UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

NEKATERI PRAVNI IN EKONOMSKI VIDIKI INTERNETA IN ELEKTRONSKEGA POSLOVANJA

Ljubljana, avgust 2003 JERNEJ KOZLEVČAR

IZJAVA

Študent Jernej Kozlevčar izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Kreša Puhariča in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, avgust 2003 Podpis_____

KAZALO

KAZALO TABEL IN SLIK

Kazalo tabel:

Kazalo slik:

UVOD

Živimo v času, v katerem sodobna tehnologija napreduje z neverjetno hitrostjo in ljudje vedno bolj pogosto uporabljamo njene dosežke in pridobitve. Najprej predvsem zaradi službenih obveznosti, zatem pa tudi zaradi osebnega zanimanja, življenjskih potreb, pa za razvedrilo in osebno zadovoljstvo. Največji napredek sodobne tehnologije in popularnosti njene uporabe trenutno zagotovo predstavlja internet in vse, kar je z njim povezano (različne vrste elektronskega poslovanja, domača uporaba, razvedrilo in zabava…). Ob tem moramo omeniti tudi razvoj računalniške tehnologije, ki je omogočila nastanek in razvoj računalnikov in omrežij v kakršnikoli obliki in kasneje tudi kot trenutno najbolj popularni svetovni splet. Uporabnikov sodobne tehnologije je bilo sprva razmeroma malo. Kasneje, z razvojem tehnologije, spoznavanjem njenih prednosti in neizbežnostjo uporabe, pa se je njihovo število hitro povečevalo.

Danes si je že težko zamisliti delovno mesto brez uporabe osebnega računalnika. Internet in vsa sodobna tehnologija vedno bolj pridobivajo na uporabni vrednosti. Uporabnikov ni več le nekaj tisoč, kot se je to dogajalo, ko je njegov razvoj šele dobro začel svojo pot, danes število uporabnikov interneta dosega nekaj sto milijonov.

In ravno tu nastopi težava. Z večanjem števila uporabnikov interneta in ostalih oblik sodobne tehnologije (osebni računalniki, različni tipi omrežij, terminali) je vedno več takšnih ljudi, ki ob uporabi sodobne tehnologije le-to želijo uporabiti v nelegalne namene. Večje število računalnikov in čedalje več omrežij, za katere skrbi relativno vedno manj strokovnjakov, samo povečuje možnosti različnih napak in nepravilnosti (vdori v omrežja, kraja podatkov, nepooblaščen dostop), ki jih bomo bolj podrobno spoznali v nadaljevanju diplomskega dela.

V času, ko se marsikdo pohvali, da živimo online[1], se ni nič spremenilo – vsaj kar se tiče elektronskega kriminala[2]. Morda je še celo huje. Tudi v virtualnem svetu obstajajo takšni, za katere zakoni ne veljajo ali pa iščejo pomanjkljivosti v njih. Del kulture, moralnih vrednot in etike se je prenesel tudi na virtualni svet, kjer je nelegalno početje v določenih primerih še lažje izvedljivo kot v resničnem svetu. Morda se bo primerjava virtualnega sveta z Divjim zahodom zdela smešna in neumestna, pa vendar. Zakoni, ki veljajo, se ne upoštevajo,

[1] Prevod besede online v primeren slovenski izraz oz. besedno zvezo bi izgubil na veljavi. Vsak, ki internet uporablja malo bolj pogosto, zagotovo dobro ve, kaj izraz pomeni in mu je bolj razumljiv kot npr. izrazi na zvezi, priključen, v direktni povezavi.
[2] Bolj natančno ga bom predstavil v tretjem poglavju.

roki pravice se je moč kaj hitro izogniti ali ji celo nasprotovati[3], glavne »nastopajoče« pa bi lahko označili kot dobre, slabe in grde, odvisno od namenov in interesov, ki jih zastopajo.

Tiste osebe, ki jim je kaj malo mar za pravila, ki veljajo v svetovnih omrežjih, delujejo nelegalno iz različnih vzgibov, razlogov in interesov. Dejstvo, da se zakoni pišejo šele potem, ko neka pojavna oblika kriminala postane moteč pojav, je v primeru elektronskega kriminala več kot očitno. Zaradi zapletene tehnologije in vrste drugih zadržkov (pravni, tehnični, etični) pa vse skupaj le ni tako enostavno, kot je to bilo včasih, ko so z zakoni uspešno in dokaj hitro zajezili vse vrste in tipe kriminala.

V svojem diplomskem delu sem se odločil predstaviti nekatere pravne vidike, ki urejajo področje interneta in različne oblike elektronskega poslovanja.

Neprimerno bi bilo, če bi svoje delo začel kar z navajanjem zakonov, zato v prvem poglavju najprej predstavim internet kot medij, ki je nekako sopovzročitelj naraščujočemu elektronskemu kriminalu. Zatem podrobneje predstavim zgodovino interneta in njegovo širjenje.

V drugem poglavju diplomskega dela bom obravnaval določujoče prvine elektronskega poslovanja, ki predstavlja potencialnega dediča celotnega poslovanja v širšem pomenu besede. Povrh vsega pa je prav elektronsko poslovanje najbolj izpostavljeno omenjenemu elektronskemu kriminalu.

V zadnjem poglavju predstavljam tematiko elektronskega kriminala in pravna orodja za njegovo preprečevanje – zakone, kar predstavlja tudi bistveni del moje diplomske naloge. Podrobneje predstavim elektronski kriminal, njegova področja in pojavne oblike. Predstavim tudi zakone, ki pravno urejajo področje elektronskega kriminala ter navedem nekaj resničnih primerov za lažje in boljše razumevanje tovrstnega kriminala.

Povezava internet – elektronsko poslovanje – zakoni se mi je ob opredelitvi zasnove diplomskega dela zdela zelo zanimiva, zato sem se tudi odločil za tako tematiko diplomskega dela.

[3] Dejstvo je, da so veljavni zakoni, ki urejajo elektronski kriminal, praviloma zastareli, nedoročeni in v veliko primerih sploh ne pokrivajo vseh kaznivih dejanj, ki lahko nastanejo.

1. INTERNET

Ko govorimo o internetu, mislimo na sestavljeno omrežje, ki vključuje različna omrežja in posameznike. Ne gre za en sam enoten sistem. Glede na obseg in število udeležencev je določljiv le okvirno. Možno ga je opredeljevati z različnih vidikov. Pravno-organizacijsko je povsem decentraliziran sestav. Le na nekaterih tehničnih področjih se kažejo prizadevanja po večji centralizaciji. Pa še v tem primeru gre bolj za dogovore o nujnih standardih, po katerih naj bi sistem deloval, kot pa za vodenje. Ker interneta neposredno in v celoti ne upravlja nobena država ali meddržavna organizacija, je dobra podlaga za razmišljanje o samostojnem, avtonomnem kibernetskem prostoru. Tako ga vidijo tudi že na pravnem področju, kjer pa vedno znova zadeva ob interese države, kot ozemeljskih tvorb (Toplišek, 1998, str. 8). Ob tem pa bi lahko tudi rekli, da gre za največje globalno sestavljeno omrežje povezav (Timmers, 1999, str. 10).

Več kot štirideset let nazaj sta matematika Manfred Kochen in Ithiel de Sola Pool kot prva znanstveno raziskovala »fenomen majhnega sveta« . V svojih raziskavah sta oblikovala omrežno strukturo in na takšen način razvila idejo o možganih sveta. Tako sta, ne da bi vedela, kakšen razvoj in obliko bo imela računalniška arhitektura, uspela oceniti potencial velikih omrežij in podatkovnih baz. Čeprav brez komunikacijskih mrež, ki jih srečujemo danes, sta Kochen in de Sola Pool uspela ugotoviti, da je svet v socialnem, ekonomskem in informacijskem smislu občutno manjši, kot nam daje občutek geografske velikosti. To sta poimenovala fenomen majhnega sveta (Westland, Clark, 1999, str. 53).

1.1. ZGODOVINA INTERNETA

Internet se je oblikoval leta 1969 kot ARPANET[4], in sicer kot rezultat vojaškega raziskovalnega projekta ameriškega obrambnega ministrstva (Westland, Clark, 1999, str. 275). Bil je zasnovan z namenom povezovanja vojaških, obrambnih in izobraževalnih institucij, ki so sodelovale pri raziskavah. Vse do začetka osemdesetih let se je uporabljal večinoma v akademske namene, vse dokler ni prišlo do uvedbe omrežja NSFNET[5], ki je predstavljal hrbtenico omrežja. Hrbtenica ali glavna oporna omrežja zagotavljajo visoko hitrost in velik obseg

[4] Advanced Research Projects Agency Network.
[5] National Science Foundation Network.

podatkovnih zvez med regionalnimi omrežji. NSFNET je povsem drugačno zasnoval model omrežja ter tako omogočil širitev matičnega omrežja do večjega števila uporabnikov. Osnovne razlike med modelom omrežja ARPANET in NSFNET so v Prilogi 1.

Velik korak naprej je bila tudi uvedba poenotenega prenosnega protokola TCP/IP, kar je bistveno prispevalo k rasti števila uporabnikov. Gre za standardni protokol, ki omogoča prenos podatkov po omrežju in s tem zagotavlja zanesljivost prenosa. Za lažje razumevanje navedimo primer dveh različnih tipov računalnikov, ki potrebujeta in morata uporabljati iste protokole, da se med seboj lahko sporazumevata (Kalakota, Whinston, 1997, str. 37).

Protokol za sporazumevanje v internetu je TCP/IP. TCP (Transport Control Protocol) pomeni protokol za nadzor prenosa, IP (Internet Protocol) pa pomeni protokol za internet in je osnovni standardni protokol interneta. Ta omogoča različnim računalnikom, ki so priključeni na internet, da komunicirajo drug z drugim. Vsak računalnik mora, če se hoče sporazumevati z drugim računalnikom na internetu, govoriti TCP/IP (Jerman-Blažič, 1996, str. 15).

Leto 1991 lahko označimo kot leto komercializacije interneta, saj je takrat Nacionalna znanstvena fundacija (NSF) del omrežja NSFNET dala v uporabo za komercialne namene (Coppel, 2000, str. 6).

Kateri dogodki so bistveno vplivali na razvoj interneta si lahko bolj natančno pogledamo v Tabeli 1, kjer je strnjena zgodovina interneta od začetka do današnjih dni. Pri tem seveda ne smemo pozabiti tudi elektronskega poslovanja, saj je prav internet tisti, ki omogoča njegov razvoj in širjenje, o čemer bo tekla beseda v poglavju o elektronskem poslovanju.

Tabela 1: Zgodovina interneta

Leto	Pomembni dogodki za zgodovino interneta
1961	Leonard Kleinrock z univerze MIT predstavi teorijo Packet-Switching[6] v svojem delu z naslovom: Pretok informacij v velikih komunikacijskih omrežjih.
1966	Kot načrt je predstavljen ARPANET v raziskavi z naslovom: Naproti kooperativnim omrežjem skupnih računalnikov.
1968	Packet-switching omrežje je predlagan za ARPANET.
1969	Ameriško obrambno ministrstvo naroči izvedbo raziskave o omrežju ARPANETU. Omrežje X.25 se razvije za potrebe študentov in fakultete. Poslano je prvo sporočilo od ene lokacije do druge (Univerza UCLA in Standfordski raziskovalni inštitut).
1970	ARPANET strežniki pričnejo uporabljati NCP protokol.
1971	ARPANET se razširi na petnajst lokacij (triindvajset gostiteljskih strežnikov). Ray Tomlison razvije program za elektronsko pošto, ki omogoča pošiljanje sporočil po omrežju. Program je nastal na osnovi dveh eksperimentalnih programov.
1973	Prva mednarodna povezava v ARPANET. Bob Metcalfe v svoji doktorski disertaciji predstavi idejo o Ethernetu. Predstavi se specifikacija protokola za prenos podatkov za potrebe interneta. Elektronska pošta predstavlja 75 % vsega prometa ARPANETA.
1974	Vint Cerf in Bob Kahn predstavita delo: Protokol za paketno komunikacijo med omrežji, kjer natančno predstavita TCP.
1980	Prvi računalniški virus povzroči prekinitev delovanja računalniškega sistema.
1981	Omrežje BITNET začne delovati, in sicer s sedežem v Mestni univerzi v New Yorku in s prvo povezavo z Univerzo Yale. Omogoča prenos elektronskih sporočil, dokumentov in imenikov gostiteljev.
1982	Protokola TCP in IP, bolj znana kot TCP/IP se uveljavita za poenoteni protokol po ARPANETU. Tu prvič nastopi definicija interneta in sicer kot povezava več omrežij, še posebej tistih, ki uporabljajo TCP/IP ali pa kot povezani TCP/IP interneti.
1984	Uveden je sistem poimenovanja domen (DNS). Število gostiteljskih strežnikov preseže 1.000.

[6] Gre za protokol, v katerem se datoteka pred začetkom prenosa razdeli v več paketov. Vsak paket je poslan posamezno in lahko do cilja pride po različnih poteh. Ko vsi paketi pridejo na cilj, se sestavijo v izvirno datoteko.

1985	15. marca postane Symbolics.com prva registrirana domena. Sledijo ji: cmu.edu, purdue.edu, rice.edu, ucla,edu, css.gov, mitre.org.
1986	Uvedeno je omrežje NSFNET in pet centrov s superračunalniki[7] za zagotavljanje zadostne procesorske moči.
1987	Število gostiteljev preseže 10.000.
1988	Jakko Oikarinen razvije IRC[8]. Povezava do NSFNET je nadgrajena v T1 (1,544 Mbps). Prvi internetni črv je okužil 6.000 od skupno 60.000 gostiteljev. ARPA ustanovi CERT kot odgovor na incident s črvom.
1989	Število gostiteljev preseže 100.000.
1990	Omrežje ARPANET se razpusti, tako ostaja samo še internet. World.std.com postane prvi komercialni ponudnik dostopa do interneta (modemska povezava).
1991	Tim Berners-Lee ja razvil WWW. Prednost storitve WWW predstavljam v Prilogi 2. Razvita je bila storitev Gopher.
1992	Število gostiteljskih strežnikov preseže 1.000.000. Univerza v Nevadi predstavi orodje za brskanje, Veronica. Pojavi se izraz deskanje, surfanje, brskanje, brkljanje[9] po internetu.
1993	NSF ustanovi InterNIC, ki zagotavlja storitve s področja interneta (registracijski servis, upravljanje podatkovnih baz, informacijske storitve). Z uvedbo komercialne rabe spletnega brskalnika MOSAIC se omrežje prične uporabljati v komercialne namene. Storitev WWW doseže 341.634 % letno stopnjo rasti prometa, brskalnik Gopher pa 977 %. Bela hiša predstavi svojo spletno stran, predsednik ZDA je dosegljiv na president@whitehouse.gov. Poslovni svet in mediji pričnejo izpostavljati internet.
1994	Prvi trgovski centri se pojavljajo na internetu. Vladimir Levin je bil prvi javnosti znan bančni ropar, ki je svoj rop zagrešil s pomočjo omrežja. Pojavijo se prva spam[10] elektronska sporočila.
1995	Uporaba interneta za komercialne namene začne silovito pridobivati na veljavi. Amazon.com je prodal prvo knjigo preko spletne prodaje. Spletna storitev WWW prehiti protokol FTP kot

[7] Gre za računalnik ali skupino računalnikov, ki imajo posebno strojno opremo za doseganje velikega števila računskih operacij.
[8] Okrajšava za Internet Relay Chat, ki je program za omogočanje pogovora med uporabniki interneta iz različnih delov sveta.
[9] Prevod v pravem pomenu besede bi sicer pomenil deskanje, v slovenščini pa se je uveljavil predvsem brskanje.
[10] Gre za elektronska sporočila, ki so praviloma komercialne narave in so pošiljana brez dovoljenja in vednosti prejemnika.

	storitev z največ prometa glede na število paketov in glede na število bitov.
1996	Vojna med spletnima brskalnikoma Netscape Navigator in Internet Explorer je vedno ostrejša.
1997	Po svetu je 77 milijonov uporabnikov interneta. Gre za prvi medij, ki je potreboval manj kot pet let za dosego 50 milijonov uporabnikov.
1998	Prva podjetja že aktivno pričenjajo z aplikacijami elektronskega poslovanja. Po svetu je 133 milijonov uporabnikov. Lahko ugotovimo, da se stopnja rasti počasi umirja.
1999	205 milijonov uporabnikov interneta. Razvijajo se poslovne aplikacije za povezovanje med vsemi subjekti elektronskega poslovanja.
2000	Vodilna podjetja po svetu že izrabljajo koristi internetnega poslovanja.
2001	Po svetu je 365 milijonov uporabnikov, v Sloveniji pa 300.000 uporabnikov. Pojmi kot so elektronsko in internetno poslovanje so vedno bolj prisotni v podjetjih. Elektronski kriminal sledi razvoju tehnike in je korak pred njo.
2003	Skupno število uporabnikov interneta po svetu znaša po najnovejših podatkih kar 652 milijonov, kar presega vse prejšnje projekcije priznanih podjetij za analizo in napovedovanje števila uporabnikov interneta po svetu (Forrester Research, Nielsen Media, Internet Trends). V Sloveniji se ta številka giblje okoli 640.000. Skupni prihodki od internetnega elektronskega poslovanja po svetu naj bi znašali približno štiri milijarde ameriških dolarjev. Države sveta aktivno delujejo na področju zakonodaje, ki ureja elektronski kriminal. Oblasti pregona tovrstnega kriminala so vedno bolj organizirane in množične.

Vir: Coppel, 2000, str. 6; Hoffman, 1996, str. 183-193; Kalakota, Whinston, 1999, str. 35-37; Meeker et al., 2000, str. 10-12; Westland, Clark, 1999, str. 275-278, 575-580; Raba interneta v Sloveniji, 2003; Internet World Usage Statistics, 2003.

1.2. ŠTEVILO UPORABNIKOV INTERNETA PO SVETU

Iz strnjenih navedkov (Tabela 1) je razvidno, da je skupno število uporabnikov interneta po svetu zelo hitro raslo. Za boljšo primerjavo si poglejmo primerjavo s televizijo, ki je potrebovala trinajst let, ali radiom, ki je potreboval osemintrideset let, da je dosegel petdeset milijonov uporabnikov. Internetu je to uspelo v petih letih (Meeker et al., 2000, str. 11). Vsako leto so različna podjetja in organizacije s projekcijami poskušala ugotoviti, kakšno bo gibanje števila uporabnikov interneta v prihodnosti in so se vedno zmotila v svojih napovedih. Dejansko število uporabnikov je bilo v napovedovanem obdobju praviloma vedno višje od tistega, ki se je prikazoval v projekcijah.

Dejansko število uporabnikov po celinah sveta je prikazano v Tabeli 2. Podatki veljajo za 11. julij 2003, kar pomeni, da so zelo točni ter tako odpravljajo vpliv spremembe in rasti števila uporabnikov, ki nastopi tudi v zelo kratkem obdobju (praviloma na tri mesece). V Tabeli 3 so tudi podatki za pomembnejše države, saj je veliko takšnih primerov, kot npr. Amerika, kjer posamezna država ali pa geografska enota predstavlja velik delež preučevane spremenljivke ter tako vpliva na rezultat posamezne celine. S takšnim načinom prikaza pa tak vpliv izločimo.

Omeniti velja še, da pri merjenju podatkov prihaja do težav zaradi različnih metodologij. V praksi se pojavlja vprašanje, kdo se šteje za uporabnika interneta in kako pogosto v nekem časovnem obdobju mora ta oseba internet uporabljati, da ga lahko uvrstimo v skupino aktivnih uporabnikov. Nadalje povzročajo težave pri merjenju tisti uporabniki, ki imajo dostop do interneta, vendar ga ne uporabljajo. V zadnjem času se je nekako uveljavilo pravilo, da se za uporabnika interneta šteje oseba, ki je uporabila internet v zadnjem mesecu.

Ravno zaradi težav z uporabo metodologije se v rezultatih raziskav, ki so bile izvedene v novejšem času, pojavlja vedno več podatkov. Tako lahko npr. na internetni strani www.ris.org najdemo podatke o dnevni, tedenski in mesečni uporabi interneta. Gre za spletno stran, ki ažurno spremlja rabo interneta v Sloveniji, kar je tudi kratica za ime strani. V drugih raziskavah se pojavljajo še vrednosti o povprečni uporabi na dan, mesec, številu bitov prenesenih preko interneta, namenu uporabe, načinu dostopa, prvih uporabnikih ipd.

Drugo težavo (predvsem v manj razvitih državah sveta) predstavlja pomanjkanje ustrezne infrastrukture (oprema, tehnologija, zaposleni,

pristojnosti, zakonske omejitve) in pristojnih služb za zagotavljanje podatkov za izvedbo raziskave. Vsekakor pa se razmere z razvojem interneta povsod izboljšujejo, saj so v večini držav že ugotovili, da s spremljanjem števila uporabnikov ne dobivajo le nepomembnih številk, ampak gre tudi za dragocene informacije o tem, kako se lahko razvija elektronsko poslovanje in kakšno število uporabnikov lahko pričakujejo. Nadalje lahko na osnovi teh podatkov ocenjujemo število elektronskega kriminala in skupen promet od elektronskega poslovanja. Na tak način lahko države že vnaprej organizirajo potrebna sredstva v obliki opreme, infrastrukture, zaposlenih, ki bodo pokrivali posamezna področja (pravna in ekonomska).

Podatki iz Tabel 2 in 3 kažejo, da se je internet najprej uveljavil v ekonomsko najbolj razvitih državah sveta, kar najbolje prikazuje podatek o deležu prebivalstva (penetracija). Državi z velikim potencialom naraščanja števila uporabnikov interneta sta predvsem Kitajska in Indija, ki imata hkrati zelo nizek delež prebivalstva, ki uporablja internet.

Precejšnjo razliko lahko ugotovimo tudi v primerjavi držav članic Evropske unije in ostalih evropskih držav, kar opozarja na to, da je razvitost držav Evropske unije na področju zagotavljanja dostopa in uporabe interneta bistveno višja kot v državah, ki niso članice Evropske unije.

Kot posledica razlik deleža uporabnikov interneta med državami, se je tudi dejavnost držav na področju pravnih vidikov interneta in elektronskega poslovanja razvijala skladno z večanjem deleža uporabnikov interneta. Tako so se države, kjer je delež uporabnikov interneta visok, veliko hitreje začele srečevati s pravnimi vidiki, ki jih uporabniki srečujejo pri vsakodnevni uporabi tega medija. Enako velja tudi za elektronsko poslovanje, ki s širitvijo interneta povečuje svoj obseg, hkrati pa sili vse vrste uporabnikov in pristojne organe k urejanju zakonodaje, da lahko poslovanje poteka čimbolj nemoteno. Bolj natančno bom pravne vidike predstavil v nadaljevanju diplomskega dela v tretjem poglavju.

Tabela 2: Število uporabnikov interneta po regijah sveta

Regija ali država	Populacija (2003)	Uporaba (2000)	Uporaba (11.7.2003)	Rast v % (2000-2003)	Delež glede na svetovne uporabnike v %	Delež prebivalstva v % (penetracija)
Afrika	879.855.500	4.514.400	8.073.500	78,8	1,2	0,9
Amerika	864.854.400	126.164.800	228.775.858	81,3	35,1	26,5
Azija	3.590.196.700	114.303.000	200.319.063	75,3	30,7	5,6
Evropa	722.509.070	103.075.900	190.297.994	84,6	29,2	26,3
Srednji Vzhod	259.318.000	5.272.300	12.019.600	128,0	1,8	4,6
Oceanija	31.528.887	7.619.500	13.058.832	71,3	2,0	4,6
SKUPAJ	6.348.262.557	360.949.900	652.544.847	80,8	100,0	10,3

Vir: Internet World Stats, 2003; lastni izračuni.

Tabela 3: Število uporabnikov interneta po posameznih državah sveta

Regija ali država	Populacija (2003)	Uporaba (2000)	Uporaba (11.7.2003)	Rast v % (2000-2003)	Delež glede na svetovne uporabnike v %	Delež prebivalstva v % (penetracija)
ZDA	291.639.900	95.354.000	176.418.380	85,0	27,0	60,5
Kitajska	1.311.863.500	22.500.000	59.100.000	162,7	9,1	4,5
Japonska	127.708.000	47.080.000	57.520.708	28,7	8,8	45,0
Indija	1.067.421.100	5.000.000	16.580.000	231,6	2,5	1,6
Evropske države (razen EU)	344.506.670	16.279.100	28.252.328	73,5	4,3	8,2
Države EU	378.002.400	86.796.800	162.045.666	86,7	24,8	42,9

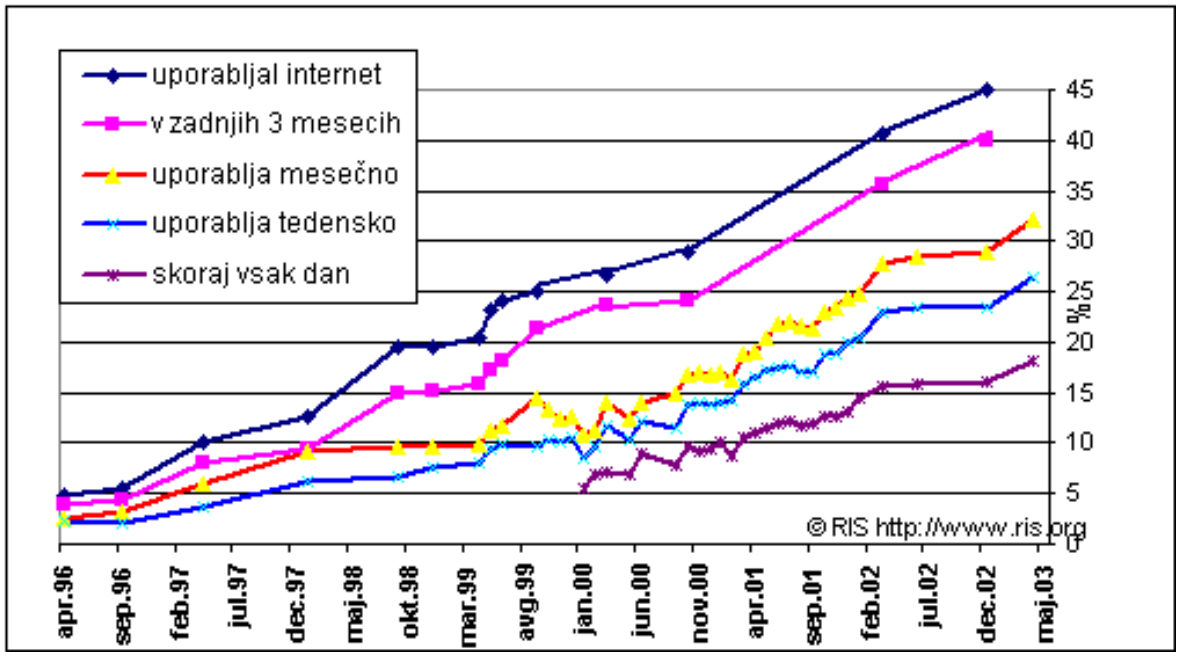
Vir: Internet World Stats, 2003; lastni izračuni.

1.3. RAZMERE V SLOVENIJI

Slovenija je med evropskimi državami, ki niso članice Evropske unije, po deležu prebivalstva, ki se štejejo za uporabnike interneta, na visokem petem mestu. Zaostaja samo za: Islandijo, Švico, Norveško in Estonijo. Po deležu uporabnikov je Slovenija na ravni povprečja držav Evropske unije. Tudi po deležu gospodinjstev Slovenija ne zaostaja preveč za povprečjem Evropske unije. Število uporabnikov se po projekcijah izvedenih v prejšnjih letih povečuje po najbolj optimističnem scenariju, ki je bil takrat predstavljen. To lahko utemeljujemo z nizko ceno računalniške opreme, nizkimi stroški dostopa in uporabe interneta, aktivno državno politiko, vplivom medijev, raznovrstnostjo in raznolikostjo uporabe in storitev interneta.

Na Slikah 1 in 2 prikazujem nekaj podatkov za število uporabnikov v Sloveniji.

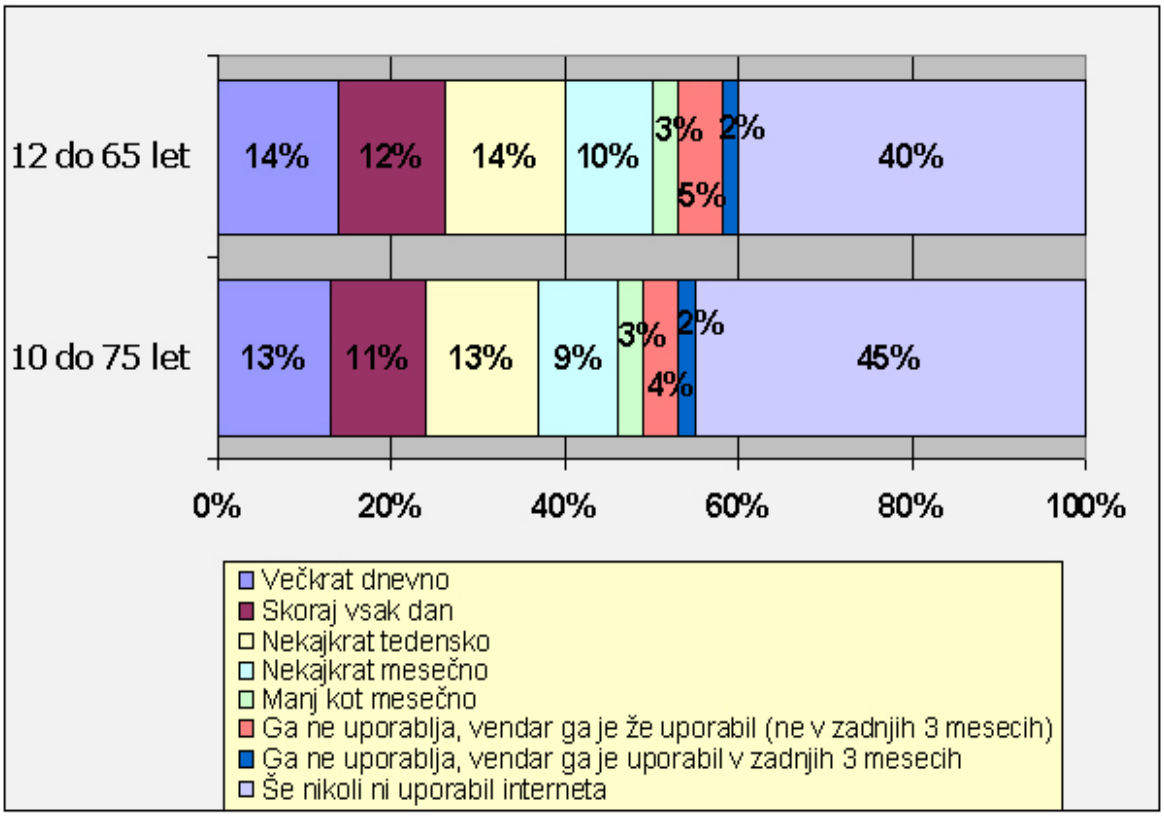
Slika 1: Uporabniki interneta v celotni populaciji v %



Vir: Raba interneta v Sloveniji, 2003.

Na Sliki 1 je prikazan delež uporabnikov interneta v Sloveniji glede na pogostost uporabe interneta v obdobju od aprila 1996 do maja 2003. Razdeljeni so na dnevne, tedenske, mesečne, trimesečne in prve uporabnike.

Slika 2: Uporabniki interneta v populaciji glede na pogostost uporabe v % (december 2002) razdeljeni v dve starostni skupini (prva od 10 do 75 let in druga od 12 do 65 let)



Vir: Internet in slovenska država v letu 2002, 2003.

Glede na namen pogosto oziroma redno uporablja internet tri četrtine obravnavanih za dopisovanje s prijatelji in znanci, dve tretjini za branje dnevnih novic, polovica za surfanje kar tako, dobra tretjina (37 %) za lokalne informacije, informacije o prireditvah in prenašanje glasbe z interneta, četrtina za informacije o kino sporedih, petina za nakupovanje, naročanje, rezervacije preko interneta (17 %), informacije o tv sporedih, šestina za borzne informacije (16 %), iskanje zaposlitve (15 %), malo (7 %) pa za igre prek interneta, še manj (4 %) za igre na srečo, najmanj (2 %) pa za služenje denarja s surfanjem.

2. ELEKTRONSKO POSLOVANJE

Ker bomo v nadaljevanju diplomskega dela govorili o elektronskem kriminalu, lahko nekaj povem tudi o elektronskem poslovanju, ki je najbolj izpostavljeno elektronskemu kriminalu. Elektronsko poslovanje ne pozna meja, je rezultat sodobne tehnologije in tehnike. Ljudje pravzaprav ne vedo točno, kaj pomeni pojem elektronsko poslovanje. Med prebiranjem različne strokovne literature sem zasledil različne razlage.

Na slovenskih tleh smo izraz prevzeli po angleškem »electronic commerce«, ki ga uporabljamo kot splošni izraz za vse možne vrste elektronskega poslovanja (Toplišek, 1998, str. 4).

Njegova definicija se iz dneva v dan razlikuje, dejstvo pa je, da se počasi vse poslovanje spreminja v elektronsko. Tako na eni strani prevzema lastnosti poslovanja, po drugi pa lastnosti elektronskega sveta. Prevzema prednosti in slabosti obeh. Za svojo širitev si je našel pravi medij, internet.

Pogosto se dogaja, da se pojma internet in elektronsko poslovanje uporabljata v splošnem jeziku kot sopomenki, ker ljudje preprosto ne poznajo prave razlike med njima.

Splošna definicija elektronskega poslovanja je:

Opravljanje katerekoli poslovne dejavnosti v elektronski obliki ne da bi pri tem obvezno obstajala denarna transakcija (Brabham, 1999, str. 6).

Lahko bi tudi rekli, da gre za katerokoli obliko poslovne transakcije, v kateri stranke delujejo elektronsko, namesto da bi si pošiljale fizična sporočila ali pa da bi bile v neposrednem stiku.

Natančnejša opredelitev pojma elektronskega poslovanja obsega naslednje sestavine:

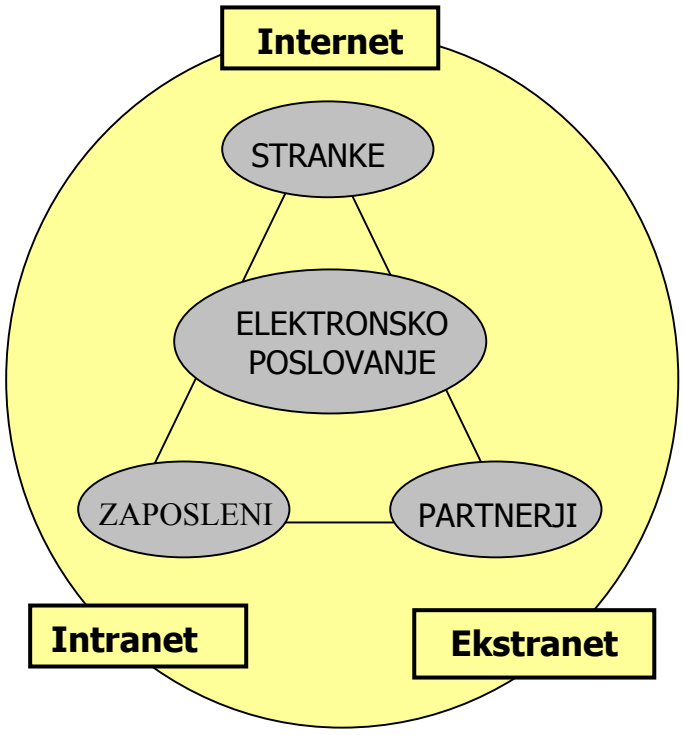
1. Način dela predstavlja elektronsko izmenjevanje podatkov (v neki meri tudi samodejne transakcije, kot npr. prenos finančnih sredstev, avtomatizirana plačila, informacijski tokovi).

2. Vsebina poslovanja je skoraj neomejena, saj lahko vključimo blago, storitve, plačila, pred in poprodajne aktivnosti, delovanje državnih organov in javnih služb.

3. Tri glavne skupine udeležencev predstavljajo podjetja / podjetniki, državne / javne službe in posamezniki (potrošniki, uporabniki). Poslovanje podjetja poteka znotraj teh skupin in med njimi. Opaznejše je prav poslovanje med posamezniki, njegov glavni spodbujevalec je prav internet s svojimi odprtimi, neomejenimi možnostmi (Toplišek, 1998, str. 4).

Možne oblike elektronskega poslovanja prikazujem v Sliki 3. Iz nje je razvidno, da elektronsko poslovanje ni le poslovanje med dvema partnerjema. Obsega tudi izmenjavo informacij in komunikacijo med zaposlenimi v podjetju preko intraneta, sodelovanje s poslovnimi partnerji po ekstranetu in v zadnjem času najbolj razširjeno komunikacijo s strankami po internetu (Vavan, 2001, str. 7).

Slika 3: Oblike elektronskega poslovanja



Vir: Vavan, 2001.

2.1. OBSEG ELEKTRONSKEGA POSLOVANJA

Elektronsko poslovanje vključuje veliko različnih vrst poslovanja, ki so našteta na naslednji strani. Kot smo že spoznali, je elektronsko poslovanje zelo širok pojem in je ob obravnavi vprašanj, ki se tičejo le določenih vrst elektronskega poslovanja, bolje uporabiti izraze, ki takšno poslovanje označujejo bolj funkcionalno in se nanašajo na posamezne vrste elektronskega poslovanja (Toplišek, 1998, str. 5):

1. elektronsko trgovanje (različni načini trgovanja brez posrednega stika in fizične izmenjave),
2. elektronsko bančništvo (online bančne storitve, bančništvo na daljavo),
3. elektronsko plačevanje (e-čeki, e-gotovina, e-kartice, bankomati),
4. elektronski finančni prenosi (komercialni, medbančni, relacije posameznik – organizacija – finančne institucije),
5. delo na daljavo (opravljanje delovnih obveznosti na daljavo, brez potrebne fizične prisotnosti, če narava dela to seveda omogoča),
6. elektronsko založništvo (celovita storitev založništva),
7. elektronska arbitraža (posredovanje, pomiritveni postopek, mediacija, reševanje sporov),
8. elektronska ponudba (katalogi, videotekst, multimedija),
9. elektronske vloge (vloge s področja sodstva, uprave),
10. elektronsko zavarovalništvo (zavarovalniška storitev brez klasičnega posrednika – zavarovalnega agenta in z izkoriščanjem prednosti medija),
11. elektronsko naročanje (letalske karte, turistične storitve, naročila borznim posrednikom),
12. nematerializirano poslovanje z vrednostnimi papirji (nakup, prodaja in upravljanje z vrednostnimi papirji),
13. elektronsko borzno poslovanje (borzno poslovanje),
14. elektronska prodaja (maloprodaja, veleprodaja, potrošniška, distribucijska),
15. notranje elektronsko poslovanje (znotraj same organizacije),
16. poprodajne aktivnosti (elektronska navodila, svetovanje, nasveti, stik s kupcem, pomoč in podpora, reševanje reklamacij, oskrba z rezervnimi deli).

Meja med različnimi vrstami elektronskega poslovanja je včasih zelo težko določljiva. Podatki, ki se pojavljajo o obsegu transakcij elektronskega poslovanja, so zaradi različnih definicij in razumevanj pojma elektronskega poslovanja zelo različni. Nekateri pod tem pojmom pojmujejo samo vse kar je

povezano z internetom, drugi samo internetno prodajo, tretji celotno elektronsko poslovanje. Kakorkoli pa se podatki analizirajo, je dejstvo, da se vedno več prihodkov ustvarja s pomočjo takšnega načina poslovanja. Samo internetno elektronsko poslovanje je v letu 2000 ustvarilo 657 milijonov ameriških dolarjev prihodkov. V letu 2004 naj bi se ta številka gibala okoli 6,8 milijarde dolarjev, pri čemer v veliki meri še vedno večino prihodkov na takšen način poslovanja ustvarijo ZDA, približno polovico (Forrester Research, 2003).

2.2. KOMISIJA ZDRUŽENIH NARODOV ZA MEDNARODNO TRGOVINSKO PRAVO (UNCITRAL)[11] IN ELEKTRONSKO POSLOVANJE

Uncitral je pravno telo znotraj organizacije Združenih narodov za področje mednarodnega trgovinskega prava. Generalna skupščina Združenih narodov je pooblastila UNCITRAL za harmonizacijo in poenotenje mednarodnih trgovinskih zakonov. To UNCITRAL dosega na naslednji način:

1. Usklajevanje delovanja organizacij na področju mednarodnega trgovinskega prava in spodbujanje k sodelovanju med njimi.
2. Promoviranje obsežnega sodelovanja na področju obstoječih mednarodnih konvencij in splošno sprejemanje obstoječih vzorčnih in enotnih zakonov.
3. Priprava in širitev sprejemanja novih mednarodnih konvencij, vzorčnih in enotnih zakonov in širitev kodifikacije in splošno sprejemanje strokovnih izrazov, navad in običajev s področja mednarodnega trgovanja.
4. Zagotavljanje enotne razlage in uvedbe mednarodnih konvencij in enotnih zakonov na področju mednarodnega trgovinskega prava.
5. Zbiranje in širjenje informacij o zakonih držav po svetu in sodobnih zakonskih sprememb, vključno s tožbenimi zakoni s področja mednarodnega trgovinskega prava.
6. Ustanovitev in ohranjanje tesnih stikov s Konferenco Združenih narodov na področju trgovine in razvoja.
7. Sodelovanje z ostalimi organi Združenih narodov in agencijami s področja mednarodnega trgovanja.
8. Izvajanje dejanj, ki bi lahko bila koristna za izpopolnjevanje delovanja.

V okviru UNCITRALA je organiziranih tudi šest delovnih skupin, med katerimi četrta delovna skupina od leta 1997 pokriva področje elektronskega poslovanja.

[11] United Nations Commision on International Trade Laws.

Bolj natančno je razvoj delovne skupine, ki nosi oznako IV, tekom let potekal na naslednji način (UNCITRAL Working Groups, 2003):

1973 – 1987 Mednarodni vrednostni papirji (obveznice, menice, čeki)
1988 – 1992 Mednarodna plačila
1993 – 1996 Računalniška izmenjava podatkov (Electronic Data Interchange)
1997 – danes Elektronsko poslovanje

Ta delovna skupina je, kot je razvidno iz zgornjega kronološkega zapisa, od leta 1973 dalje, ko je pričela z obravnavo mednarodnih vrednostnih papirjev, pa do današnjih dni, sledila aktualnim razmeram in spremembam s področja mednarodnega trgovanja. Tako v zadnjem času spremlja področje elektronskega poslovanja.

2.2.1. VZORČNI ZAKONI UNCITRALA

Leta 1996 je UNCITRAL izdal vzorčni zakon o elektronskem poslovanju. Vzorčni zakon naj bi zastopal interese vseh ljudi, posebej tistih iz držav v razvoju. Tudi v Sloveniji so se ob pripravi Zakona o elektronskem poslovanju in elektronskem podpisu, o katerem bomo bolj natančno spregovorili v poglavju 3.6., zgledovali po vzorčnem zakonu UNCITRALA.

Vzorčni zakon Komisije Združenih narodov za mednarodno trgovinsko pravo o elektronskem poslovanju nima nobene pravne veljave, saj služi samo kot model zakona, ki ga lahko uporabijo sodne oblasti po svetu. Po njem so se zgledovale naslednje države: Avstralija, Bermudski otoki, Ekvador, Filipini, Francija, Hong Kong, Indija, Irska, Južna Koreja, Kolumbija, Nova Zelandija, Pakistan, Singapur, Slovenija, Tajska. Kanada in ZDA pa so pri sprejemanju zakonodaje s področja elektronskega poslovanja delovale v skladu z njim (Chuach, 2001, str. 176).

Vzorčni zakon o elektronskem poslovanju obsega strani od ena do devet, vsebino pa dopolnjujejo še poglavja s pojasnili o uzakonitvi (Giude to Enactment[12]) na straneh od devet do petinštirideset.

[12] Gre za posebno poglavje objavljeno poleg samega vzorčnega zakona (elektronsko poslovanje, elektronski podpis), kjer je po posameznih delih bolj natančno predstavljen sam zakon ter njegova čim lažja uzakonitev.

Pojasnila o uzakonitvi obsegajo:

1. predstavitev vzorčnega zakona,
2. komentar posameznih členov:

- splošne določbe,
- uporaba pravnih zahtev za elektronska sporočila (ročna pisava, podpis, izvirnik),
- komunikacijo elektronskih sporočil (funkcija, sprejem, prepoznavanje, prenos in čas elektronskih sporočil) (UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996).

Leta 1998 je bil vzorčni zakon o elektronskem poslovanju dopolnjen s členom 5 bis, ki pravno ureja status sklicevanja na obstoječe dokumente.

UNCITRAL je leta 2001 sprejel še vzorčni zakon o elektronskem podpisu, ki ravno tako vključuje pojasnila za lažjo, učinkovito in primerno uzakonitev. Vzorčni zakon sam obsega strani od ena do šest, od strani sedem do dvainsedemdeset pa je drugi del s pojasnili o uzakonitvi.

Pojasnila obsegajo:

1. predstavitev vzorčnega zakona:

- namen in izvor vzorčnega zakona,
- vzorčni zakon kot orodje za skladnost zakonov,
- glavni komentarji o elektronskem podpisu (namen elektronskega podpisa, digitalni podpis in ostali elektronski podpisi),
- glavne značilnosti zakona (zakonodajna narava, povezava z vzorčnim zakonom o elektronskem poslovanju),
- sodelovanje UNCITRAL-ovega sekretariata,

2. komentar posameznih členov (UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001).

Generalna skupščina Združenih narodov si prizadeva za uveljavitev vzorčnih zakonov po svetu, za njihovo splošno znanost in dostopnost, saj ugotavlja, da se vedno večje število transakcij mednarodne menjave izvaja s pomočjo elektronske izmenjave podatkov in drugih načinov komunikacije, ki jim navadno rečemo elektronsko poslovanje. Elektronsko poslovanje pomeni alternativo papirnim metodam komunikacije in shranjevanja informacij.

2.2.2. ARBITRAŽA[13]

Mednarodne arbitraže, organizirane po svetu lahko veliko svojih storitev izvajajo kar online. Te storitve so lahko:

- objava arbitražnih klavzul ali dogovorov,
- nepristranski izbor sodnega postopka,
- zabeležba priseg in izjav,
- določanje datumov obravnav,
- online pričevanja ali izjave prič,
- online obrambni zagovor dokumentacije,
- kratka razlaga tožbene reči,
- predstavitev trditev in dokazov,
- pogajanja o času zasedanja,
- predložitev vprašanj in navodil razsodnikov,
- dogovor o načinu odškodnine (Naimark, 2002, str. 6).

Naštete storitve v primeru arbitraže se v določenih primerih lažje in hitreje izvajajo online, kot pa na tradicionalen način. Predvsem to velja za objave, obvestila, zabeležbo listin in dokumentov, dogovor o zasedanju, dogovor o načinu odškodnine. Še vedno pa velja, da stik in zaslišanje v živo online metode (še) ne morejo nadomestiti (Naimark, 2002, str. 7).

V Sloveniji je organizirana stalna arbitraža pri Gospodarski zbornici Slovenije. Gre za samostojno in neodvisno arbitražno institucijo, ki v skladu s svojim Pravilnikom o arbitražnem postopku obravnava naraščajoče število mednarodnih sporov in tudi zagotavlja storitve za reševanje sporov v skladu z Arbitražnimi pravili UNCITRAL (Pravila za vodenje postopkov v skladu z arbitražnimi pravili UNCITRAL, 2003, str. 1-11).

3. PRAVNI VIDIKI INTERNETA IN ELEKTRONSKEGA POSLOVANJA

Napredku tehnologije in medijev ne sledi z enako hitrostjo pravna ureditev novega navideznega okolja. V mnogih državah so zakoni še nespremenjeni in komaj razumejo obstoj »virtualnega« sveta v obliki interneta, kriminal, ki

[13] Razsodišče v nesodnih sporih.

nastaja v elektronski obliki skušajo kaznovati po obstoječi zakonodaji, pri čemer pogosto prihaja do težav. Težko je npr. enačiti fizično tatvino s tatvino, izvedeno s pomočjo računalnika in / ali omrežja, saj na eni strani predstavljata enak prestopek, po drugi strani pa je zaradi načina izvedbe in dokazovanja postopek precej bolj zapleten. Države v današnjem času aktivno delujejo na tem področju, prvi rezultati se kažejo v obliki na novo izdanih zakonov ali pa popravkov obstoječe zakonodaje, kar bomo spoznali malo kasneje (Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002).

3.1. OPREDELITEV ELEKTRONSKEGA KRIMINALA

Računalniški ali elektronski kriminal se smatra kot nelegalno, neetično in nepooblaščeno ravnanje ljudi v zvezi z avtomatiziranimi postopki, prenašanjem podatkov, uporabo računalniških sistemov in omrežij (Lunker, 2001, str. 2).

Elektronski kriminal kot škodljivo delovanje izvršeno s pomočjo ali pa proti računalniku ali omrežju se razlikuje od zakonov, ki veljajo na svetu, v štirih stvareh:

1. Lahko se jih je naučiti.
2. Zahtevajo le malo sredstev glede na to, kakšno škodo lahko povzročijo.
3. Za izvedbo kriminala pogosto ni potreba fizična prisotnost.
4. Pogosto se izkaže, da takšna dejanja niso povsem v nasprotju z zakonom.

3.2. FORMALNI PRAVNI VIRI

Vprašamo se lahko, če so potrebni novi zakoni, ki naj urejajo najpomembnejša pravna vprašanja elektronskega sveta. Ali obstoječa zakonodaja dovolj dobro ureja področje elektronskega sveta? Nadalje pa lahko ugotavljamo pomembnost dejstva, da je k izredni rasti interneta veliko prispevalo tudi pomanjkanje centralizacije oblasti in pristojnosti, ki bi skrbela za nadzor in delovanje interneta že od njegovega zgodnjega začetka.

Kdorkoli, ki ima dostop do računalnika in telefonskega ali podobnega omrežja, se lahko poveže na internet. Kazalniki o širjenju interneta ustvarjajo potrebo po njegovem nadzorovanju. Sistemi, razkropljeni po svetu, imajo različna pravila, ki veljajo za dejanja uporabnikov. Ti uporabniki so v večini držav popolnoma

neodvisni v svoji odločitvi ali (ne)uporabljajo sistem, katerega pravila se jim zdijo primerna oz. neprimerna za njih. Takšna možnost prostega odločanja pogosto pripelje do neprimernega vedenja uporabnikov. Prav tako pa v pomanjkanju primernega pravnega okvirja sistemski administratorji oz. tisti, ki v kakršnikoli obliki skrbijo za sistem, težko pregledujejo in nadzirajo nepravilno vedenje posameznih uporabnikov, kot so npr. prevare, uničevanje (internet strani, podatkov, dokumentov, računalniškega sistema), zlorabe, žalitve, izsiljevanja, kar pogosto oteži življenje velikemu število online uporabnikov (Lunker, 2001, str. 5).

Naveden primer v prejšnjem odstavku mojega diplomskega dela je resen, saj vsak element nezaupanja v internetu lahko povzroči, da se ljudje izogibajo poslovanju na internetnih straneh in tako neposredno vplivajo na počasnejše širjenje elektronskega poslovanja. Zloraba interneta kot odličnega komunikacijskega medija lahko v določenih situacijah privede tudi do neposrednega škodovanja družbi sami. Kot primer navedimo neplačevanje davkov iz naslova elektronskega poslovanja, kar ima lahko škodljive posledice na fizično poslovanje in na prihodke države. Kot drugi primer pa navedimo teroriste, ki uporabljajo internet za ustvarjanje zarot in nasilja v družbi na različne načine. Ravno zato je za vse uporabnike in neuporabnike interneta potrebna neka oblika nadzora ali pa zunanje kontrole za spremljanje online transakcij in elektronskega sveta, z namenom preprečevanja nepravilnosti.

3.3. ELEKTRONSKI KRIMINAL NA SPLOŠNO

V današnjem času hitrega razvoja zajema informacijska tehnologija vse vrste poklicev po celem svetu. Tehnološki dosežki so omogočili prehod iz papirne v nepapirno poslovanje. Oblikujejo se novi standardi hitrosti, učinkovitosti in natančnosti v komunikacijah, ki so postale glavno orodje za povečevanje inovativnosti, kreativnosti in povečevanja delovne uspešnosti na splošno. Računalniki se razširjeno uporabljajo pri vsakdanjem delu, med drugim pa tudi za shranjevanje pomembnih podatkov politične, socialne, ekonomske ali osebne narave, kar prinaša ogromne prednosti družbi sami v obliki večje ekonomske učinkovitosti, družbene blaginje, izboljšanja socialnih razmer, večjega mednarodnega sodelovanja.

Prav hiter razvoj interneta in računalniške tehnologije je pripeljal do novih oblik kriminala. Elektronski kriminal dejansko ne pozna meja in lahko prizadene

katerokoli državo na zemeljski obli. In ravno zato je potreba po ozaveščenosti in uzakonitvi potrebnih zakonov v vseh državah kot orodje za preprečevanje kriminala, ki se izvaja s pomočjo računalnikov in katerega primere bomo spoznali v nadaljevanju.

Internet, elektronsko poslovanje in komunikacije, ki temeljijo na računalniški tehnologiji, presegajo teritorialne meje in ravno zato ustvarjajo novo področje človeških aktivnosti, ki spodkopavajo izvedljivost, izvršljivost in legitimnost obstoječih zakonov, ki temeljijo glede na geografsko ozemlje posamezne države. Ta nova meja, ki jo sestavljajo različne slike, programska koda, uporabniška imena in gesla ločuje elektronski svet od tistega resničnega, v katerem živimo vsak dan. To novo nastajajoče okolje, ki se iz dneva v dan širi in vse bolj pridobiva na veljavi, predstavlja veliko nevarnost za tiste, ki skrbijo, da se zakoni, ki temeljijo na geografskem ozemlju, oblikujejo, nastajajo, razvijajo, dopolnjujejo in seveda tudi izvršujejo.

Nove oblike elektronskega kriminala se pojavljajo iz dneva v dan (finančne prevare, neobstoječe online trgovine, različne vrste življenjskih zavarovanj in varčevanj). Različne vrste internetnih prevar tako vsakodnevno pridobivajo nove člane, tipi internetnega kriminala pa mutante. Ker sodobna tehnologija ne pozna meja, tudi ni ovir za njene uporabnike, sploh tiste s slabimi nameni ne.

3.3.1. POJAVNE OBLIKE ELEKTRONSKEGA KRIMINALA

Pojavnosti elektronskega kriminala lahko razvrstimo v naslednje skupine (Lunker, 2001, str. 2):

1. Zoper posameznika;

a) Zoper osebo:
- nadlegovanje po elektronski pošti,
- elektronsko nadlegovanje, vznemirjanje in izsiljevanje,
- širjenje nespodobnega materiala, gradiva po internetu,
- klevetanje, obrekovanje,
- hacking / cracking[14],

[14] Hacking in cracking sta širok pojem, s katerim v ožjem pomenu besede razumemo predvsem vdiranje v računalniške sisteme in spreminjanje programske kode. Pod širšim pomenom besede pa lahko razumemo uporabo računalniških sistemov in programske opreme v neuporabniške namene.

- nespodobno razkazovanje.

b) Zoper imetje posameznika:
- prenašanje računalniškega virusa,
- računalniški vandalizem,
- nadlegovanje po internetu,
- nepooblaščen nadzor nad računalniškim sistemom,
- hacking / cracking,
- lažno predstavljanje in kraja identitete.

2. Zoper organizacije;

a) zoper vlado, državne službe, privatna podjetja in družbe, skupine posameznikov:
- hacking / cracking,
- posedovanje nedovoljenih informacij,
- elektronski terorizem,
- distribucija piratske programske opreme.

3. Zoper družbo na splošno;

- pornografija (posebej otroška pornografija),
- neetično in nemoralno delovanje, kvarjenje, blatenje, onečiščevanje družbe in njenih članov,
- zvijačenje, spletkarjenje, intrigantstvo.

3.3.2. VRSTE ELEKTRONSKEGA KRIMINALA

Različne vrste elektronskega kriminala razvrščamo glede na vlogo, ki jo ima pri samem dejanju računalnik. Tako razlikujemo tri vrste elektronskega kriminala, in sicer (Sherman, 2000, str. 5) :

Računalnik kot predmet, žrtev ali tarča[15]

Kazniva dejanja v tej kategoriji vključujejo napade na zasebnost, celovitost in dostopnost računalniških informacij in storitev, npr. napad na računalniški sistem za pridobitev informacij, krajo storitev, uničevanje podatkov ali onemogočanjem dostopa do računalnika ali strežnika.

[15] Računalnik napada samega sebe.

Računalnik kot fizični dejavnik ali kot nosilec zapisa
Nedovoljena dejanja takšne vrste vključujejo uporabo računalnika ali povezane naprave za shranjevanje podatkov pomembnih za izvajanje kaznivih dejanj npr. prenašanje računalniškega programa, ki vsebuje navodila za samodejno izvedbo škodljivega dejanja.

Računalnik kot pripomoček ali orodje
S to vrsto kaznivih dejanj gre razumeti klasična nezakonita dejanja, ki so s pomočjo računalnikov, omrežja ali povezanih naprav izvedena hitreje in lažje.

Pri naštevanju praktičnih primerov kaznivih dejanj s področja elektronskega kriminala in pri njihovem kratkem opisu, bi lahko v celotnem diplomskem delu pisali samo o njih. Ker smo prostorsko omejeni si bomo pogledali samo nekaj glavnih vrst, ne pa tudi posameznih kaznivih dejanj, ki so sestavni del različnih vrst kaznivih dejanj (Sherman, 2000, str. 7):

Otroška pornografija
Širjenje otroške pornografije na različne načine, ki jih omogoča internet (elektronska pošta, internet pogovori, IRC, različni forumi…).

Prevare
Sem sodijo prevare s kreditnimi karticami in v zadnjem času zelo razširjene internetne prevare, ki jih bolj podrobno predstavljam v nadaljevanju diplomskega dela. Obtoženi uporabljajo različno programsko opremo za krajo ali generiranje uporabniških računov. Tako programsko opremo se lahko brezplačno poišče na internetu.

Manipulacije z omrežjem
V tem primeru gre praviloma za kazniva dejanja, storjena s strani nezadovoljnih ali pa bivših zaposlenih, ki dostopajo v računalniški sistem z namenom kraje denarja ali pa kraje vrednih informacij.

Hacking / Cracking
Vsebuje vlome v računalniški sistem. Zelo pogosto se potrebne informacije o dostopu in gesla zagotovijo s pomočjo prevare (predvsem družbene tehnike, katere bomo spoznali v poglavju o pristopih hackerjev) z namenom kraje ali uničevanja podatkov in onemogočanja komunikacije. Zelo podoben prestopek je kloniranje mobilnega telefona, pri katerem se telefonski račun žrtve ukrade in prenastavi v drug mobilni telefon.

Kraja identitete

Računalniki so pogosto sestavni del tega kaznivega dejanja. Obsega pridobivanje podatkov o identiteti posameznika z namenom kaznivega dejanja protipravne koristi. V ZDA je bilo v letu 2001 približno 100.000 oseb žrtev kraje identitete (Identity Theft Victim Complaint Data, 2002, str. 3).

V Prilogi 3 so slikovno predstavljeni podatki o številu kraj identitet na 100.000 prebivalcev za vse zvezne države ZDA v letu 2001.

Ostale vrste elektronskega kriminala so še piratstvo programske opreme, elektronsko nadlegovanje, izsiljevanje, zavajanje… Navedimo samo še primer elektronskega pretvarjanja. Pred kratkim je bil v Kaliforniji, ZDA, proces proti moškemu, ki je bil obsojen kaznivega dejanja lažnega predstavljanja z namenom spodbujanja k posilstvu. Petdesetletnik se je namreč na različnih internet pogovorih predstavljal kot osemindvajsetletna ženska, ki ga je pred kratkim zavrnila. V pogovoru z drugimi je izdajal njeno telefonsko številko in naslov skupaj s sporočili, da ima željo po posilstvu. Nesrečnici se je pogosto dogajalo, da so na njena vrata trkali moški, ki so njen naslov in ostale podatke dobili od obsojenega.

Posebno poglavje so tudi internetne prevare, ki z vidika uvrstitve spadajo v naštete vrste elektronskega kriminala. Ker pa so internetne prevare vedno bolj popularne, si poglejmo nekaj vrst in področij, ki jih pokrivajo:

- internetne dražbe,
- poneverba ali kraja kreditnih kartic,
- verižna pisma in elektronska sporočila,
- dobrodelni nameni,
- lažna spričevala o zaključenih šolanjih,
- lažne registracije domenskih imen,
- zaposlitvene možnosti,
- finančne prevare,
- prevare proti posameznim podjetjem,
- darilni klubi,
- vladne subvencije in podpore,
- kraja identitete,
- investicije,
- igre na srečo,
- večstopenjsko trženje,
- piramidne sheme,

- telefonske prevare,
- prevara »nigerijske« vlade,
- športne stave,
- štipendije,
- davčne prevare,
- potovalne agencije,
- delo na domu,
- WWW storitve,
- premoženjski skladi (Cyber Criminals Most Wanted, 2003).

3.3.3. ELEKTRONSKI KRIMINALCI

Posamezniki in združbe posameznikov, ki se organizirajo z namenom, da svoje znanje, programsko in strojno opremo ter ostala sredstva, ki jih imajo v svoji lasti, združijo z namenom večje učinkovitosti in doseganja boljših rezultatov na področju elektronskega kriminala, imenujemo elektronski kriminalci. Imen za njihov protipraven poklic je več, v praksi se še najbolj uporablja hacker[16]. Rezultati raziskav za kriminalce takšnega tipa v ZDA so pokazali, da gre v večini primerov za državljane ZDA, moškega spola, belopolte, z višjo ali univerzitetno izobrazbo in praviloma brez kazenske kartoteke (Sherman, 2000, str. 6).

3.3.3.1. Tipi hackerjev

Obstaja več različnih tipov hackerjev, ki jih v grobem lahko razvrstimo v štiri skupine (Brinkema, 2000, str. 8):

1. »Naključni« hacker

Gre za osebo, ki povsem naključno najde programskega hrošča[17]. Ponavadi gre za uporabnika sistema ali aplikacije, ki pri svojem delu pogosto uporablja nek del sistema ali aplikacijo. Npr. pri pogostem delu z aplikacijo uporabnik namesto pravilne funkcije uporabi napačno in program mu namesto potrebnih

[16] Prevod besede hacker je zelo zahteven, saj se pod tem pojmom v državah, od koder izvira ta termin, razume v bolj širokem pomenu besede, kot pa razlage, ki krožijo v slovenskem jeziku. Pogosto srečujemo različne prevode, ki pa besedi odvzamejo pravi pomen. Veliki slovar tujk Cankarjeve založbe iz leta 2002 besedo heker (hacker) prevaja kot a) tehnično dobro podkovan računalniški navdušenec in b) kdor vdira v računalniške sisteme.
[17] Programska napaka.

izpiše še veliko drugih podatkov, ki so zaupne narave.

2. Namišljeni hacker

Slabo računalniško znanje, drznost in nepremišljenost so dejavniki, ki povzročajo, da gre za najmanj cenjeno in najbolj popularno skupino hackerjev. Člani te skupine se praviloma zanašajo na že znane programske kode in skripte, pomagajo si z malo spremenjeni računalniškimi orodji, ki si jih najpogosteje priskrbijo kar iz interneta, kjer ne zmanjka takšnih in drugačnih pripomočkov. Praviloma gre za posameznike, ki jih premami nepooblaščen dostop in prevzem podatkov ali sistema. Brez zadržkov uporabljajo nepreverjeno programsko opremo, s katero spravljajo v nevarnost svoje tarče (omrežja ali posamezniki).

Ravno zaradi tega razloga imajo najmanj ugleda in so zato najbolj nadležni in nevarni. Lahko povzročijo precejšnje težave omrežju, čeprav točno ne vedo, kaj skripta[18], ki so jo uporabili, sploh počne in kakšne so lahko posledice. Ta kombinacija neodgovornega eksperimentiranja in nepopolnega znanja pogosto povzroči veliko škodo, kot npr. brisanje in izguba podatkov, sistemske težave.

3. Hacker strokovnjak

So precej bolj pogosti kot poklicni hackerji. Imajo izkušnje z različnimi operacijskimi sistemi, poznajo delovanje TCP/IP protokola in znajo izkoriščati napake v programih. Človek s takšnim znanjem je primeren za varnostno ekipo v večji organizaciji, saj veliko prispeva k večji uspešnosti na področju varnosti omrežja in računalniškega sistema.

4. Poklicni hacker

So zelo redki med hackerji. Gre za razvijalce programskih rešitev, ki so zmožni ugotoviti redke napake v obstoječi programski opremi ter napisati njene popravke. Nočejo popularnosti in se redko izpostavljajo javnosti. Vlagajo precej časa in energije v svoje tehnično in strokovno znanje. Mnogi med njimi nimajo slabih namenov, pogosto aktivno sodelujejo v razvijanju tehnologij za izboljšanje varnosti omrežij.

[18] Programska koda, ki predstavlja del računalniškega programa.

3.3.3.2. Motivi hackerjev

Veliko pregovorov po svetu je na temo, da ima vsaka oseba za določeno ravnanje svoje motive in vzgibe. Na kratko si poglejmo skupine motivov, ki vodijo hackerje po svetu.

1. Ugled, veljava (kot pri vsakem poklicu je tudi tu prisoten prestiž, ugled in sloves najboljšega, ki je zelo cenjen).

2. Zbirka (ni pomemben samo en uspešno izveden napad, šteje čim večja zbirka, kolekcija »žrtev« v zbirki hackerja).

3. Odskočna deska (v primeru uspešno izvedenega načrta hacker pridobi na ugledu in cenjenosti, kar je ključnega pomena za njegovo nadaljnjo življenjsko pot in uspešnost na tem področju).

4. Informacije, podatki (informacije so v današnjem času informacijske družbe vedno bolj vredne, dragocene in iskane, ljudje so zanje pripravljeni odšteti velike vsote).

5. Maščevanje (dejavnik, ki pogosto usmerja bivše zaposlene, ali pa tudi zaposlene, ki niso zadovoljni s svojo plačo, delovnimi razmerami, svojimi predpostavljenimi).

3.3.3.3. Pristopi hackerjev

Načini, na katere hackerji uresničujejo svoje načrte:

- neposredni napad (uporaba skripte),
- posredni napad (z uporabo modema, za lažje zakrivanje sledi),
- družbene tehnike (navezovanje stikov, poznanstev z namenom pridobitve potrebnih podatkov in informacij),
- kazniva dejanja (vlom, kraja, uporaba fizične sile, podkupovanje, napeljevanje, izsiljevanje zaposlenih z namenom uresničitve željenih ciljev).

Če si nekdo res želi dostopa do računalnika ali omrežja, mu bo to zelo verjetno uspelo. Dejstvo je, da med 50 in 85 % resnih kaznivih dejanj izvedejo insiderji[19] (zaposleni, pogodbeno zaposleni, sodelavci, bivši zaposleni) (Jacques, 2003).

Rezultati različnih raziskav kažejo, da naj bi bilo do leta 2005 60 % vseh stroškov, ki nastanejo zaradi računalniškega kriminala, povzročenih s strani insiderjev kot posameznikov ali kot sodelavcev v različnih združbah. Njihov glavni motiv bo (je) finančne ali politične narave[20](Jacques, 2003).

Težava je v tem, ker sodobne poslovne tehnike in sodelovanje med zaposlenimi zahtevajo precejšnjo povezavo informacij in podatkov med zaposlenimi. Prav to utegne pripeljati do nepooblaščene uporabe računalnikov in omrežja.

3.4. ELEKTRONSKI KRIMINAL IN PRAVNA UREDITEV NJEGOVEGA PREPREČEVANJA PO SVETU

V zadnjem času vedno večjo pozornost v glavnih mestih držav zahteva naraščajoča nevarnost pred kriminalom, ki se zagreši proti računalniškim sistemom ali pa informacijam, ki so shranjene na računalnikih. Vendar pa v večini držav po svetu obstoječi zakoni slabo varujejo uporabnike (posameznike, podjetja, institucije) ali pa sploh ne varujejo pred kriminalom takega tipa. Takšno pomanjkanje pravne zaščite pomeni, da se morajo podjetja in državne institucije zanašati samo na tehnično zaščito, da se lahko zavarujejo pred tistimi, ki bi ukradli, onemogočili dostop ali uničili dragocene informacije.

Samozaščita, čeprav nujna, pa ni zadostna, da lahko elektronski svet postane varen prostor za sklepanje poslov in razvijanje kakršnegakoli elektronskega poslovanja. V vsakem primeru se morajo uveljaviti in določiti zakonski okvirji, ki bodo čimbolj natančno določali vsa pravila elektronskega sveta in dogajanje v njem. Države, kjer je pravna zaščita neprimerna, bodo postajale vedno bolj nekonkurenčne v razmerah nove ekonomije.

Elektronski kriminal se širi čez državne meje, v države z neurejeno zakonodajo, ki veljajo za zatočišče tistih oseb s protipravnimi nameni. V takšnih primerih pa se takšne države izpostavljajo tveganju, da ostala omrežja zavračajo

[19] Za boljše razumevanje se pojem nanaša na osebe, ki so člani neke organizacije oz. določene razmere dobro poznajo od znotraj.

[20] Motivi kot so ugled, maščevanje, ideologija, prepričanje, ki prevladujejo v današnjih dneh izgubljajo na veljavi, finančno ozadje tudi tu prevzema glavno vlogo.

kakršnokoli obliko elektronskega komuniciranja z omrežjem, ki je locirano v tej državi. Države bi morale same preveriti in ugotoviti, če so dovolj močne za boj proti kriminalu, ki ga predstavljam v svojem diplomskem delu. Kjer se pojavljajo zakonodajne luknje, bi bilo najbolje, da se pristojni organi zgledujejo po ostalih državah, ki imajo takšne primere že zakonsko rešene. Potrebna je tudi tesna povezava z industrijo in tistimi, ki imajo resnično opravka s kriminalom takšne vrste, zato da se lahko uveljavijo zakonske zaščite proti takšnim kaznivim dejanjem.

V nadaljevanju obravnave elektronskega kriminala in njegove pravne ureditve si bomo pogledali razmere, ki veljajo v zakonodaji za dvainpetdeset držav po svetu. Samo deset od obravnavanih dvainpetdesetih držav je popravilo in izboljšalo svoje zakone do takšne mere, da lahko obravnavajo vsaj polovico pojavnih oblik elektronskega kriminala (Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002).

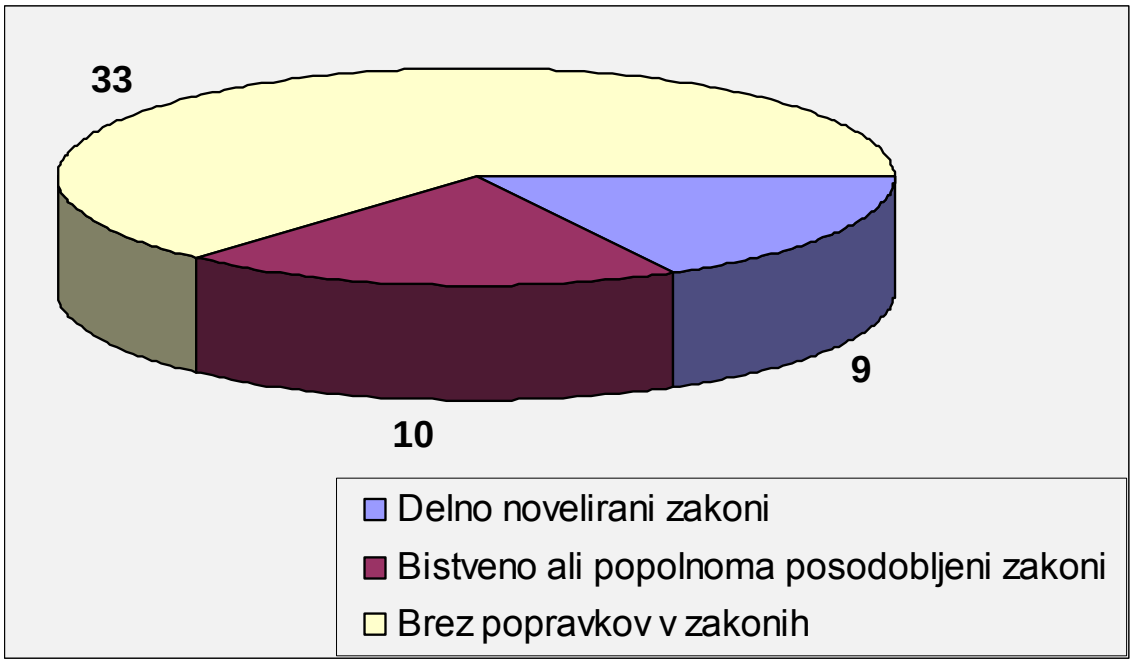
Ostale države pa so šele začele s pobudami za spremembo obstoječe zakonodaje, kar pomeni, da utegne miniti še dokaj dolgo obdobje in bo potrebno vložiti še veliko truda, preden bodo lahko podjetja in posamezniki imeli neko zaupanje v samo elektronsko poslovanje in komuniciranje in bodo tako nastale razmere, v katerih bodo elektronski kriminalci dvakrat premislili, preden bodo napadli računalniške sisteme in informacije.

Zaradi majhne možnosti preganjanja in aretacije elektronski kriminalci čakajo na svojo priložnost nekje v svetovnem omrežju, v eni izmed njegovih oblik. So povsod prisotna nevarnost za vse tiste, ki uporabljajo internet ali le lokalna omrežja bodisi samo za komuniciranje ali pa tudi za elektronsko poslovanje. V nevarnost spravljajo podjetja, posameznike in družbo. V medijih in javnih občilih (dnevno časopisje, tv poročila, internetne strani) predvsem v tujini, se vedno pogosteje pojavljajo, prestopki, ki naj bi jih zagrešili, so vedno hujši in povzročajo vedno višjo materialno škodo.

V nadaljevanju diplomskega dela bomo ugotovili, da zakoni mnogih držav ne urejajo elektronskega kriminala povsem jasno in tudi ne dovolj celovito. Obstoječi zakoni za prestopke različnih oblik (vlom, prepovedan dostop, kraja) pogosto ne obsegajo svojih »virtualnih« dvojnikov.

3.5. STANJE NA PODROČJU ELEKTRONSKIH ZAKONOV PO SVETU

Slika 4: Stopnja razvoja pri posodabljanju zakonov z vidika elektronskega kriminala med dvainpetdesetimi obravnavanimi državami



Vir: Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002.

Na Sliki 4 prikazujem stopnjo razvoja pri posodabljanju zakonov z vidika elektronskega kriminala med dvainpetdesetimi obravnavanimi državami, pri čemer velja da so v navedene skupine uvrščene naslednje države:

1. Skupina (devet držav):
delno novelirani zakoni (Brazilija, Češka, Čile, Danska, Kitajska, Malezija, Poljska, Španija, Velika Britanija).

2. Skupina (deset držav):
bistveno ali popolnoma posodobljeni zakoni (Avstralija, Estonija, Filipini, Indija, Japonska, Kanada, Mauricius, Peru, Turčija, Združene države Amerike).

3. Skupina (triintrideset držav):
brez popravkov zakonodaje za področje elektronskega kriminala (Albanija, Bolgarija, Burundi, Dominikanska republika, Egipt, Etiopija, Fidji, Francija, Gambija, Iran, Islandija, Italija, Jordanija, Južna Afrika, Kazahstan,

Kuba, Latvija, Lesoto, Libanon, Madžarska, Malta, Maroko, Moldavija, Nigerija, Nikaragva, Norveška, Nova Zelandija, Romunija, Srbija in Črna Gora, Sudan, Vietnam, Zambija, Zimbabve).

V Tabeli 4 prikazujem podatke za devetnajst držav (uvrščene v skupini delno novelirani in bistveno ali popolnoma posodobljeni zakoni), katera področja kriminala so bila zakonsko delno, bistveno ali popolnoma spremenjena. Čeprav so bili v neki državi zakoni za določene prestopke morda samo delno popravljeni, v drugi pa popolnoma, sem jih v Tabeli 4 označil enako, saj je po mojem mnenju na tem mestu obravnave pomembno dejstvo, da se neka vrsta kriminala sploh kvalificira za kaznivo dejanje in zato zakonsko preganja. Vsekakor pa moram po drugi strani poudariti, da gre vseeno za veliko razliko, če so bili v eni državi zakoni le delno, v drugi pa popolnoma spremenjeni, saj je na tak način neko področje zakonsko povsem pokrito, dorečena so vsa tehnična vprašanja, pravni postopki in kazni so jasne, prav tako tudi pristojni organi za izvajanje zakonov. Za države z delno popravljenimi zakoni pa naštetega še ne moremo trditi, pojavljajo se pravne vrzeli in nedokončana področja (Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002).

Tako se npr. med naštetimi državami enaka vrsta kriminala ne obravnava enotno. V nekaterih državah se tako nepooblaščen dostop smatra za prestopek samo, če so bili prisotni elementi škodovanja. Spet drugje je kraja podatkov prekršek samo, če so podatki povezani s posameznikovo vero ali zdravjem ali pa so prisotni elementi želje po prevari in škodovanju.

Do protislovij prihaja celo znotraj držav. Septembra 2000 je Avstralska demokratska stranka kritizirala vlado Južne Avstralije, ker je ustvarila zavetišče za elektronske kriminalce s tem, ko ni sprejela zakonov s področja boja proti računalniško povezanemu kriminalu skladno z zakoni, ki so jih sprejele vlade drugih delov Avstralije (South Australian Internet Censorship Bill, 2002).

Tudi zagrožene kazni so zelo različne med državami s posodobljenimi zakoni. Filipini, Mauricius, in Združene države Amerike imajo precej višje kazni kot večina preostalih držav za kazniva dejanja s področja elektronskega kriminala.

Tabela 4: Posodobitve zakonov za različne vrste elektronskega kriminala po posameznih državah

Država	Podatkovni			Omrežni		Dostop		Soroden		
	Prestrezanje podatkov	Spreminjanje podatkov	Kraja podatkov	Vmešavanje, oviranje omrežja	Sabotaža omrežja	Nepooblaščen dostop	Širjenje virusov	Pomoč in podpora	Računalniško povezano ponarejanje	Računalniško povezane prevare
Avstralija	✓	✓	✓	✓		✓			✓	✓
Brazilija		✓			✓	✓		✓		
Kanada	✓	✓	✓	✓	✓	✓	✓			✓
Čile	✓	✓	✓	✓	✓					
Kitajska		✓		✓			✓			
Češka		✓	✓		✓	✓				✓
Danska		✓		✓						✓
Estonija		✓	✓	✓	✓	✓	✓	✓		✓
Indija		✓	✓	✓	✓	✓	✓	✓		✓
Japonska	✓	✓	✓	✓	✓	✓		✓	✓	✓
Malezija		✓				✓		✓		✓
Mauricius	✓	✓		✓	✓	✓	✓	✓	✓	
Peru	✓	✓	✓	✓	✓	✓				✓
Filipini	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Poljska		✓	✓	✓				✓		
Španija	✓	✓	✓					✓		✓
Turčija		✓	✓	✓	✓		✓	✓	✓	✓
Velika		✓		✓	✓	✓		✓		
ZDA	✓	✓	✓	✓	✓	✓	✓	✓		✓

Vir: Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002.

Za lažje razumevanje posameznih vrst oz. tipov elektronskega kriminala iz Tabele 4 si poglejmo Tabelo 5, ki bolj natančno opisuje posamezne vrste prestopkov.

Tabela 5: Pojasnilo vrst oz. tipov elektronskega kriminala

Vrsta elektronskega kriminala	Pojasnilo
Prestrezanje podatkov	Prestrezanje, prekinitev, preprečitev prenosa podatkov
Spreminjanje podatkov	Sprememba, predelava, spreminjanje, uničevanje ali brisanje podatkov
Kraja podatkov	Odvzem ali kopiranje podatkov, ne glede na to, ali so podatki zaščiteni z zakoni (založniška, avtorska pravica…)
Vmešavanje, oviranje omrežja	Oviranje ali onemogočanje dostopa za uporabnike
Sabotaža omrežja	Spreminjanje ali uničevanje omrežja ali sistema
Nepooblaščen dostop	Hacking ali cracking za dostop do sistema ali podatkov
Širjenje virusov	Vpeljava programske opreme, ki škoduje sistemu ali podatkom
Pomoč in podpora	Omogočanje izvajanja elektronskega kriminala
Računalniško povezano ponarejanje	Spreminjanje podatkov z namenom, da se le ti predstavijo kot avtentični
Računalniško povezane prevare	Spreminjanje podatkov z namenom, da se ustvari ekonomska korist zaradi napačnega prikaza

Vir: Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002.

Od triintridesetih držav, ki niso sprejele še nobenih popravkov pri zakonih z vidika elektronskega kriminala, pa je pri trinajstih državah viden napredek na področju zakonodaje in ustanavljanju pristojnih organov za boj proti elektronskemu kriminalu. Sedem od teh trinajst držav je v Afriki ali pa na Srednjem vzhodu in čeprav se te države še niso srečale z elektronskim kriminalom v pravem pomenu besede in v takšnih oblikah kot se kaže v drugih, s tega vidika bolj razvitih državah, pa rezultati kažejo, da se zavedajo, da so ukrepi več kot potrebni. Napredek v teh državah prikazujem v Tabeli 6.

Tabela 6: Napredek v trinajstih državah brez popravkov v zakonih z vidika elektronskega kriminala

Albanija
Odgovorni za regulacijo telekomunikacij pripravljajo snov s področja elektronskega kriminala, s ciljem ustvariti protokole o sodelovanju in izmenjavi podatkov.
Gambija
Pripravlja načrt nacionalnega informacijsko-tehnološkega programa, povezuje se tudi z mednarodnimi organizacijami z namenom izdelave potrebnih zakonov.
Iran
V zadnjih letih aktivno deluje na področju izbiranja primernega vidika elektronskih zakonov, vendar pa še ni vpeljal nobenih zakonov ali predpisov v zvezi z računalniškim kriminalom. Področja, ki jih proučujejo, so: računalniški kriminal, intelektualna lastnina, zasebnost podatkov in svoboda informacij.
Kuba
Delovna skupina Ministrstva za pravosodje pripravlja spremembe v kazenskem zakoniku.
Latvija
Amandmaji v kazenskem zakoniku so načrtovani. Le ti predlagajo precejšnje kazni za računalniško povezana kriminalna dejanja.
Lesoto
Ustanovljena je bila posebna skupina za preučitev različnih vidikov informacijske varnosti povezane z elektronskih poslovanjem.
Malta
Sprejeti so bili pomembni zakoni in močan pravni okvir s področja elektronskega poslovanja, zaščite podatkov in zlorabe računalnikov. Zakonski osnutki čakajo na pregled v parlamentu.
Maroko
Komisija, ki jo sestavljajo člani različnih ministrstev in jo podpira vlada, ugotavlja različne vidike računalniške varnosti.
Nova Zelandija
Trenutno ni nobenih resnih prestopkov z vidika računalniškega kriminala. Kljub temu pa parlament in sodna oblast razmišljajo o potrebnih spremembah.
Sudan
Privablja tuje odvetnike, strokovnjake iz različnih področij (računalništvo, telekomunikacije) na delovne delavnice, kjer izmenjujejo informacije in ugotavljajo pravi pristop k elektronskemu kriminalu.
Vietnam
Zbira informacije, da se bodo lahko ustvarili primerni predlogi za popravke in dopolnila obstoječih zakonov.
Zambija
Ustanovili so svet telekomunikacijske in informacijske tehnologije.

Vir: Cyber Crime and Punishment? Arhaic Laws Threaten Global Information, 2002.

Širitev uporabe zakonov v elektronskem svetu je ključnega pomena za ustvarjanje okolja, ki bo temeljilo na zaupanju ljudi in podjetij. Podjetja se morajo v današnjem času najprej in najbolj zanašati na lastno obrambo v primeru napada na sistem in informacije, šele nato se lahko zanašajo na obrambo s pomočjo pravnih mehanizmov. Za zagotovitev samozaščite morajo podjetja usmeriti svojo pozornost na načrtovanje, izvedbo in vgradnjo varnostnih projektov, ki vključujejo tako zaposlene, delovni proces in pa seveda tehnologijo.

Podjetja in organizacije morajo zagotoviti zadostna sredstva za izobraževanje zaposlenih s področja varnosti, pravočasno razvijati celovite načrte za upravljanje s pomembnimi podatki, zapisi in transakcijami, v celoten sistem je potrebno integrirati močno varnostno tehnologijo s požarnimi zidovi, protivirusnimi programi, orodji za ugotavljanje vdorov ter sredstvi za ugotavljanje verodostojnosti uporabnikov.

Našteta varnostno-sistemska orodja (strojna in programska oprema za zaščito informacijskega sistema) so zelo draga in zahtevna za uporabo. Nadalje ni nobenih dogovorjenih standardov za ugotavljanje kakovosti teh orodij in prav tako ni sprejeta nobena metodologija za podjetja, da bi le ta lahko ugotovila, kolikšni so potrebni izdatki za zagotovitev varnosti celotnega računalniškega sistema in informacij.

Nezmožnost oceniti stroške in koristi investicij v informacijsko varnost postavlja vodje oddelkov za varnost[21] v podrejen položaj, ko se potegujejo pri predsednikih uprav za finančna sredstva skupaj z ostalimi organizacijskimi enotami in oddelki. Na področju upravljanja in tehničnih rešitev za informacijsko zaščito je zaradi naštetih dejstev potrebno narediti še marsikaj. Potrebno bi bilo uveljaviti standarde, ustanoviti združenja razvijalcev in uporabnikov strojne in programske varnostne opreme, sodelovanje v podjetju med informacijsko in ostalimi enotami bi moralo biti boljše itd.

Sistemski operaterji rutinsko ne nastavljajo vseh privzetih ali pa dodatno izdelanih varnostnih možnosti in tako po nepotrebnem povečujejo ranljivost sistema in informacij. Programske napake in varnostne luknje, za katere so razvijalci programskih rešitev že izdelali popravke, se pogosto ne posodabljajo.

[21] Namesto vodja oddelka za varnost bi lahko uporabili tudi naziv vodja za informatiko, informacijski sistem, računalništvo, omrežje ipd. Oddelek za varnost računalniškega sistema je praviloma del informacijskega oddelka podjetja.

Kot enega zadnjih primerov lahko navedem posodobitev operacijskega sistema Windows 2000, Windows XP, Windows NT in Windows 2003 Server z dne 16. julija 2003[22]. Uporabnik ali pa skrbnik sistema, ki na svojem računalniku nima te posodobitve, izpostavlja računalnik možnemu »napadalcu«, ki lahko z uporabo pravih orodij prevzame nadzor nad računalnikom, ter ima tako pregled nad vsemi datotekami in podatki, dostop do baz podatkov na omrežnih pogonih, lahko upravlja različne sistemske vire, spreminja sistemske nastavitve, onemogoča delo ostalim uporabnikom napadenega računalnika ali pa tudi računalniškega sistema. Škoda, ki nastane v takem primeru, je lahko precejšna. Brez prevelikega ugotavljanja in kompleksnih izračunov pa lahko zatrdim, da je kazen za premajhno zagotavljanje denarja za navedena varnostna orodja ne samo bistveno višja od morebiti prihranjenih sredstev, temveč je lahko celo usodna za nadaljnje nemoteno poslovanje podjetja, saj lahko nastala škoda resno ogrozi finančno stanje podjetja.

Da pa razmere le niso tako neurejene, lahko navedemo tudi nekaj naslednjih dejstev. Podjetja iz različnih držav sveta in različnih gospodarskih panog ustanavljajo centre za delitev in analizo informacij. S tem v realnem času sodelujejo pri informacijah v zvezi z grožnjami, ranljivostjo, napadi in protiukrepi, vse seveda nanašajoč se na elektronski kriminal. World Information Technology and Services Alliance je ustanovil Global Information Security Summit, v katerem so svoje sile združili industrija, vlade in vsestranske organizacije z različnih ekonomskih področij z namenom izmenjave informacij in ustanavljanjem partnerstev. Posebne delovne skupine razvijajo pristope k najbolj pomembnim informacijsko-varnostnim problemom (World Information Technology and Services Alliance, 2000).

Glede na vse, kar je bilo povedano o pravni ureditvi, bi lahko na temelju zapisanih dejstev ugotovili naslednje:

1. Zanašanje na trenutno veljavne zakone je napačen pristop.

Kljub napredku, ki smo mu priča v veliko državah, se še vedno veliko držav zanaša na obstoječe tradicionalne zakone, ki veljajo za pregon elektronskih kriminalcev. Večina držav se zanaša na zastarele zakone, ki šele predvidevajo rojstvo elektronskega sveta in dejansko še niso obravnavali praktičnih primerov na sodišču.

[22] Gre za posodobitev varnostne napake v naštetih operacijskih sistemih, ki nosi ime Microsoft Security Bulletin MS03-026. Sistemske napake takšnega tipa omogočajo tudi širitev računalniškega virusa.

2. Nizke kazni so slab zgled.
V večini novel in amandmajev zakonov so določene nizke kazni za zločine, ki imajo lahko razsežne ekonomske in socialne posledice.

3. Slabo sodelovanje med državami.
Raven soglasja med državami o tem, kateri kriminal bi bilo potrebno preganjati, je zelo nizka. V Tabeli 4 je to jasno prikazano za devetnajst držav, ki so že spreminjala svoje zakone za zmanjšanje elektronskega kriminala. Če se kriminal ne bo obravnaval na podoben način po vsem svetu, bodo skupni napori organov pregona za boj proti kriminalu razmeroma zahtevni in zapleteni.

4. Vzorčen zakon o elektronskem kriminalu je potreben.
Večina držav, še posebej tiste v razvoju, iščejo vzorec, model pravne ureditve, ki bi mu lahko sledile. Te države se zavedajo pomembnosti zlonamernih dejanj dovolj zgodaj, saj želijo zagotoviti varno okolje za razvoj elektronskega poslovanja. Vendar jih ima le malo med njimi potrebna pravna in tehnična sredstva za prilagoditev obstoječih zakonov elektronskemu svetu. Usklajena javno-zasebna združenja bi lahko kot rezultat svojega delovanje omogočila razvoj vzorčnih zakonov in tako izločila možne nevarnosti pred nepazljivimi zakoni, kar bi lahko ustvarilo zatočišče za elektronske kriminalce.

3.6. RAZMERE V SLOVENIJI

Tako kot smo do sedaj že spoznali v prejšnjih poglavjih diplomskega dela, države po svetu aktivno delujejo in poskušajo čimbolj izboljšati obstoječo zakonodajo. Enako lahko ugotovimo tudi za Slovenijo, ki pa po mojem mnenju v zadnjem času vseeno le ni tako napredna z vidika uvajanja zakonskih sprememb za elektronski kriminal. Tako moram seveda najprej omeniti leto 2000, ko je bil sprejet Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/00), v nadaljevanju ZEPEP.

Vsebino ZEPEP so v veliki meri prispevali vzorčni zakoni UNCITRALA in Direktiva št. 1999/93/EC Evropskega parlamenta in Sveta EU (Pavliha et al., 2002, str. 22).

Iz predpisa na prvi pogled izhaja mednarodna svežina, saj temelji na nediskriminaciji elektronske oblike, odprtosti oziroma tehnološki nevtralnosti, pogodbeni svobodi strank, dvojnemu pristopu, varstvu osebnih podatkov,

varstvu potrošnikov in mednarodnemu priznavanju elektronskih podpisov (Pavliha et al., 2002, str. 10).

Ko se zakon natančno pregleda, se izkaže, da je izrazito tehnično naravnan. Obsega petinpetdeset členov, razvrščenih v pet poglavij:

1. splošne določbe,
2. elektronsko poslovanje,
3. elektronski podpis,
4. kazenske določbe,
5. prehodne ter končne določbe.

Za natančen seznam oddelkov, ki jih posamezno poglavje ZEPEP pokriva, prilagam Prilogo 4.

Omeniti moram seveda še, da sta bila na podlagi ZEPEP izdana še dva podzakonska predpisa: Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00 in 2/01) in Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji (Uradni list RS, št.99/01). V Prilogi 5 sta bolj natančno predstavljena oba podzakonska predpisa, v Prilogi 6 in 7 sta dodana obrazca za Prijavo overitelja in Prijavo spremembe vpisa v registru overiteljev.

Razvoj elektronskega poslovanja in elektronskih podpisov pa delno obsegajo tudi drugi najnovejši slovenski predpisi, med drugim Obligacijski zakonik (Uradni list RS, št. 83/01), ki med drugim upošteva možnost sklepanja pogodb s sodobnimi načini komuniciranja, predvsem z uporabo elektronskega poslovanja in elektronskega podpisa. V drugem odstavku 57. člena Obligacijskega zakona je tako zapisano, da ima enake učinke kot listina ali katerikoli način ali oblika sporočanja, ki ohranja zapis sporočila nespremenjen in poleg tega omogoča preverjanje izvora sporočila z uporabo splošno priznanih sredstev (Ilešič, 2001, str. 47).

Navkljub vsemu pa je dejstvo, da je pravi in edini zakon s tega področja že prej omenjeni ZEPEP, ki je zgodaj pokazal svoje napake, ki so postale s časom še bolj očitne (pomanjkljivosti s tehničnega vidika, nejasnost, neobravnava pomembnih področij). Tudi stroka mu očita precej napak, med drugim pa sem med njihovimi pripombami zasledil tudi tisto, ki je meni kot bralcu zakona zelo kmalu po začetku branja postala očitna. Gre za sam elektronski podpis, ki se

mu pripisuje prevelik pomen, sploh ob upoštevanju dejstva, da je veliko bolj pomembnih področij ostalo povsem nepokritih.

Zakon žal ni popoln, zato lahko kaj kmalu pričakujemo spremembe. Očitno je bil pripravljen na podlagi treh različnih tujih pravnih virov, zato je nedosleden in posledično nejasen, precej okorno napisan, določena poglavja so težko razumljiva in strokovno vprašljiva. Kot smo spoznali v drugem poglavju diplomskega dela, je elektronsko poslovanje proces, ki zajema veliko različnih oblik elektronskega komuniciranja, elektronski podpis pa se zahteva le v nekaterih ozkih delih elektronskega poslovanja. Verjetno bi bilo bolj smiselno, da bi obstoječi zakon nadomestili z dvema predpisoma: Zakonom o elektronskem podpisu in Zakonom o elektronskem poslovanju (Pavliha et al., 2002, str. 11).

Za kazenske določbe ZEPEP pa lahko navedem primer na podlagi analize dveh členov (17. in 49. člena):

17. člen
Uporaba podatkov ali sredstev za elektronsko podpisovanje brez vednosti podpisnika ali imetnika potrdila, ki se nanaša na te podatke ali sredstva, je prepovedana.

49. člen
Z denarno kaznijo od 50.000 tolarjev do 150.000 tolarjev se kaznuje za prekršek posameznik, ki brez vednosti podpisnika ali imetnika potrdila uporabi njegove podatke ali sredstva za elektronsko podpisovanje (17. člen).

V opisanem nedopustnem ravnanju po določbi 17. člena ZEPEP je dejansko stanje takšno, da lahko kršitev iz tega člena zagreši kdorkoli, kazen, ki se mu očita za takšen prekršek pa je relativno nizka, ker je lahko dejansko nastala škoda bistveno višja od zagrožene denarne kazni.

ZEPEP tako po eni strani zelo dobro navede dejstva o elektronskem podpisu ter njegovem tehničnem in pravnem vidiku, predstavi nam, da je elektronski podpis dejansko enakovreden lastnoročnemu (razen v posebej navedenih primerih), po drugi strani pa se njegova uporaba s strani tujega uporabnika sankcionira z nizko denarno kaznijo. Moramo se zavedati, da so transakcije, ki se opravljajo s pomočjo elektronskega podpisa, vedno večjih vrednosti in je tako možna nastala škoda lahko precejšnja. Pri kršitvi 17. člena ZEPEP dejansko velja, da se nekdo izdaja za drugo osebo in uspešno izvede neko vrsto elektronskega

poslovanja, saj se je pravilno identificiral ter tako lahko povzroči finančno precejšnjo škodo. Po drugi strani pa brez pomoči elektronskega poslovanja takega kaznivega dejanja sploh ne bi mogel izvesti, saj ne bi mogel prevzeti fizične oblike podpisnika ali imetnika potrdila za uspešno izpeljavo svojih kaznivih namenov.

3.7. POTREBNI UKREPI

Nizka raven pravnega varstva po svetu proti elektronskemu kriminalu po mojem mnenju nalaga oblikovanje nekaterih ukrepov.

1. Podjetja morajo zaščititi svoje informacije.

Zakoni za uveljavljanje zasebne lastnine delujejo samo, če tudi sami imetniki lastnine sprejemajo prave odločitve in korake za njeno zaščito. S praktičnim primerom to najbolje predstavimo če npr. lastnik hiše ne bi kupil ključavnic, nato pa od državnih organov pričakoval, da zagotovijo varnost in zakonske člene s tem, da zaposlijo dovolj policistov. Tudi kjer zakoni dovolj dobro urejajo pravna področja elektronskega kriminala, se morajo podjetja, ki so odvisna od omrežij, sama potruditi za zaščito informacij in sistemov. V državah, kjer bodo prave zakonske spremembe šele čez nekaj mesecev ali let, kot to velja za večino držav, pa je njihova odgovornost pa lastnem zagotavljanju varnosti še toliko večja.

2. Vlade in pristojni organi morajo zagotoviti, da njihovi zakoni dejansko urejajo področje elektronskega kriminala.

Vlade ostajajo glavni dejavnik za pravno preprečitev v zadevnem okolju. ZDA so že utrpele veliko škodo in zato izboljšale pravno ureditev, potem ko so se soočile z izzivom elektronskega kriminala. Zelo pomembno je, da se tudi ostali narodi kaj naučijo iz te lekcije, pregledajo obstoječo zakonodajo in preverijo, če le ta sploh omogoča sodni pregon elektronskih kriminalcev. V večini primerov je obstoječa zakonodaja zrela za popravke. Sprejetje potrebnih zakonov, ki prav tako vključujejo pravice posameznika, so pomemben korak v boju proti naraščajoči nevarnosti elektronskega kriminala.

3. Pri izdelavi in izboljšanju pravnega okvirja za elektronsko varnost morajo sodelovati podjetja, pristojni organi in civilna družba.

Da se lahko kazensko-pravno preganja elektronski kriminal tudi čez državne meje, mora takšno dejanje veljati za prestopek v vsaki državi sveta. Države bi morale elektronski kriminal obravnavati na podoben način, kljub temu pa še vedno lahko upoštevajo lokalno pravno tradicijo. Pomemben prispevek pri izdelavi vzorčnega predpisa lahko pripišemo Svetu Evrope, ki obsega enainštirideset držav. Svet Evrope oblikuje mednarodno konvencijo o elektronskem kriminalu. V konvenciji so zajeti nepooblaščen dostop, nezakonito prestrezanje in spreminjanje podatkov, vdor in motnje v sistemu, računalniško povezano ponarejanje, računalniško povezane prevare, pomoč in podpora elektronskemu kriminalu. Prav tako pa obsega preiskovalne zadeve v zvezi z sodno oblastjo, izročitvijo, prestrezanjem komunikacij, izdelavo in varstvom podatkov. Predvideva pa tudi sodelovanje med pristojnimi sodnimi organi čez državne meje z različnimi mednarodnimi predpisi.

3.7.1. NEKATERI VIDIKI VARSTVA PRED ELEKTRONSKIM KRIMINALOM

Vprašanje načina, vrste, načrtovanja, vgradnje in izvajanja zaščite je zelo zapleteno. Gotovo zaščito ponuja le možnost, da je računalnik, na katerem je shranjena ključna infrastruktura, ločen od ostalih računalnikov, ki so povezani na omrežje. Ker pa je takšen primer zaradi zapletenosti izvedbe in še mnogih drugih dejavnikov (neažurnosti, izgube časa, neusklajenosti, velike možnosti napake, ovir v strojni in programski opremi) praktično neizvedljiv, je potrebno slediti določenim postopkom za ohranjanje varnosti samega sistema. Te postopke lahko kratko strnimo v nekaj naslednjih točkah:

1. potrebno je vzdrževati jasno in konsistentno varnostno politiko in postopke,
2. ocenjevanje ranljivosti za ugotavljanje slabosti sistema je ključnega pomena,
3. nameščena mora biti strojna in programska oprema za prepoznavanje vdorov (požarni zid, enkripcija, pametne kartice, protivirusna zaščita),
4. vsa gesla je potrebno pogosto menjavati, sploh tista, ki omogočajo dostop do različnih informacij in infrastrukture, gesla naj bodo v alfanumerični obliki,
5. znane težave se morajo hitro odpraviti, vsako čakanje je lahko usodno,
6. vsak napad je neke vrste izkušnja, le tako lahko ugotovimo slabosti in pomanjkljivosti sistema in temu primerno ukrepamo,

7. hitra reakcija je potrebna v primeru različnih incidentov, le tako se lahko storilca najde,
8. v primeru škode s strani napadalcev je potrebno hitro ugotoviti nastalo škodo in kar najhitreje vzpostaviti integriteto celotnega sistema,
9. vsi uporabniki računalnikov se morajo zavedati varnostnih tveganj, ki se jim izpostavljajo,
10. potrebno je zagotoviti, da imajo odgovorni zaposleni dovolj časa in znanja za izvajanje svojih delovnih obveznosti,
11. ključnega pomena je vzdrževanje varnostne kopije vseh pomembnih podatkov, vključno s programsko opremo operacijskega sistema.

3.7.2. RESNIČNI PRIMERI ELEKTRONSKEGA KRIMINALA

Zapisano o elektronskem kriminalu kaže ilustrirati s sporočilnostjo resničnih primerov.

Vladimir Levin, diplomant matematike Univerze v St. Petersburgu se je vpisal v zgodovino kot prvi bančni ropar, ki mu je to uspelo s pomočjo računalnikov in omrežja. Levin je s pomočjo prenosnega računalnika v Londonu uspel vdreti v bazo banke Citibank. Z vdorom v njihovo omrežje se je polastil seznama strank, vključno z njihovimi številkami in gesli. Nato se je v razdobju nekaj tednov osemnajstkrat prijavil na omrežje in prenesel skupno za 3,7 milijona dolarjev na različne račune svoje kriminalne združbe v ZDA, na Finskem, Nizozemskem, Nemčiji in Izraelu. Citibanki je kasneje uspelo povrniti vse razen 400.000 dolarjev. Ko je Citibank uspela ugotoviti pretoke denarja, je takoj vzpostavila stik z oblastmi, ki so uspele Levina aretirati v Londunu, marca 1995. V ZDA je bil obsojen na tri leta zaporne kazni. Ostali člani njegove združbe so priznali krivdo in odslužili različne kazni. Od tega vdora v omrežje naprej Citibank uporablja varnostni sistem z imenom dinamična enkripcijska kartica. Gre za zmogljiv varnostni sistem, ki ga nima nobena druga finančna institucija na svetu. Podatek, ki je skoraj neznan, je Levinova trditev, da je bil eden od odvetnikov, ki mu je bil dodeljen, agent FBI-ja, kar samo kaže na to, da so oblasti poskušale biti čimbolj na tekočem v zvezi z njegovimi metodami dela (Hackers Hall of Fame, 2002).

Zelo zanimiv je tudi primer Kevina Poulsena. Leta 1990 je zasedel vse telefonske linije za klice na radijsko postajo KISS-FM v Los Angelesu in si tako zagotovil, da je bil 102. klicatelj. Nagrada je bil Porsche 944 S2. Med drugim je

z vlomi v računalnike uspel pridobiti informacije o podjetjih, ki jih upravlja FBI (Hackers Hall of Fame, 2002).

Ker je seznam kriminalcev zelo obsežen omenimo samo še Iana Murphya. Pisalo se je leto 1981. Ian in še trije sodelavci so vlomili v računalnike AT&T in spremenili njihove interne ure. Tako so uporabniki dobivali popuste za nočne klice čez dan, medtem ko so drugi, ki so klicali ponoči, misleč da gre za cenejše pogovore, plačevali višjo ceno pogovora. Murphy je bil prva oseba v zgodovini, ki je bil aretiran in obsojen zaradi računalniškega kriminala. 1000 ur prostovoljnega dela in dve leti in pol pogojne kazni se je glasila razsodba. V današnjem času bi v ZDA za takšen prekršek dobil bistveno večjo kazen. Danes Murphy vodi svoje podjetje, ki se ukvarja z vdiranjem v sisteme na legalen način. Podjetja ga namreč najemajo za ugotavljanje varnostnih lukenj v svojih sistemih (Hackers Hall of Fame, 2002).

Takšna storitev je v zadnjem času zelo iskana in tudi dobro plačana, saj je strošek za podjetje bistveno nižji, kot v primeru nelegalnega vdora v računalniški sistem. Podjetja ravnajo ekonomsko učinkovito, če imajo na svoji plačilni listi specializirana podjetja, ki se ukvarjajo z vdori v omrežja in iskanjem napak v računalniških sistemih.

3.7.2.1. Računalniški terorizem

Računalniški terorizem lahko opišemo kot uporabo računalnikov za ustrahovanje in uničevanje prebivalstva. Oboroženi samo s tipkovnico in trdim diskom teroristi lahko prevzamejo nadzor nad svetovnimi borzami, spremenijo varnostne kode Bele hiše, spremenijo lahko celo sestavo in sestavine zdravil (Cyber Terrorism, 2003).

Za računalniške teroriste pa je še bolj privlačno dejstvo, da internet ne pozna meja. Nobenih poledenelih, visokogorskih poti, ki bi jih morali prečkati, nobenih dokumentov, ki bi jih morali predložiti. Tako lahko s pomočjo interneta dostopijo do občutljivih virov informacij in lahko širijo svojo doktrino dlje, kot kdajkoli prej.

Šejk Omar Bakri Muhammad (povezujejo ga s terorističnim napadom 11. 9. 2002 v New Yorku) pravi takole: »Islam upravičuje uporabo vseh tehnologij za obrambo muslimanskega ozemlja. Ne bom presenečen, če se bo jutri zgodil

ekonomski zlom zaradi napada na računalniške sisteme v velikih podjetjih (Cyber Terrorism, 2003).«

3.7.2.2. Internetne prevare – aktualne razmere

Aktualnih zgodb, ki jih lahko zasledimo v različnih medijih obveščanja o elektronskem kriminalu, je vsak dan več. Razmere v nekaterih državah postajajo že prav nevzdržne, pristojni organi so prisiljeni ukrepati. Združene države Amerike so tako ena vodilnih držav na področju urejanja zakonodaje, sodnega pregona, izpopolnjevanja tehnologije.

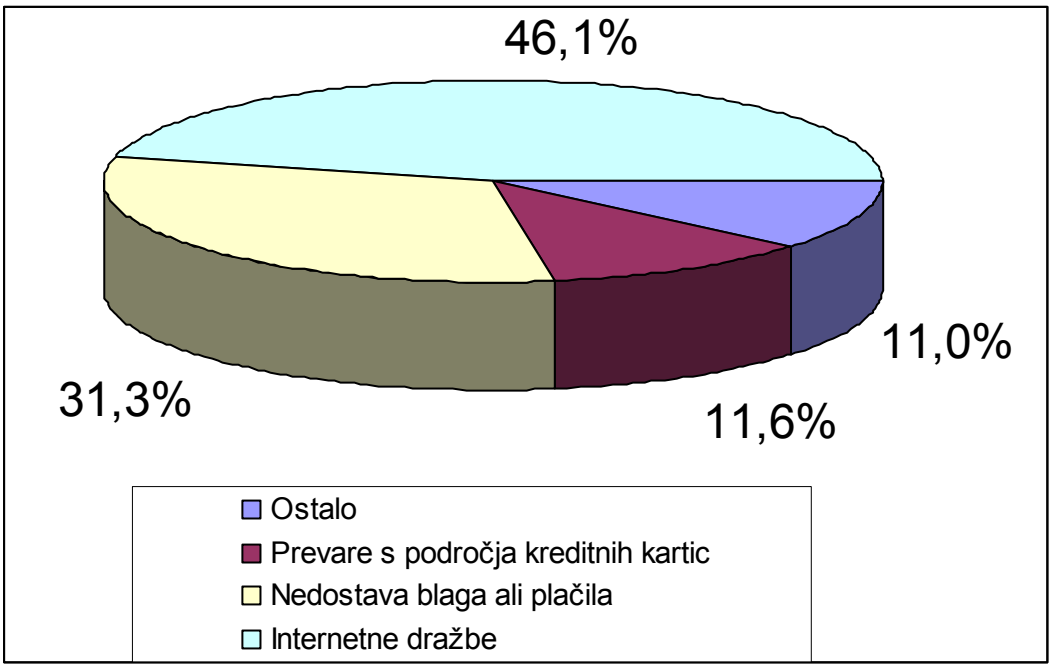
Kot smo v tretjem poglavju diplomskega dela že spoznali, je področje računalniških prevar zelo široko. V tem poglavju si bomo bolj podrobno pogledali aktualne razmere na področju internetnih prevar, katerim je oz. bo izpostavljeno največje število uporabnikov interneta.

Podatki so iz ZDA, ki velja za eno izmed držav z najbolj urejeno zakonodajo, sodnimi oblastmi in vodenjem statistike s področja računalniškega kriminala. Po podatkih IFCC[23] se je število prijav internetnih prevar v letu 2002 po celi državi povečalo za skoraj 300 % na skupno 48.252. V letu 2001 je bilo prevar 16.775. Samo četrtina, ki jih je prevaro prijavila IFCC, je predhodno prijavila prevaro pristojnim službam, kar je tudi trend pri prevarah nasploh (IFCC 2002 Internet Fraud Report, 2003, str. 18).

Na Sliki 5 so prikazani deleži različnih vrst internetnih prevar, pri čemer je razvidno, da je velik delež prevar povezanih predvsem z internetnimi dražbami, nedostavo blaga ali s plačili in a prevarami s kreditnimi karticami. Pod ostalo so uvrščene prevare s področja komunikacij, investicij, čekov, zaupnosti, poslovanja.

[23] Internet Fraud Complaint Center, ki deluje pod okriljem The National White Collar Crime Centra (Zveznega centra za preprečevanje kriminala belih ovratnikov).

Slika 5: Delež posameznik vrst internetnih prevar v ZDA v letu 2002 v %



Vir: IFCC 2002 Internet Fraud Report, 2003.

Za lažje predstavo navedimo primer Chris Chong Kim, ki je na svoji internetni strani najmanj dve leti prodajal računalnike in računalniške dele. Kasneje je svojo dejavnost prenesel na Ebay[24], ki velja za največjo dražbeno stran na svetu. Od kupcev je prejemal plačilo, blaga pa ni nikoli dostavil. 183 kupcev je prijavilo škodo v višini najmanj 407.000 ameriških dolarjev. Proces proti Kimu poteka, če bo spoznan za krivega ga čaka zaporna kazen v višini do štiriindvajset let zapora.

V ZDA se ves elektronski kriminal kaznuje po določbah Federal Sentencinga[25], v katerem je predpisana zaporna kazen za različna kazniva dejanja, ki so ovrednotena po sistemu točk. Prilagam ga v Prilogi 8.

[24] Gre za www.ebay.com, kjer podjetje Ebay preko svoje infrastrukture in internet strani omogoča prodajalcem, da prodajajo svoje stvari po svetu, na drugi strani pa kupci lahko kupujejo. Kljub izdelanemu mehanizmu za zaščito prodajalcev in kupcev prihaja do zlorab.
[25] Vsako kaznivo dejanje ima glede na svoje lastnosti predpisano število točk. V Federal Sentencingu je zapisana zaporna kazen za kazniva dejanja ovrednotena po točkah in se razlikuje tudi na to, če je obsojeni že bil kdaj obsojen.

4. SKLEP

Pogledali smo si nekaj dejstev o internetu in elektronskem poslovanju. Več podrobnosti smo izvedeli o elektronskem kriminalu. Vsaka tema s področja interneta ali elektronskega poslovanja je v današnjem času lahko zelo obsežna, ne glede na to, katerega izmed vidikov pokriva (tehničnega, uporabniškega, skrbniškega, finančnega, trženjskega…). Zato bi bilo tudi nesmotrno v diplomskem delu obravnavati vse vidike, razen če bi obravnavali zelo ozko področje, saj bi zelo težko predstavili pregleden izdelek, ki bi bralcu dobro predstavil določeno področje in mu tudi učinkovito prikazal del pridobljenih podatkov in znanja.

Tako pa po drugi strani obstaja kar precej tem s področja interneta in elektronskega poslovanja, ki so komaj v razvojnih fazah in se dopolnjujejo iz dneva v dan. Uporabniki sami povzročajo ta proces, kateremu ni videti konca. Ena izmed takšnih tem je področje pravne ureditve elektronskega kriminala.

Pravna ureditev je, kot smo videli iz vsebine diplomskega dela, trajen proces, ki sili pristojne organe, da sledijo spremembam na področju uporabe in varnosti računalniških in omrežnih sistemov. Vsak dan se po svetu pojavijo nove ali spremenjene oblike elektronskega kriminala. Na tem mestu moram poudariti, da ljudje pogosto ne razlikujejo med kriminalom na internetu, računalniško povezanim kriminalom in kriminalom, povezanim z nepooblaščeno uporabo in vdori v omrežja.

Velika večina za navedene tri kategorije, ki bi jih lahko oblikovali tudi malo drugače, misli, da gre za eno in isto zadevo. Dejansko gre za različne vrste elektronskega kriminala, ki pa so v zadnjem času vedno bolj prepletene. Brez uporabe ene kategorije ni možna izvedba druge kategorije in v končni fazi celoten načrt nekega računalniškega kriminala lahko propade.

V zadnjem času se namreč ves elektronski kriminal enoti s pojmom kriminala preko interneta, za kar pa upam, da je pozoren bralec v diplomskem delu uspel ugotoviti, da še zdaleč ni res.

Pomembno dejstvo je, da mora biti zakonodaja, ki ureja računalniški kriminal, enotna za vsa njegova področja in združena v smiselno celoto. Kot smo spoznali v diplomskem delu, težave nastopijo tudi v primeru, ko se zakonodaja razlikuje med različnimi državami sveta. V ZDA novelirana zakonodaja ureja

celoten računalniški kriminal, podzakonski predpisi pa njegove posamezne dele (različni tipi elektronskega kriminala, dejavniki izvedbe, namen in način storitve kaznivega dejanja).

Na kriminal s tega področja je zaradi prepletenosti njegovih sestavnih delov potrebno gledati kot na celoto. Nerazumno bi namreč bilo npr. posebej kaznovati vdor v omrežje, nepooblaščen dostop, krajo podatkov, njihovo poneverbo in uporabo. Tako bi v navedem primeru imeli pet prestopkov, ne bi pa upoštevali dejstva, da je bil vdor v omrežje že v samem začetku načrtovan zaradi poneverbe in uporabe podatkov.

Upam, da sem bralcu v diplomskem delu vsaj malce približal pojem elektronskega kriminala in predstavil, kakšne so njegove posledice in potrebni ukrepi. Gre za problem, ki je vedno bolj aktualen in pogost. Kot pri večini stvari pa tudi zanj velja, da se vanj praviloma poglobimo šele takrat, ko se z njim srečamo. Statistika o uporabi interneta in elektronskega poslovanja nam pove veliko o številu uporabnikov interneta in o prometu, ki ga ustvarja elektronsko poslovanje, nič pa iz statistike ni mogoče sklepati o gibanju elektronskega kriminala. Z večanjem števila uporabnikov je vedno več tistih, ki vidijo nelegalne možnosti zaslužka.

Ko bomo žrtve elektronskega kriminala in se bomo po sili razmer bolj poglobili v celotno zadevo, bomo ugotovili, za kako pravno neurejeno področje gre. Gledano z ekonomskega vidika pa bo zaman, ko bomo kot posameznik (fizična oseba) ali kot zaposleni v nekem podjetju, instituciji, ugotavljali nastalo škodo.

5. LITERATURA

1. Braham Bruce: E-Commerce. [URL: http://apollo4.bournemouth.ac.uk/si/ bbraham/bbraham_website_index.html/BARM1-E-Commerce/sld006.htm], 20. 5. 2003.
2. Brinkema John R.: Security Issues. [URL: http://www.law.ufl.edu/icair/ dixon/2-3/tsld001.htm], 21. 2. 2000.
3. Chuach J. C. T.: Law of International Trade. London: Sweet & Maxwell Limited, 2001. Str. 173 - 177.
4. Coppel Jonathan: E-Commerce: Impacts and Policy Challenges. Economics Department Working Papers No. 252. Paris: Organization for Economic Co-operation and Development (OECD), 2000. 26 str.
5. Cyber Crime and Punishment? Arhaic Laws Threaten Global Information. [URL: http://www.mcconnellinternational.com/services/cybercrime.htm], 5. 4. 2002.
6. Cyber Criminals Most Wanted. [URL: http://www.ccmostwanted.com/ scams.htm], 15. 6. 2003.
7. Cyber Terrorism. [URL:http://tlc.discovery.com/convergence/ hackers/articles/cyberterror.html], 15. 5. 2003.
8. Electronic Frontiers Australia: South Australian Internet Censorship Bill 2002. [URL: http://www.efa.org.au/Campaigns/sabill.html], 17. 5. 2003.
9. Federal Trade Comission: Identity Theft Victim Complaint Data. Washington: Federal Trade Comission, 2002. 7 str.
10. Hackers Hall of Fame. [URL: http://tlc.discovery.com/convergence/ hackers/hackers.html], 2. 12. 2002.
11. Ilešič Marko: Obligacijski zakonik z uvodnimi pojasnili Marka Ilešičca in stvarnim kazalom. Ljubljana: Založba uradni list Republike Slovenije, 2001. Str. 47.
12. Jacques Robert: Most cyber-attacks will come form insiders. [URL: http://www.itweek.co.uk/News/1141354], 5. 6. 2003.
13. Jerman Blažič Borka: Internet. Ljubljana: Novi Forum, 1996. 87 str.
14. Kalakota Ravi, Whinston Andrew B.: Electronic Commerce: A Managerial's Guide. Reading: Addison-Wesley, 1997. 431 str.
15. Lunker Manish: Cyber Laws: A Global Perspective, 2001, 5 str. [URL: http://www.itcd.net/itcd-2001/papers/doc_pdf/doc_45.PDF], 13. 5. 2003.
16. Meeker Mary et al.: The Global Internet Primer. Equity Research. New York: Morgan Staneley Dean Witter, June 2000. 160 str.

17. Naimark Richard W.: The Potential Effect of E-Commerce: Developments on International Treaties. Haag: The International Bureau of the Permanent Court of Arbitration, 2002. 7 str.
18. Pavliha Marko et al.: Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem. Ljubljana: GV Založba, 2002. 222 str.
19. Pravila za vodenje postopkov v skladu z arbitražnimi pravila UNCITRAL. Ljubljana: Stalna arbitraža pri GZS, 2003. 11 str.
20. Sherman Mark: Introduction to Cyber Crime. Federal Judicial Center: Special Needs Offenders Bulletin, 2000, 5. 5 str.
21. The National White Collar Crime Center and the Federal Bureau of Investigation: IFCC 2002 Internet Fraud Report: January 1, 2002 - December 31, 2002. Washington: The National White Collar Crime Center. 2003. 23 str.
22. Timmers Paul: Electronic Commerce: Strategies and Models for Business to Business Trading. Chichester: Wiley, 1999. 268 str.
23. Toplišek Janez: Elektronsko poslovanje. Ljubljana: Založba Atlantis, 1998. 336 str.
24. Vavan Ilijana: B2C End-to-End Solution. [URL: http://www.microsoft.si/6ntk/PPTpredstavitve/Tor/241.ppt], 21.7.2001.
25. Westland Christopher J., Clark H. K. Theodore: Global Electronic Commerce: Theory and Case Studies. Cambridge: The MIT Press, 1999. 592 str.
26. World Information Technology and Services Alliance. [URL: http://www.witsa.org], 10. 5. 2003.

6. VIRI

1. Ahuja Vijay: Secure Commerce on the Internet. London: Academic Press, Inc., 1997. 298 str.
2. Barrett Daniel J.: Bandits on Information Superhighway: What you need to know. Bonn: O´Reilly & Associates, Inc., 1996. 229 str.
3. Computer Communication Networks. [URL: http://www.cs.washington.edu/homes/lazowska/cra/networks.html], 1997.
4. Computer Economics Security Review 2002. [URL: http://www.computereconomics.com/article.cfm?id=356], 7. 5. 2003.

5. Computer Mail Services: Spam cost calculator.
[URL: http://www.cmsconnect.com/Marketing/spamcalc.htm], 7. 5. 2003.
6. Dern Daniel P.: The Internet Guide for New Users. New York: McGraw-Hill, 1994. 570 str.
7. Ellsworth Jill H., Ellsworth Matthew V.: The Internet Business Book. New York: John Wiley & Sons, Inc., 1994. 376 str.
8. Faggioli Gabriele: Computer Crimes. Napoli : Esselibri - Simone, 2002. 158 str.
9. Forrester Research.
[URL: http://www.forrester.com/home/0,6092,1-0,FF.html], 15. 4. 2003.
10. Grad Anton, Leeming Henry: Slovensko angleški slovar. Ljubljana: DZS, 1993. 827 str.
11. Grad Anton, Škerlj Ružena, Vitorovič Nada: Veliki angleško-slovenski slovar. Ljubljana: DZS, 1992. 1377 str.
12. Hoffman Paul: Vse o internetu in World Wide Webu. Ljubljana: Pasadena, 1995. 203 str.
13. Honeycutt Jerry: Internet v uporabi. Izola: DESK, 1997. 338 str.
14. Internet in slovenska država v letu 2002.
[URL: http://www.sisplet.org/ris/ ris/uploads/publikacije/2003/34 Internet in Slo 2002.pdf], 15. 4. 2003.
15. Internet World Stats.
[URL: http://www.internetworldstats.com], 8. 2. 2003.
16. Kazenski zakonik RS in vdori v računalniški sistem.
[URL: http://www.arnes.si/si-cert/kz.html], 25. 2. 2003.
17. Kent Peter: 10 Minute Guide to the Internet. Indianapolis: QUE, 1994. 162 str.
18. Kodelja Marjan: Internet čedalje bolj doma med nami. Ljubljana: Slovenski delničar, 17. 5. 2000. Str. 1.
19. Marusich Carmen, Blackthron Sandy: Elektronsko poslovanje za telebane. Ljubljana: Založba Pasadena, 2000. 80 str.
20. Nielsen NetRatings. [URL: www.nielsennetratings.com], 26. 10. 2001.
21. Obligacijski zakonik (Uradni list RS, št. 83/01).
22. Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji (Uradni list RS, št.99/01).
23. Raba interneta v Sloveniji.
[URL: http://www.ris.org], 19. 4. 2003.
24. Sentencing Table.
[URL: http://www.ussc.gov/1998guid/Sentable.htm], 1998.
25. Skbnet: Varnost na internetu.
[URL: http://www.skb.si/html/skbnet/varnost_internet.html], 7. 5. 2003.

26. Smith Graham J. H.: Internet law and regulation. London : Sweet & Maxwell, 2002. 737 str.
27. Smith Richard E.: Internet Cryptography. Massachusetts: Addison Wesley Longman Inc., 1997. 356 str.
28. Šega Lidija: Veliki moderni poslovni slovar, angleško-slovenski. Ljubljana: CZ, 1997. 957 str.
29. Tavzes Miloš, Adelešič Gregor: Veliki slovar tujk. Ljubljana: Cankarjeva založba, 2002. 1303 str.
30. Turban Efraim, King David: Introduction to E-Commerce. New Jersey: Pearson Education, 2003. 537 str.
31. Turk Tomaž, Jaklič Jurij: Internet, Intranet in Ekstranet. Zbornik posvetovanja: Dnevi slovenske informatike 1998. Portorož: Slovensko društvo Informatika, 1998. Str. 133 - 141.
32. UNCITRAL: Model Law on Electronic Commerce with Guide to Enactment 1996. New York: United Nations, 1996. 56 str.
33. UNCITRAL: Model Law on Electronic Signatures with Guide to Enactment 2001. New York: United Nations, 2001. 72 str.
34. UNCITRAL Working Groups.
[URL: http://www.uncitral.org/english/workinggroups], 19. 4. 2003.
35. Uporabniki interneta in njihove značilnosti.
[URL: http://www.ris.org/splet/abstracts/uporab-ab.htm], 5. 6. 2003.
36. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00 in 2/01).
37. Vehovar Vasja et al.: Internet v Sloveniji. Izola: DESK, 1998. 315 str.
38. What You Should Know About Microsoft Security Bulletin MS03-026.
[URL: http://www.microsoft.com/security/security_bulletins/ms03-026.asp], 16. 6. 2003.
39. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/00).
40. Zorec Miha: Svetovni splet. Ljubljana: Tehniška založba Slovenije, 1998. 63 str.

PRILOGE

Priloga 1: Primerjava med ARPANET in NSFNET

Priloga 2: Prednost WWW storitve glede na ostalo tehnologijo

Priloga 3 : Število žrtev kraje identite po zveznih državah ZDA (na 100.000 prebivalcev) v obdobju od 1.1.2001 do 31.12.2001

Priloga 4: Vsebina Zakona o elektronskem poslovanju in elektronskem podpisu

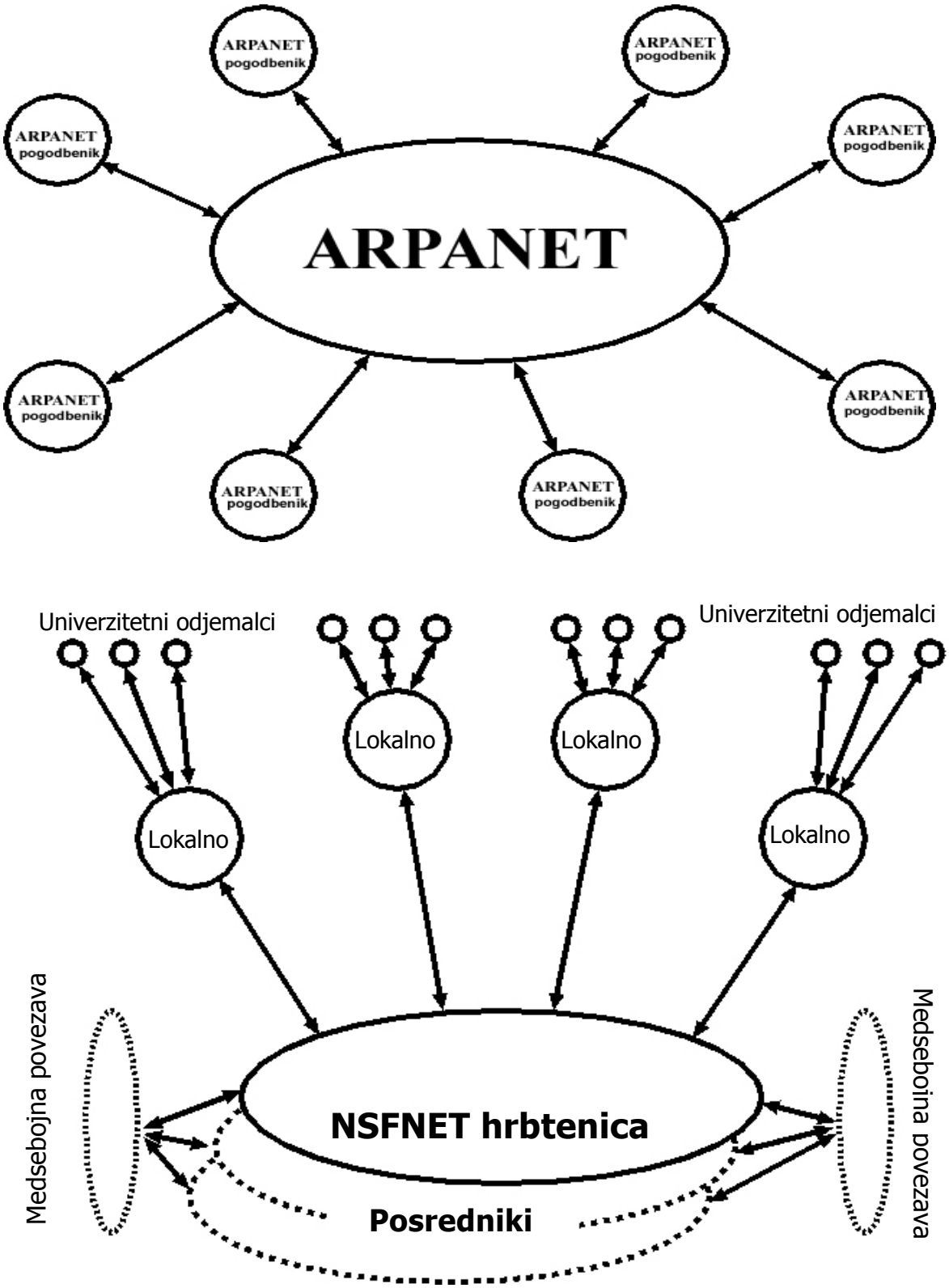
Priloga 5: Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje

Priloga 6: Obrazec za prijavo podatkov o overitelju

Priloga 7: Obrazec za prijavo predloga spremembe vpisa v register

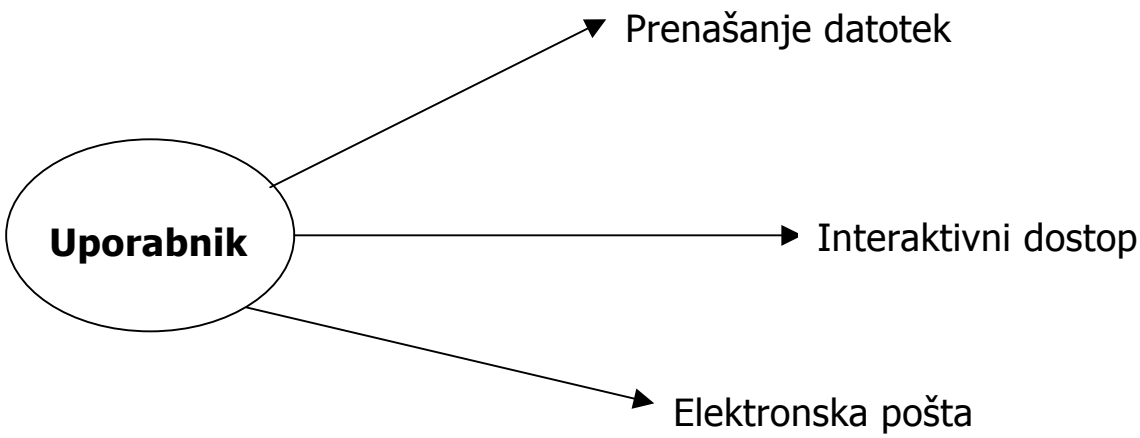
Priloga 8: Zaporne kazni v ZDA v mesecih glede na stopnjo kaznivega dejanja in kategorijo kriminalne zgodovine

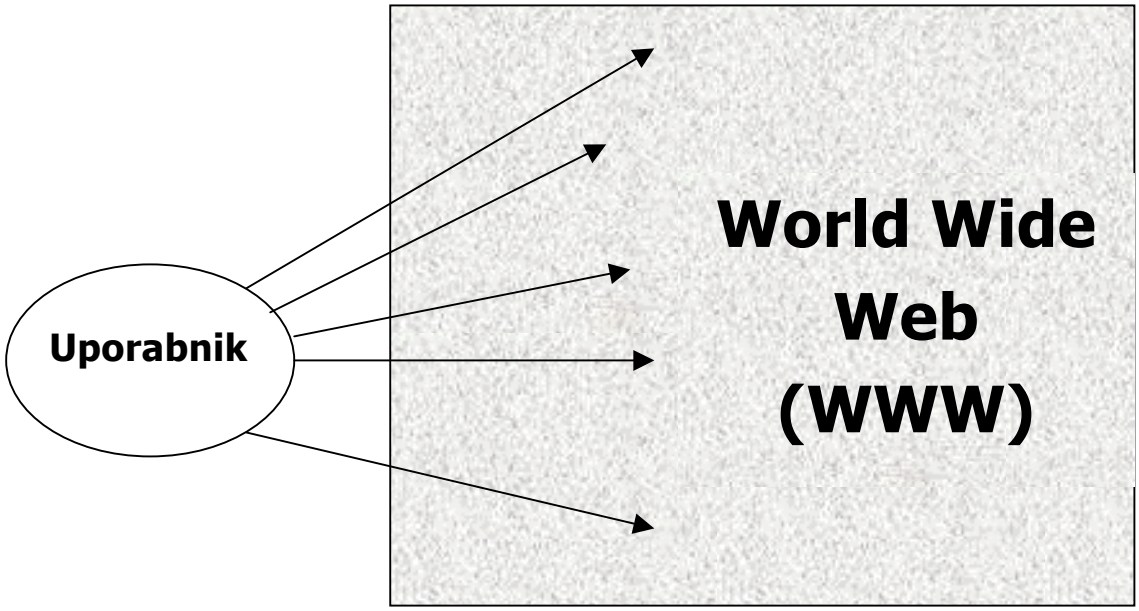
Priloga 1: Primerjava med ARPANET in NSFNET



Vir: Computer Communication Networks, 1997

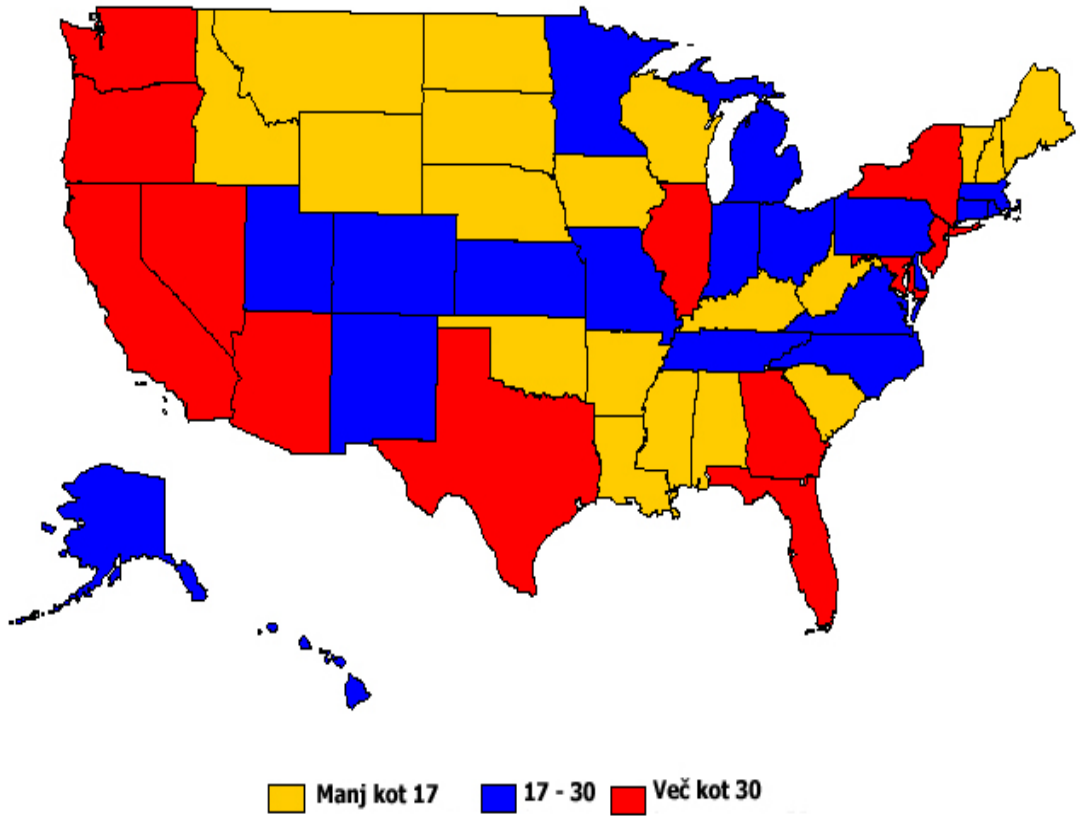
Priloga 2: Prednost WWW storitve glede na ostalo tehnologijo





Vir: Computer Communication Networks, 1997

Priloga 3 : Število žrtev kraje identite po zveznih državah ZDA (na 100.000 prebivalcev) v obdobju od 1.1.2001 do 31.12.2001



Vir: Identity Theft Victim Complaint Data, 2002.

Priloga 4: Vsebina Zakona o elektronskem poslovanju in elektronskem podpisu

Prvo poglavje
SPLOŠNE DOLOČBE

Drugo poglavje
ELEKTRONSKO POSLOVANJE

1. oddelek: Elektronsko sporočilo
2. oddelek: Podatki v elektronski obliki

Tretje poglavje
ELEKTRONSKI PODPIS

1. oddelek: Splošne določbe
2. oddelek: Potrdila in overitelji, ki jih izdajajo
3. oddelek: Kvalificirana potrdila in overitelji, ki jih izdajajo
4. oddelek: Tehnične zahteve za varno elektronsko podpisovanje
5. oddelek: Odgovornost overiteljev
6. oddelek: Nadzor
7. oddelek: Prostovljna akreditacija
8. oddelek: Veljavnost tujih potrdil

Četrto poglavje
KAZENSKE DOLOČBE

Peto poglavje
PREHODNE IN KONČNE DOLOČBE

Vir: Pavliha et al., 2002, str. 5-6.

Priloga 5: Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje

1. Splošne določbe
2. Splošno o varovanju infrastrukture overitelja
3. Fizično varovanje infrastrukture overitelja
4. Elektronsko varovanje infrastrukture overitelja
5. Tehnične zahteve na strani overitelja
6. Prijavna služba
7. Overiteljevi zaposleni
8. Tehnične zahteve za varno elektronsko podpisovanje in preverjanje varnega elekotrnskega podpisa
9. Zavarovanje odgovornosti
10. Notranja pravila overiteljev
11. Časovna veljavnost kvalificiranih potrdil
12. Varni časovni žig
13. Označba akreditiranega overitelja
14. Elektronsko poslovanje v javni upravi
15. Prehodni končni določbi

Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji

1. Splošne določbe
2. Prijava v register
3. Vodenje registra
4. Prehodne in končne določbe

Vir: Pavliha et al., 2002, str. 6.

Priloga 6: Obrazec za prijavo podatkov o overitelju

PODATKI O OVERITELJU:

I SPLOŠNI DEL

1. Firma oz. ime in priimek osebe, ki opravlja dejavnost overitelja:

2. Sedež oz. stalni naslov osebe, ki opravlja dejavnost overitelja:

3. Številka vpisa v sodni ali drug register:

4. Poštni naslov:

5. Elektronski naslov:

6. Spletni naslov:

7. Telefon:

8. Faks:

Če overitelj izdaja kvalificirana potrdila

9. Število overiteljevih zaposlenih:

10. Izobrazba overiteljevih zaposlenih
(navedeni morajo biti najmanj trije, ki izpolnjujejo pogoje):

11. Usposobljenost overiteljevih zaposlenih:

12. Dokaz o sklenjenem obveznem zavarovanju
(navedi priloge):

Tuj overitelj

13. Podatki o izpolnjevanju pogojev glede veljavnosti potrdil v republiki Sloveniji (navedi priloge):

II POSEBNI DEL *(Podatki se izpolnijo za vsako storitev posebej ter se priloži zahtevana dokumentacija)*

1. Naziv storitve:

2. Vrsta storitve:

3. Vrsta potrdil in elektronskega podpisa oz. časovnega žiga:

4. Notranja pravila in druga pomembna dokumentacija glede storitve:

5. Podatki o imeniku potrdil in registru preklicanih potrdil, če obstaja:

6. Podatki o tehnoloških značilnostih potrdila ali časovnega žiga:

7. Podatki o tehnoloških značilnostih ter načinu in pogostosti osveževanja imenika in registra preklicanih potrdil, če obstaja:

8. Podatki o službi za preklic ali drugi dežurni službi overitelja:

9. Podatki o prijavnih službah overitelja:

10. Seznam podatkov, ki so vsebovani v potrdilu ali časovnem žigu

11. Podatki o namenu ali omejitvi uporabe potrdil ali storitve:

12. Podatki o postopku in načinu preverjanja identitete imetnikov potrdil:

13. Rok veljavnosti izdanih potrdil:

14. Opis overiteljeve infrastrukture in postopkov s pripadajočo tehnično dokumentacijo (mora omogočati ocenitev v skladnosti z zahtevami veljavnih predpisov za vsako prijavljeno storitev)

15. Začetek opravljanja storitve:

16. Konec opravljanja storitve:

17. Drugi pomembni podatki glede prijavljene storitve:

Vir: Pavliha et al., 2002, str. 209-210.

Priloga 7: Obrazec za prijavo predloga spremembe vpisa v register

PRIJAVA PREDLOGA SPREMEMBE VPISA V REGISTRU

1. Firma oz. ime in priimek osebe, ki opravlja dejavnost overitelja:

2. Sedež oz. stalni naslov osebe, ki opravlja dejavnost overitelja:

3. Zaporedna številka vpisa v register overiteljev v Republiki Sloveniji:

Nove okoliščine ali dejstva, zaradi katerih se predlaga sprememba vpisa

Datum in podpis pooblaščene osebe:

Vir: Pavliha et al., 2002, str. 211.

Priloga 8: Zaporne kazni v ZDA v mesecih glede na stopnjo kaznivega dejanja in kategorijo kriminalne zgodovine

(V mesecih zaporne kazni)

	Kategorije kriminalne zgodovine (število točk kriminalne zgodovine)					
Stopnja kaznivega dejanja	**I (0 ali 1)**	**II (2 ali 3)**	**III (4, 5, 6)**	**IV (7, 8, 9)**	**V (10, 11, 12)**	**VI (ali več)**
1	0-6	0-6	0-6	0-6	0-6	0-6
2	0-6	0-6	0-6	0-6	0-6	1-7
3	0-6	0-6	0-6	0-6	2-8	3-9
4	0-6	0-6	0-6	2-8	4-10	6-12
5	0-6	0-6	1-7	4-10	6-12	9-15
6	0-6	1-7	2-8	6-12	9-15	12-18
7	0-6	2-8	4-10	8-14	12-18	15-21
8	0-6	4-10	6-12	10-16	15-21	18-24
9	4-10	6-12	8-14	12-18	18-24	21-27
10	6-12	8-14	10-16	15-21	21-27	24-30
11	8-14	10-16	12-18	18-24	24-30	27-33
12	10-16	12-18	15-21	21-27	27-33	30-37
13	12-18	15-21	18-24	24-30	30-37	33-41
14	15-21	18-24	21-27	27-33	33-41	37-46
15	18-24	21-27	24-30	30-37	37-46	41-51
16	21-27	24-30	27-33	33-41	41-51	46-57
17	24-30	27-33	30-37	37-46	46-57	51-63
18	27-33	30-37	33-41	41-51	51-63	57-71
19	30-37	33-41	37-46	46-57	57-71	63-78
20	33-41	37-46	41-51	51-63	63-78	70-87
21	37-46	41-51	46-57	57-71	70-87	77-96
22	41-51	46-57	51-63	63-78	77-96	84-105
23	46-57	51-63	57-71	70-87	84-105	92-115
24	51-63	57-71	63-78	77-96	92-115	100-125
25	57-71	63-78	70-87	84-105	100-125	110-137
26	63-78	70-87	78-97	92-115	110-137	120-150
27	70-87	78-97	87-108	100-125	120-150	130-162
28	78-97	87-108	97-121	110-137	130-162	140-175
29	87-108	97-121	108-135	121-151	140-175	151-188
30	97-121	108-135	121-151	135-168	151-188	168-210
31	108-135	121-151	135-168	151-188	168-210	188-235
32	121-151	135-168	151-188	168-210	188-235	210-262
33	135-168	151-188	168-210	188-235	210-262	235-293

34	151-188	168-210	188-235	210-262	235-293	262-327
35	168-210	188-235	210-262	235-293	262-327	292-365
36	188-235	210-262	235-293	262-327	292-365	324-405
37	210-262	235-293	262-327	292-365	324-405	360-D
38	235-293	262-327	292-365	324-405	360-D	360-D
39	262-327	292-365	324-405	360-D	360-D	360-D
40	292-365	324-405	360-D	360-D	360-D	360-D
41	324-405	360-D	360-D	360-D	360-D	360-D
42	360-D	360-D	360-D	360-D	360-D	360-D
43	D	D	D	D	D	D

*Oznaka D velja za dosmrtno zaporno kazen

Vir: Sentencing Table, 1998.

SLOVAR TUJIH IZRAZOV

ARPANET – omrežje Agencije za razvoj projektov, predstavlja začetnika interneta
Computer virus – računalniški virus, ki s svojim delovanjem onemogoči nemoteno delovanje računalniškega sistema
Cybercrime – elektronski kriminal
Cybercriminals – elektronski kriminalec
Common types of cybercrime – pojavne oblike elektronskega kriminala
Fraud – prevara
Host – gostitelj
IFCC – Center za prijavo internetnih prevar
Internet browser – spletni brskalnik
Internet scam – internetna prevara
Novel – novelirani, spremenjeni, dopolnjeni veljavni zakoni
Server – strežnik
Model law – vzorčni zakon
NSFNET – omrežje Nacionalne znanstvene fundacije, naslednik ARPANETA
Update – posodobitev, praviloma programska
WWW – svetovni splet