu gre za dva elementa zasebnosti: pričakovanje zasebnosti in upravičenost pričakovanja, kar pomeni, da posameznik upravičeno pričakuje, da ne bo nadzorovan, ko bo v (virtualnem) prostoru oziroma odnosu. Ta doktrina je pomembna predvsem, ko posameznik uporabi storitve elektronskega poslovanja preko interneta, in sicer v primerih, ko zakonodajalec upravičenega pričakovanja zasebnosti ni priznal še na abstraktni zakonski ravni, e-pošta, za katero je praviloma potrebna sodna odredba. Delojemalec v marsičemu pričakuje, da vsebina njegovih razgovorov kljub nadzorovanim klicanim telefonskim številkam ni nadzorovana[14] (Kalan 2002, 25).

5.2 Pravica do informacijske zasebnosti

Sklopi zasebnosti pri elektronskem poslovanju se nanašajo na naslednja vprašanja:

1. tajnost in dostop do vsebine sporočil,
2. ravnanje in dostop do prometnih podatkov, ki so potrebni za posredovanje vsebinskih sporočil,
3. identifikacija udeležencev, ki opravljajo s podatki,
4. varstvo osebnih podatkov,
5. samodejna obdelava podatkov (Makarovič et al., 2001).

V Sloveniji je zelo pomemben Zakon o elektronskih komunikacijah št. 043-03/04-3/1 Ljubljana, dne 09.04.2004. V ospredju je zaščita interesa uporabnika telekomunikacijskih storitev vključno z varstvom tajnosti in zaupnosti. Določbe se nanašajo tudi na ponudnike in upravljavce e-poštnih strežnikov v Sloveniji. To ne velja za notranja oziroma zaprta računalniška omrežja v podjetjih in državnih ustanovah, pač pa za javne odprte sisteme. Zakon o telekomunikacijah nudi tudi določeno zaščito zasebnosti pri uporabi telekomunikacij. Vendar to ne pomeni, da ščiti e-pošto v zaprtem (zasebnem) sistemu. S tem problemom se ne sooča samo Slovenija, ampak tudi Evropska unija, zato že pripravljajo spremembe v zakonu.

Zato je ZVOP[15] toliko pomembnejši, za varstvo informacijske zasebnosti. Uporablja se za pridobivanje osebnih podatkov tako za javni kot zasebni sektor, za

[14] Kazenski zakonik: zaradi selitve javnih občil v elektronsko okolje se bo pojavljalo vedno več posegov v zasebnost. Nejasna bo razmejitev medijske informacije in informacij, ki jih po internetu lahko širi kdorkoli.

[15] ZVOP – Zakon o varstvu osebnih podatkov št. 210-01/89-3/20 Ljubljana, dne 08.07 1999, sprememba zakona št. 210-01/89-3/21 Ljubljana, dne 26.06.2001 in naslednja sprememba št. 210-01/89-3/25 Ljubljana, dne 15.07.2004.

upravljanje zbirk osebnih podatkov, zbranih na podlagi zakonskega pooblastila ali pisne privolitve posameznika.

Zelo pomembna sta tudi dva predpisa Evropske unije:

1. direktiva o varstvu posameznikov pri obdelovanju osebnih podatkov in prostem gibanju takšnih podatkov[16] (95/46/EC),
2. direktiva o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (97/66/EEC).

Tema dvema se morajo države članice EU prilagoditi glede varstva in zaščite osebnih podatkov. Predpisa se nanašata tako na javni kot zasebni sektor, uporabljata se za zbiranje in obdelavo osebnih podatkov pri elektronskem poslovanju na internetu. V naslovu Direktive 95/46/EU ni omenjena avtomatska oziroma elektronska obdelava podatkov, vendar je bil to glavni povod za njen sprejem.

Najbolj pomembno je, da se od ponudnikov in upravljavcev storitev elektronskega poslovanja zahteva dvoje:

1. uporabnik mora biti vedno vnaprej seznanjen s politiko varovanja njegovih osebnih podatkov, njihovega obdelovanja in posredovanja tretjim osebam,
2. uporabniku se nudi možnost izbire, da omeji obseg uporabe in nadaljnje posredovanje njegovih osebnih podatkov. Tu moramo paziti da ima upravljalec dejansko uporabnikovo izrecno dovoljenje, ali se podatki lahko uporabijo, in na uporabnikovo izrecno prepoved, da se podatki uporabijo.

Ker je narava elektronskega poslovanja taka, da se podatki v elektronski obliki hitro in nenadzorovano prenašajo prek raznih medijev čez državne meje, je smiselno, da bi mednarodno pravo uskladilo vse pojme glede tega. Ko bodo dosegli uskladitev, bo tudi manj kršitev pravic zasebnosti. Najboljši zakon imajo v Nemčiji, kjer se imenuje Zakon o varstvu podatkov pri elektronskih storitvah[17] (Kalan 2002, 28).

5.4 Zasebnost v elektronskem okolju

Možnosti, da bi bile zasebnostne vrednote ogrožene z elektronskim poslovanjem je precej. Nekatera vrsta ogrožanja izhajajo iz napadalnega konkurenčnega poslovanja (poslovno vohunstvo, nenaročene e-pošiljke, kršitev zasebnosti zaposlenih, ogrožanje potrošnika/uporabnika). Slabšo zasebnost omogočajo tudi nekatere tehnologije elektronskega poslovanja (neanonimni prenosi, delo komunikacijskih posrednikov in operaterjev). Sporne utegnejo biti nekatere rešitve glede dajanja biometričnih podatkov, ki naj bi jih uporabljali v elektronskem poslovanju. Veliko tveganj je povezanih s kazenskimi preiskavami in z nedemokratičnimi političnimi prijemi (prisluškovanje,

[16] Skrajšano poimenovanje »Evropska direktiva o varstvu osebnih podatkov«.
[17] Sprejet je bil že leta 1997.

prestrezanje sporočil[18]...).

Treba je poudariti, da so pri elektronskem poslovanju potrebna tehnološka in organizacijska zagotovila (sredstva) za varovanje zasebnosti, ker pravna niso dovolj. Tako v odprtih kot tudi v zaprtih elektronskih okoljih so se na področju zasebnosti že izoblikovale problemske skupine, ki so značilne le za elektronsko poslovanje.

V elektronskem okolju je anonimno sporočanje ena od učinkovitih možnosti varovanja zasebnosti. Podoben učinek lahko dosežemo tudi pri sporočanju z izmišljenim imenom. Anonimiziranje spodbuja tudi Evropska direktiva o varstvu osebnih podatkov (95/46/EC; 26. tč. preambule), ki v tem vidi eno od učinkovitih možnosti za zakrivanje osebnih podatkov. Kako zagotoviti anonimnost pri elektronskem poslovanju, je predvsem stvar tehnoloških rešitev in ne prava. Tudi stvar zaupanja v operaterje, ki naj bi zanjo skrbeli. Torej ni popolnega jamstva za zanesljivo elektronsko anonimnost.

V odprtem elektronskem okolju si z anonimnostjo lahko zagotovi varnost tudi organizacija/podjetje, ki ne želi, da bi konkurenca spremljala njene proizvode po internetu.

Anonimno poslovanje je izvedljivo na več načinov: z e-pošto prek anonimnih ali psevdoanonimnih strežnikov, s storitvami za anonimno pregledovanje spletnih strani, z varnostnimi rešitvami, ki jih ima pošiljateljev računalnik, zakrit identiteto posameznega pošiljatelja ipd.

Glavni nasprotniki anonimnosti so državne varnostne službe, ki skušajo tako ali drugače nadzorovati elektronsko sporočanje.

Anonimnemu poslovanju bi lahko očitali, da slabo vpliva na človekovo socialno zadržanost, ki je za skupno življenje potrebna. Računalniški sistemi, zlasti če so oddaljeni, delujejo na človeka neosebno. Takšno razmerje se še krepi, če je možen anonimen ali kako drugače zakrit dostop. Etičnost stopa v ozadje, izgubljajo se vrednote in osebne vloge. Anonimnost postane problematična zlasti takrat, ko gre za kaznivo početje, kar pomeni zlorabo anonimnosti.

Šifrirne tehnike se uporabljajo tudi pri digitalnem podpisovanju, zato moramo šifrirno zakrivanje vsebine načeloma ločiti od digitalnega podpisovanja. Z digitalnim podpisom zagotovimo naloge lastnoročnega podpisa, lahko tudi celovitost sporočila, ki je s podpisom neločljivo povezan. Šifrirne tehnike zagotavljajo predvsem zaupnost (zasebnost) sporočila. V obeh primerih gre za to, da šifrirne tehnike zagotavljajo varnejše, bolj verodostojno in bolj predvidljivo elektronsko poslovanje. Dejstvo, da je možno sporočilo verodostojno podpisati digitalno, ne da bi ga hkrati tudi zakrili pred branjem, uporabljajo kot utemeljitev, da je digitalno podpisovanje in šifriranje možno

[18]Mnoge elektronske tehnike spadajo med t.i. tehnologije politične kontrole.

urejati ločeno. Digitalni podpis je za varnostne službe celo zanimiv, saj pošiljatelj težko zanika, da sporočila ni poslal.

Države kažejo različen odnos do množične rabe elektronskih šifrirnih tehnik: nekatere jih prepovedujejo zunaj uradne državne rabe, nekatere jih skušajo prepovedati oz. njihovo rabo nadzorovati, v večini držav pa je šifriranje prosto. Med zadnje uvrščamo tudi demokratične države, kjer raba ni izrecno urejena in se zato šteje, da je prosta. Ker države ne morejo v uporabnem času razkrivati sporočil, ki so sporna zaradi kriminalnih dejavnosti, lahko pričakujemo, da bo prišlo do meddržavnih dogovorov o neke vrste nadzorovani rabi šifriranja, ki bo še v mejah ustavno varovane zasebnosti. Med »varnostniki« in zagovorniki necenzurirane svobode potekajo znotraj držav živahne razprave, kar kaže tudi poročilo avstralskega državnega tožilca o šifrirni politiki, ki so ga brez nekaterih izpuščenih delov objavili šele na odločno zahtevo civilne javnosti[19].

Mnogi strokovnjaki opozarjajo, da je za operaterja varovanje osebnih podatkov težja naloga kot varovanje zasebnosti vsebine. Zanjo namreč lahko poskrbi tudi sam uporabnik (šifriranje in drugi ukrepi). Varovanje tajnosti vsebine velja ne glede na način prenosa (analogno, digitalno) in ne glede na njegovo vsebino (govor, podatki). Tudi v Nemčiji, kjer imajo razmeroma najnovejše in dobro urejeno telekomunikacijsko področje ter elektronsko poslovanje, ugotavljajo, da so pri razmejevanju telekomunikacijskih in elektronskih storitev velike težave.

Kršitev tajnosti pisem je kaznivo dejanje. To velja tudi za ponudnika storitev (npr. za strežnik e-pošte), čeprav računalnik ni njegov. Brisanje naročnikove vsebine je dovoljeno le v skladu z medsebojno pogodbo. To pomeni, da bi bila operaterjeva nedogovorjena »cenzura« vsebine protipravna (razen če bi šlo za preprečevanje kaznivega dejanja, za dejanje skrajne sile, za preprečevanje operaterjeve civilne odgovornosti proti tretjim osebam ipd.).

Vsako neposredno uveljavljanje ustavne določbe, to velja tudi glede tajnosti in zasebnosti sporočanja, je razmeroma zahtevno in manj razvidno, kot če gre za izvajanje zakonskih ali podzakonskih predpisov. Zato bi moralo prej ali slej priti do skupnega predpisa, ki bi urejal tajnost vsebine sporočanja na vseh področjih telekomunikacij, infrastrukture interneta in na področju podatkovnih storitev. To bi pripomoglo, da bi bilo elektronsko poslovanje pravno bolj predvidljivo (Toplišek 1998, 143).

5.5 Zasebnost delojemalca

Informacijska zasebnost zaposlenega se dotika tako papirnih kot tudi elektronsko zbranih podatkov. V obeh primerih v enaki meri veljajo pravila in načela spoštovanja

[19]»The Walsh Report«, vsebina poročila in dogajanja ob njem so na naslovu [http://www.efa.org.au/Issues/Crypto/Walsh].

zasebnosti. Če gre za podatke v zvezi z delovnim razmerjem, je treba omeniti posebno Priporočilo Sveta Evrope[20], ki opozarja, naj delodajalec ne uporabi ročno procesiranih podatkov zato, da bi se izognil načelom, ki veljajo za varstvo elektronsko obdelanih podatkov. To je pomembno načelo, ki je vsaj posredno uporabno tudi za druga razmerja med pisnimi in elektronskimi podatki.

Zlasti v okoljih, ko so računalniki povezani v omrežje, je možno zlahka nadzorovati, kaj zaposleni počnejo na svojem računalniku:

1. kdaj se priključijo in odjavijo,
2. katere programe uporabljajo in koliko časa,
3. kakšna je vsebina njihove e-pošte,
4. v katerih diskusijskih skupinah sodelujejo,
5. koliko časa je bil kdo priključen na splet, kdaj in koliko podatkov je prenesel k sebi,
6. katere igrice se igrajo med delovnim časom in koliko časa,
7. druga dogajanja na računalniškem zaslonu.

Ker del delavčevega komuniciranja hkrati poteka tudi po javnih komunikacijskih omrežjih, opozarjajo, da bi bilo potrebno vzpostaviti ravnovesje med varstvom zasebnosti po javnem omrežju in tistim delom sporočanja, ki poteka po delodajalčevem omrežju. Možne vzporednice so tudi glede pisemske pošte, ki prihaja v podjetje na ime zaposlenega.

Vprašanje zasebnosti je seveda nekoliko drugačno v okoljih, kjer morajo zaradi svojega osnovnega dela nadzorovati sporočila (npr. v varnostni službi[21]). Če izvzamemo primere, ko zaposleni po naravi stvari ne bi smeli vedeti za nadzor, prevladuje mnenje, da je pravno sporno, če zaposleni ne vedo vnaprej, da jih bodo nadzorovali oz. da bodo preiskovali njihovo elektronsko okolje. Pri tem je temeljno izhodišče ustavna pravica do zasebnosti, ki nalaga dokazno utemeljevanje tisti strani, ki ravna v nasprotju s to človekovo pravico. Spoštovanje zasebnosti delojemalcev izrecno narekuje Priporočilo Sveta Evrope (gl. v op. št. 29), ki omenja pravico, da zaposleni na delovnih mestih lahko vzpostavljajo osebne in socialne stike. Delodajalec naj bi jih vnaprej seznanil, da bodo uvedli ali prilagajali sistem za zbiranje osebnih podatkov ter sistem za spremljanje gibanja ali storilnosti. Vnaprej mora biti znano, kdaj naj bi delodajalec glede zbiranja podatkov pridobil soglasje zaposlenih. Nadzor je možen z vnaprejšnjo najavo, objavo in s soglasjem sodelujočih. Tudi če obstajajo notranja

[20]Protection of personal data used for employment purposes, Recommendation No. R (8912, Komite ministrov Sveta Evrope, 989).

[21]Tako je npr. nemško sodišče v primeru podjetja, ki se ukvarja s telefonskimi rezervacijami za letalski promet, odločilo, da pravno ni sporen dogovor z zaposlenimi, da sme delodajalec v prisotnosti zaposlenega poslušati zunanje telefonske razgovore, če gre za usposabljanje zaposlenega (LAG Frankfurt/M. I ABR 4/95, 30.8.1995).

pravila o nadzoru, je treba preveriti razmernost takšnih omejitev – ali so širše, kot je nujno potrebno, da se doseže legitimni, dovoljeni, dogovorjeni namen. Gre za tehtanje razumnih, z ustavo zagotovljenih pričakovanj zaposlenega in legitimnih nalog oziroma ciljev delodajalca. Pravila o dovoljenem preiskovanju računalnikov v organizaciji se samodejno ne nanašajo na računalnik, ki bi ga zaposleni prinesel s seboj v službo (Toplišek 1998, 150).

5.6 Primeri kršenja zasebnosti v elektronskem okolju

Eden od načinov kršenja zasebnosti je primer, ki so ga odkrili na Švedskem, ker so ugotovili, da ima ameriška država del šifrirnega ključa iz programa Lotus Notes, ki ga uporablja tudi slovenska uprava in drugi podobni primeri kažejo, da je treba ob šifrirni tehniki, ki ni »lastna«, vedno pomisliti na možnost, da njen dobavitelj lahko razkriva vsebino sporočil. Če gre za sporočila zasebne narave, lahko govorimo o kršenju zasebnosti.

Velikokrat prihaja do kršenja zasebnosti na delovnem mestu, če delodajalec ne vnaprej seznani svojih delavcev, da bodo uvedli ali prilagajali sistem za zbiranje osebnih podatkov ter sistem za spremljanje gibanja ali storilnosti. Vnaprej mora biti znano, kdaj naj bi delodajalec glede zbiranja podatkov pridobil soglasje zaposlenih. Nadzor je možen z vnaprejšnjo najavo, objavo in s soglasjem sodelujočih. V kolikor delodajalec ne upošteva zgoraj navedenih postopkov, prihaja do kršenja zasebnosti na delovnem mestu.

O primerih kršenja zasebnosti lahko govorimo tudi, ko gre za vdore v računalniški sistem, ali za nepooblaščeno spreminjanje podatkov. Tu je mišljena predvsem zloraba osebnih podatkov, kršitev avtorske pravice, neupravičeno izkoriščanje avtorskega dela, neupravičen vstop v zaščiteno računalniško bazo podatkov. [URL: http://www.arnes.si/si-cert/kz.htm], 20. 03. 2004).

Sodobna elektronska tehnologija omogoča preprosto, ceneno in hkratno razpošiljanje sporočil na mnogo naslovov. Takšno početje je lahko sporno z več vidikov.

Množična e-pošta je nemalokrat povezana z nezakonitim pridobivanjem seznamov naslovnikov (udeleženci diskusijskih e-list in podobnih oblik druženja[22]), s kupovanjem zbirk naslovov. Pri tem se krši jo pravila o varstvu osebnih podatkov. V ZDA prodajajo sezname s tisoči e-naslovnikov za 10-40 $ in računajo, da stane ena e-pošiljka okrog 0,01 centa (Toplišek 1998, 154).

[22]»Harvesting« imenujejo nabiranje e-naslovov po diskusijskih skupinah. BBS-il, pogovornih krožkih (chat rooms).

V Zagrebu se je pojavil spisek, ki kroži po elektronski pošti z imeni in ostalimi osebnimi podatki pod naslovom »gej imenik«. V njem so osebni podatki več kot 800 homoseksualcev. Ta seznam zelo hitro kroži po elektronski pošti, med tistimi, ki so na njem je zavladala panika, saj gre za kršenje njihove zasebnosti. Poleg njihovih imen in letnice rojstva so na njem tudi njihove telefonske številke, kraj bivanja, spolne navade in celo imena njihovih bivših spolnih partnerjev (Kajzer 2005, 24).

Tako lahko z gotovostjo trdim, da kljub uspešni zakonodaji, ki se nanaša na zasebnost v elektronskem okolju, prihaja do velikega števila kršitev.

6. JURISDIKCIJA V ELEKTRONSKIH OKOLJI

6.1 Izbira prava

V večini držav se dogajanja v elektronskem poslovanju dotikajo pravne ureditve posamezne države. Država določa, v katerih okoliščinah bo uporabljeno njeno pravo. Ta dejstva v mednarodnem in zasebnem pravu imenujemo navezne okoliščine. Primeri:

1. osebne navezne okoliščine: državljanstvo, prebivališče, sedež pravne osebe, kraj registracije plovila/pravne osebe,
2. stvarne navezne okoliščine: kraj sklenitve pogodbe, lega nepremičnine, kraj, kjer je bilo izvršeno dejanje, kraj izpolnitve obveznosti, kraj nastanka škode,
3. sestavljene in druge navezne okoliščine: okoliščina največje povezanosti, navezna okoliščina hipotetične volje strank (katero pravo bi stranke verjetno same izbrale), pravo kraja sodišča (če ni možno določiti ustreznejšega prava).

Pravila, ki določajo, katero pravo se bo uporabilo v nekem razmerju s tujim elementom, so kolizijska pravila. Ta ne odločajo o vsebini pravnega problema, temveč usmerjajo na drugo pravno pravilo. Ko torej sodišče ali kak drug organ ugotovi, da je treba uporabiti »njegovo« pravo, hkrati določi, da je pristojen odločati o vsebini zadeve. Redkejši so primeri, ko sodišče/arbitraža uporabi tuje pravo – to je zlasti ob pogodbeno dogovorjeni rabi kakega prava.

Srečujemo različna pojmovanja izraza *jurisdikcija:* sami ga bomo uporabljali kot pristojnost za obravnavanje pravnega razmerja (krajevna, stvarna-vsebinska pristojnost...). V takšni postopkovni povezavi se uporablja največkrat. Pojavljajo se tudi druga pojmovanja, npr. jurisdikcija kot območje določenega pravnega sistema, jurisdikcija kot problem predpisovanja pravil (zakonodajna jurisdikcija), jurisdikcija za izvršitev odločitve (Toplišek 1998, 161).

6.2 Pristojnost slovenskega sodišča

V postopkovnih predpisih najdemo določbe, v katerih primerih je krajevno ali stvarno pristojen organ na ozemlju naše države. V pravdnih zadevah je predvsem pristojno sodišče toženca. Odločilno je, kje ima toženec (stalno, začasno) prebivališče. Če slovenski državljan stalno živi v tujini, je pristojno sodišče glede na njegovo zadnje stalno prebivališče v Sloveniji. Podobna kot za fizično osebo je pristojnost tudi za

organizacijo. To je t. i. splošna krajevna pristojnost (46 do 49. čl. ZPP)[23].

Obstajajo tudi posebne krajevne pristojnosti. Za elektronsko poslovanje je pomembna pristojnost v odškodninskih sporih (52. čl. ZPP). Če gre za nepogodbeno škodo (npr. zaradi razžalitve, nelojalnega poslovanja...), je poleg splošno pristojnega krajevnega sodišča pristojno tudi sodišče, na območju katerega je bilo storjeno škodno dejanje, ali sodišče, na območju katerega je nastopila škodljiva posledica.

V nekaterih primerih je lahko pred slovenskim sodiščem tožen tudi tujec, toda izvedba takšnega postopka, zlasti izvršba je negotova (66. čl. ZPP). Če ni mogoče dognati, katero sodišče bi bilo pristojno, odloča Vrhovno sodišče. Za elektronsko poslovanje je pomembno, da lahko najvišje sodišče določene vrste na predlog stranke ali sodišča določi, da v posamezni zadevi postopa drugo pristojno sodišče, če je očitno, da se bo tako lažje opravil postopek ali če so za to podani drugi tehtni razlogi.

O vsaki pristojnosti, za katero zakon ni določil, da je izključna, se lahko stranke sporazumejo, da bo sodilo drugo stvarno pristojno sodišče. Sporazum o tem mora biti dokazljiv v pisni obliki, mora se nanašati na določen spor ali na več sporov iz določenega pravnega razmerja. Tožnik mora priložiti listino o sporazumu.

Dokler pravni postopki ne bodo bolj prilagojeni elektronskemu poslovanju, morajo udeleženci sami poskrbeti za dokazljivost nekaterih svojih dejanj, kar ne pomeni, da ne bi smeli pogumno nastopati tudi z elektronskimi dokazili.

Tudi pri kaznivih dejanjih je nekaj negotovosti. Med takšne npr. sodi vprašanje kako za dejanja elektronskega poslovanja uporabiti v zakonu določeno pristojnost. ZKP (Uradni list RS št. 63/1994).

Pristojnost, ki velja za dejanja, storjena s tiskom (28. čl. ZKP), očitno velja le za klasična sredstva javnega obveščanja. To je povsem neskladno z možnostmi sodobnega elektronskega objavljanja. Sedaj veljavna vsebinska opredelitev sredstva javnega obveščanja, postaja pretesna za sodobne možnosti razširjanja sporočil, namenjenih javnosti. Če kraj tiskanja ni znan ali če je v tujini, je pristojno sodišče, na območju katerega se spis razširja. V enem samem stavku vidimo vsaj tri pojme, ki so sprti z naravo razširjanja sporočil elektronskega poslovanja.

V problem pristojnosti v ožjem smislu ne štejemo vprašanj medsebojne pravne pomoči med državami, vprašanja izročitve storilca in vprašanja izvršitve tuje odločitve (civilne ali kazenske). Zahteva tuje države, naj se v Sloveniji prevzame pregon slovenskega državljana ali osebe, ki ima tukaj stalno prebivališče, zaradi kaznivega dejanja, storjenega v tujini, se pošlje državnemu tožilcu, na katerega območju ima ta oseba stalno prebivališče (520. čl. ZKP) (Toplišek 1998, 165).

[23]ZPP – Zakon o pravdnem postopku št. 710-01/95-4/6, Ljubljana, dne 25.03.1999, sprememba zakona št. 710-01/95-4/16 Ljubljana, dne 25.10.2002, naslednja sprememba zakona Št. 710-01/95-4/28 Ljubljana, dne 19.12.2003.

6.3 Pristojnost tujega sodišča

Pri elektronskem poslovanju v mednarodnem okolju, se bo pogosto zgodilo, da se bodo udeleženci dogovorili za sodišče določene države. Tak dogovor bo obojestranski, ko bosta sprejela splošne pogoje poslovanja. Dogovor o sodni pristojnosti bo nujno potreben v poslovanju, ki bo segalo čez državne meje. Če dogovora ne bo, bo o pristojnem sodišču odločal tožnik oz. tuje sodišče. Seveda ni nujno, da se bodo s tem ujemali interesi vseh udeležencev. S tujim sodiščem bo praviloma povezana tudi raba njegovega prava. Pristojnost tujega sodišča se presoja po predpisih njegove države.

Vprašanje je, ali je možno od nerezidenta zahtevati, da pozna predpise vseh držav, do katerih njegove informacije sežejo. V vsakem primeru je možno dokazovati, da toženi ni mogel poznati tujega prava, zlasti če predvideva rešitve, ki so neobičajne v njegovi ali v drugih državah. Ker je poznavanje prava eno temeljnih načel pravne države, bo uspeh takšnega dokazovanja negotov.

Po ZMZPP[24] v (6. do 12. členu) obravnava, da v primeru, če pravila tuje države, ki določajo, katero pravo je treba uporabiti, zavračajo na pravo Republike Slovenije, se uporabi pravo Republike Slovenije, ne da bi se pri tem upoštevala njena pravila o napotilu, katero pravo se uporabi. Če se ne da ugotoviti, katero pravo države z neenotnim pravnim redom je treba uporabiti, se uporabi pravo tistega območja v taki državi, ki je z razmerjem v najtesnejši zvezi. V primeru, da ima državljan Republike Slovenije tudi državljanstvo kakšne druge države, se za uporabo tega zakona šteje, da ima samo državljanstvo Republike Slovenije. Če ima oseba, ki ni državljan Republike Slovenije, dvoje ali več tujih državljanstev, se za uporabo tega zakona šteje, da ima državljanstvo tiste države, katere državljan je in v kateri ima tudi stalno prebivališče. Vprašanje je v kolikor oseba nima državljanstva ali njenega državljanstva ni mogoče ugotoviti, se uporabi pravo njenega stalnega prebivališča, če tega ni mogoče ugotoviti se uporabi pravo začasnega bivališča, če tudi tega ni mogoče ugotoviti, se uporabi pravo Republike Slovenije (Uradni list RS št. 700-01/95-44/3).

Ponudnik storitve prek interneta se lahko izogne sporu v tujini, če tehnično izloči sodelovanje kupca/uporabnika z določenega območja. To lahko stori tudi na pravni način - z uporabnikovo izjavo, da npr. »ni državljan neke države« ipd. Toda takšna tehnična ali pravna omejevanja so v nasprotju z naravo elektronskega poslovanja v odprtih okoljih, kjer ponudba velja za vnaprej nedoločen krog uporabnikov (ne glede na države, pravne rede). Uporabljajo jih pri dejavnostih, za katere je znano, da so v drugih državah prepovedane, omejene ali kako drugače sporne (igre na srečo, razširjanje

[24]ZMZPP – Zakon o mednarodnem zasebnem pravu in postopku št. 700-01/95-44/3 Ljubljana, dne 30.06.1999.

gradiv, ki so lahko ocenjena kot pornografska ali lahko prizadenejo mladoletnike, ipd.) (Toplišek 1998, 167).

Kadar je evropska norma sposobna neposrednega učinkovanja in je pravno razmerje jasno razmejeno v pristojnosti prava Skupnosti, posebnih težav v praksi nebi smelo biti. Seveda velja enako za razmerja, ki so ustrezno urejena z domačim pravom, če je v celoti in jasno harmonizirano z evropskimi predpisi. Možno pa si je predstavljati številne primere, ko se bosta oba pravna reda prepletala na način, ki povzroča dvome o tem, kdo, koliko in kako naj pravno vprašanje uredi in, ali je tako tudi urejeno. Seveda bodo pri tem stranke, ne glede na to, ali gre za zadevo upravnega prava ali pa za klasičen spor po načelu kontradiktornosti, z namenom, kot ga pač zasledujejo, večkrat pravno sliko le dodatno zapletle. Nastale dvome o tem, kako glasi zgornja premisa pravnega silogizma, rešujeta navedeni načeli primarnosti in neposredne uporabe prava Skupnosti.

Teorija opozarja, da gre pri načelu primarnosti evropskega prava za določitev hierarhije pravnih norm tako, da ima prednost pri uporabi pravo Skupnosti, ki prevlada nad nacionalnim (Primath 2004, 187).

6.4 Nauki iz tujine

Države različno določajo krajevno pristojnost svojih organov (razlike so celo med zveznimi državami v ZDA), vendar je možno iz dosedanjih odločitev izluščiti nekaj splošnih skupnih potez.

Iz dosedanjih primerov izhaja, da sodišča ločujejo primere, ko ponudnik ponuja zgolj informacijo, ali trajneje posluje oz. povzroča nekomu škodo. Ob kaznivem ali škodnem delovanju je število oz. intenzivnost stikov z ozemljem sodišča bistveno manj pomembno kot v civilnih in drugih poslovnih zadevah. Nemško sodišče se je razglasilo za pristojno glede obravnavanja domene, ki je vsebovala sporno nemško blagovno znamko, čeprav je bila domena registrirana v ZDA. Menili so, da škodljive posledice po internetu segajo tudi na nemško ozemlje.

Če so informacije na domačih straneh omejene zgolj na pasivno gledanje, je veliko manjša možnost, da imetnika strani ujame tuja jurisdikcija. Bolj ko je elektronska objava dvosmerna (interaktivna), večja je ta nevarnost. Položaj v vmesnih primerih je seveda negotov. Predstavitev je pasivna, če npr. ponudnik prek spletne strani neposredno ne prodaja, če prek strani ni možno skleniti pogodbe, če na strani ni gumbov ali obrazcev za sporočila ponudniku ali za registracijo pri njem. Če torej spletna stran mora biti interaktivna, se njen imetnik lahko izogne povezanosti z nezaželenim območjem tako, da postavi vidna opozorila o svojih namenih. Pri dejanskem poslovanju mora seveda tako zapisane namene tudi spoštovati. Možnosti, da se izločijo določene vrste oseb, je več: naročnik mora sam vpisati podatke o svojem

prebivališču (državljanstvu), naročanje ponujenega blaga na spletni strani mora biti obvezno telefonsko (pisno, po faksu) ipd. (Toplišek 1998, 161).

7. SKLEP

Usklajevanje zakonodaje na področju elektronskega poslovanja se zdi v zadnjih letih glavna naloga različnih svetovnih organizacij, institucij in držav, ki hočejo poenotiti zakonodajo v elektronskih medijih, kot bi omogočilo popolno sprostitev globalne uporabe elektronskega poslovanja na mednarodni ravni brez ovir pri mednarodnem, poslovanju, trgovanju in hitrejšo komunikacijo s pomočjo interneta. Vendar ne glede na uspešnost državnih zakonodaj pri njihovi uskladitvi in njihovi kvaliteti v sami implementaciji in izvajanju, elektronsko poslovanje ni področje, kjer bi bil zakonodajalec lahko dalj časa zadovoljen z doseženim, saj se področje zelo hitro spreminja.

Težave pri oblikovanju ustrezne zakonodaje povzročajo tudi različni lobiji in interesne skupine, ki izvajajo pritisk na zakonodajne oblasti in zakonodajne institucije, kako naj se le-ta uredi oziroma prepušča samoregulaciji. Za regulacijo elektronskega poslovanja se zavzemajo zlasti poslovni oziroma podjetniški lobiji, katerih interes je zaščititi svoj vir dohodka pred različnimi zlorabami.

Prav zaradi vseh mogočih zlorab, ki jih elektronsko poslovanje kot digitalen medij omogoča, s pomočjo interneta in sega od nadlegovanja, kratenja zasebnosti, kršenja avtorskih pravic, podjetniškega ali medvladnega vohunjenja, vdiranja v zasebne računalnike in do kraje informacij, se je v svetu sprožil vsesplošni alarm pred nevarnostjo, ki vsako leto napravi ogromno škode. Posledično temu sledi tudi pospešen razvoj različnih varnostnih tehnologij, za zaščito uporabnikov. Uporaba varnostne tehnologije od požarnih zidov, zanesljive programske opreme, metod šifriranja pretoka informacij in učinkovitih sistemov nadzora, po možnosti podkrepljeno s strogo in učinkovito zakonodajo o elektronskem poslovanju, je vizija prihodnosti. Varnostna tehnologija bo postala najpomembnejši člen v razvoju elektronskega poslovanja.

Največje pomanjkljivosti so na področju nezanesljivosti programske opreme, pomanjkljive standardizacije ter nedorečene zakonodaje. Zlasti programska oprema, na kateri slonijo računalniški sistemi po vsem svetu, zlasti osebni računalniki in strežniška programska oprema, je vedno pogosteje povzročitelj številnih varnostnih lukenj, zato se resno postavlja vprašanje o morebitni odpravi zaščite pred vsakršno odgovornostjo, ki jo uživajo proizvajalci programske opreme. Med potrošniki se je v zadnjih letih pohoda programske opreme zasidral vtis, da je programska oprema izjema, ki ji ni treba zadostiti osnovnih varnostnih standardov. Če se nam pokvari strojna oprema, jo lahko

reklamiramo, pri pomanjkljivostih programske opreme se nimamo kam pritožiti. Pri zdajšnji ravni varnosti najbolj razširjene programske opreme je množično uničenje podatkov vedno bolj verjetna zgodba. Zdi se, da je pri razvoju programske opreme še vedno prvo vodilo razvoja in večanje funkcionalnosti, ki bi jo bilo potrebno v prihodnosti podrediti večji varnosti in trdoživosti programske opreme.

Na področju standardizacije in legalizacije različnih šifrirnih postopkov, zlasti asimetričnega šifriranja podatkov oziroma kriptografije javnega ključa, se še vedno pojavljajo dileme glede potrebe po nadzoru in regulaciji šifriranja podatkov, saj mnoge države, zlasti ZDA in Velika Britanija vztrajajo, med drugim tudi zaradi državne varnosti in zaščite pred terorističnimi napadi, pri predaji javnih ključev s strani overiteljev in drugih nosilcev enkripcijskih metod. Tako bi lahko oblasti v primerih ogrožene državne varnosti, ali tudi ne, prebirale pošto svojih državljanov in dešifrirale pretok informacij. Zlasti na področju, kjer se križa interes za ohranjanje zasebnosti na medmrežju s šifrirnimi metodami in interes držav za ohranjanje nadzora nad pretokom informacij, se kažejo navzkrižni interesi, ki zavirajo sprejemanje ustreznih tehnoloških standardov in tudi ustrezne zakonodaje o elektronskem poslovanju.

LITERATURA

Akademska in raziskovalna mreža Slovenije. 20.08.2004. *Registracija domen.* [URL: http://www.arnes.si/domene/registracija.html].

Čebulj, J. 1992. *Varstvo informacijske zasebnosti v Evropi in Sloveniji.* Ljubljana. Inštitut za javno upravo pri Pravni fakulteti.

Evropsko pravo. 2004. Ljubljana. Založniška hiša Primath. ISBN 961-6431-10-2.

Internet Corporation for Assigned Names and Numbers. 21.08.2004. [URL: http://www.ICANN.org].

Jerman-Blažič, Borka. 2001. *Elektronsko poslovanje na internetu. 1. Natis.* Ljubljana. Gospodarski vestnik.

Kajzer, Rok. 2005. *Hrvaški »gej imenik«. Delo 15.02.2005 št*. 37. Ljubljana.

Kalan, Barbara. 2002. *Zasebnost v računalniških omrežjih. Diplomska naloga.* Ljubljana. Visoka policijsko varnostna šola.

Kazenski zakonik RS in vdori v računalniški sistem. 20.03.2004. [URL: http://www.arnes.si/sicert/kz.htm].

Koželj, Samo 1995. *Sprememba teoretičnih osnov knjigovodstva ob prehodu na dajanje prednosti vsebini pred obliko. Doktorska disertacija.* Ljubljana. Ekonomska fakulteta.

Kuščer, Samo. 2004. *Revija Monitor 14/6 junij 2004.* Ljubljana. Informacijska varnost.

Makarovič, B. et.al. 2001. *Internet in pravo: izbrane teme s komentarjem zakona o elektronskem poslovanju in elektronskem. Podpisu.* Ljubljana. Pasadena.

Modelni zakon o elektronskem poslovanju. 1996 UNCITRAL; [URL: http://www.uncitral.org/english/texts/electcom/ml-ec.htm].

Obligacijski zakonik – OZ (Ur.l. RS, št. 83/2001, 32/2004)

Pavliha, Jerman-Blažič, Borka. 2001. *Zakon o elektronskem poslovanju in elektronskih podpisih (ZEPEP).* Ljubljana. Vlada Republike Slovenije. Center za informatiko.

Štrakl, Marjan. 2001 *Varnost in varnostna politika.* Ljubljana. Revija Sistem, marec 2001.

Toplišek, Janez. 1998. *Elektronsko poslovanje. 1.izdaja.* Ljubljana. Založba Atlantis 1.

Zakon o avtorskih in sorodnih pravicah – ZASP št. 120-01/94-1/26, Ljubljana 09.04.2004.

Zakon o elektronskem poslovanju in elektronskem podpisu - uradno prečiščeno besedilo – ZEPEP-UPB1 (Ur.l. RS, št. 98/2004).

Zakon o mednarodnem zasebnem pravu in postopku – ZMZPP (Ur.l. RS, št. 56/1999).

Zakon o pravdnem postopku – ZPP št. 710-01/95-4/6, Ljubljana, dne 25.03.1999, sprememba zakona št. 710-01/95-4/16 Ljubljana, dne 25.10.2002, naslednja sprememba zakona št. 710-01/95-4/28 Ljubljana, dne 19.12.2003.

Zakon o varstvu osebnih podatkov – ZVOP št. 210-01/89-3/20 Ljubljana, dne 08.07 1999, sprememba zakona št. 210-01/89-3/21 Ljubljana, dne 26.06.2001 in naslednja sprememba št. 210-01/89-3/25 Ljubljana, dne 15.07.2004.

Župan, Andrej. 2002. *Nevarnosti pri elektronskem poslovanju na internetu. Diplomsko delo*. Ljubljana. Ekonomska fakulteta.