

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

TINA ZUPANIČ

**ZAZNAVANJE DEVIANTNEGA VEDENJA NA
INTERNETU MED MLADIMI**

DIPLOMSKO DELO

Ljubljana, 2005

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

TINA ZUPANIČ

MENTORICA: doc. dr. Tanja Oblak

SOMENTOR: doc. dr. Gregor Petrič

**ZAZNAVANJE DEVIANTNEGA VEDENJA NA
INTERNETU MED MLADIMI**

DIPLOMSKO DELO

Ljubljana, 2005

Iskreno se zahvaljujem mentorici dr. Tanji Oblak za vse idejne vzpodbude pri pisanju naloge ter somentorju dr. Gregorju Petriču za kritično oceno mojega diplomskega dela.

Posebna zahvala pa gre moji družini ter mojima najdražjima Ivu in Maiu.

KAZALO

KAZALO TABEL.....	4
KAZALO SLIK.....	5
1 UVOD	6
1.1 Struktura naloge	8
2 TEORETSKI VIDIKI DEVIANTNEGA DELOVANJA	8
2.1 Pregled različnih teorij deviantnega delovanja	12
2.1.1 Biološke oziroma fiziološke teorije deviantnosti	12
2.1.2 Psihološke teorije deviantnosti	13
2.1.3 Sociološke teorije deviantnosti.....	14
a) Funkcionalistični pogled	14
b) Interakcionistični pogled.....	16
c) Marksistični in neomarksistični pogled.....	18
2.1.4 Ekonomske teorije deviantnosti	20
3 DEVIANTNOST V KIBERNETSKEM PROSTORU	26
3.1 Zgodovinski razvoj pojma kibernetške kriminalitete.....	29
3.1.1 Opredelitve pojma	30
3.2 Kdo so kibernetški »kriminalci« in kdo so žrtve?	31
3.2.1 Kibernetški prestopniki	31
3.2.2 Žrtve kibernetškega kriminala.....	34
3.3 Vrste kaznivih dejanj v kibernetškem prostoru in odkrivanje kibernetškega kriminala.....	34
3.3.1 Kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov.....	34
a) Nedovoljen dostop do računalniških sistemov.....	34
b) Onemogočanje in poškodovanje računalniških sistemov	35
c) Izdelava in distribucija računalniških programov za storitev kaznivih dejanj	35
3.3.2 Kazniva dejanja, povezana z računalnikom	35
3.3.3 Kazniva dejanja, povezana z vsebino.....	36
3.3.4 Kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic	36
3.3.5 Problematika odkrivanja kibernetškega kriminala	36
3.4 Zakonodaja v zvezi s kibernetško kriminaliteto.....	38
3.4.1 Konvencija o kibernetški kriminaliteti	40

4	RAZISKOVALNI OKVIR ZAZNAVANJA DEVIANTNEGA VEDENJA NA INTERNETU.....	41
	4.1 Definicije pojmov.....	42
	4.2 Hipoteze.....	42
5	OPIS VZORCA IN ZBIRANJE PODATKOV.....	44
6	OPERACIONALIZACIJA.....	46
	6.1 Indikatorji spremenljivk.....	46
	6.2 Operacionalni model.....	49
7	ANALIZE IN REZULTATI.....	50
	7.1 Osnovne statistike posameznih indikatorjev in izvedenih spremenljivk.....	50
	7.2 Povezanost izvedenih spremenljivk.....	59
	7.3 Preverjanje modela in hipotez.....	60
	7.3.1 Preverjanje modela.....	60
	7.3.2 Preverjanje hipotez.....	64
8	ZAKLJUČEK.....	65
9	LITERATURA in VIRI.....	68
10	PRILOGE.....	71
	Priloga A - Statistična analiza - dodatek.....	71
	Priloga B - Členi kazenskega zakonika RS, ki neposredno ali posredno rešujejo vprašanje kibernetke kriminalitete.....	74
	Priloga C - Povzetek konvencije o kibernetki kriminaliteti.....	86

KAZALO TABEL

Tabela 1: Členi, ki urejajo področje kibernetске kriminalitete, ter število kaznivih dejanj s področja kibernetске kriminalitete v letu 2002	38
Tabela 2: Poimenovanje posameznih indikatorjev na podlagi Kazenskega zakonika	48
Tabela 3: Frekvenčne porazdelitve posameznih indikatorjev – deleži (spremenljivka percepcija pravnih norm).....	50
Tabela 4: Frekvenčne porazdelitve posameznih indikatorjev – deleži (spremenljivka izkušnja deviantnosti)	51
Tabela 5: Frekvenčne porazdelitve posameznih indikatorjev – deleži (spremenljivka toleriranje deviantnosti).....	51
Tabela 6: Spremenljivka toleriranje deviantnosti – osnovne statistike	52
Tabela 7: Faktorska analiza – »patteren« uteži (n=324)	55
Tabela 8: 1. faktor – toleriranje »škodljive« deviantnosti.....	56
Tabela 9: 2. faktor – toleriranje »neškodljive« deviantnosti	56
Tabela 10: Korelacijska matrika izvedenih spremenljivk (n=332)	59
Tabela 11: Regresijska analiza 1 – odvisna spremenljivka toleriranje »škodljive« deviantnosti – regresijski koeficienti (n=332).....	60
Tabela 12: Regresijska analiza 1 – odvisna spremenljivka toleriranje »škodljive« deviantnosti – vrednosti posameznih statistik (n=332).....	60
Tabela 13: Regresijska analiza 2 – odvisna spremenljivka toleriranje »neškodljive« deviantnosti – regresijski koeficienti (n=332).....	62
Tabela 14: Regresijska analiza 2 – odvisna spremenljivka toleriranje »neškodljive« deviantnosti – vrednosti posameznih statistik (n=332)	62
Tabela 15: Korelacije med faktorji pri poševni rotaciji:	71
Tabela 16: Korelacijska matrika posameznih indikatorjev spremenljivke percepcija pravnih norm.....	71
Tabela 17: Korelacijska matrika posameznih indikatorjev spremenljivke izkušnja deviantnosti	72
Tabela 18: Korelacijska matrika posameznih indikatorjev spremenljivke toleriranje deviantnosti	73

KAZALO SLIK

Slika 2: Teoretski model zaznavanja deviantnega vedenja na internetu	41
Slika 3: Grafični prikaz porazdelitve deležev anketiranih študentov glede na spol (n =332)	45
Slika 4: Grafični prikaz porazdelitve deležev anketiranih študentov po letniku študija (n = 330).....	45
Slika 5: Grafični prikaz porazdelitve deležev anketiranih študentov glede na fakulteto (n = 334).....	46
Slika 6: Grafični prikaz operacionalnega modela	49
Slika 7: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke percepcija pravnih norm (n=331).....	53
Slika 8: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke izkušnja deviantnosti (n=324).....	54
Slika 9: Faktorska analiza – »scree« diagram (n=324)	55
Slika 10: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke toleriranje deviantnosti – 1. faktor (n=318).....	57
Slika 11: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke toleriranje deviantnosti – 2. faktor (n=336).....	58
Slika 12: Regresijski model 1 – odvisna spremenljivka toleriranje »škodljive« deviantnosti.	61
Slika 13: Regresijski model 2 – odvisna spremenljivka toleriranje »neškodljive« deviantnosti	63
Slika 14: Grafični prikaz faktorjev po poševni rotaciji	71

1 UVOD

V zadnjem desetletju prejšnjega stoletja se je internet razvil v globalno omrežje, ki briše meje med lokalnimi skupnostmi, državami in nenazadnje tudi med kontinenti. Milijoni uporabnikov ga vsakodnevno uporabljajo za izvajanje različnih poslov, prenosa pošte, zabave itd., saj v primerjavi s tradicionalnimi komunikacijskimi potmi nudi številne prednosti, kot so npr. izredno hiter prenos informacij, anonimnost in nizki stroški uporabe. Vendar pa se prav v prednostih interneta skrivajo tudi njegove slabosti, saj nudi potencialnim storilcem kaznivih dejanj veliko možnosti zlorab.

Znano je namreč, da je v primerjavi s kriminalnimi dejanji, storjenimi v fizičnem prostoru, kazniva dejanja v kibernetnem prostoru veliko težje odkriti, saj v kibernetnem prostoru, katerega del je tudi internet, pravila delovanja pogosto ostajajo nepoznana pa tudi sankcije za potencialne zlorabe le redko dosežejo storilce kaznivih dejanj. Organi pregona torej stojijo na bolj majavih tleh, kar storilcem kaznivih dejanj omogoča, da njihova dejanja ostanejo neopažena ali pa celo nekaznovana. Zaradi slednjih dveh dejstev pa posameznik, ki se zaveda, da je njegovo dejanje težko odkriti in bo zelo verjetno ostal nekaznovan, v primeru, da mu takšno dejanje pomeni kakršno koli korist, na takšen način deluje še naprej ali pa na ta dejanja gleda kot na nekaj čisto normalnega, saj takšna dejanja tako ali tako niso kaznovana. Storilci kaznivih dejanj torej pogosto tehtajo med potencialnimi stroški in koristmi. Ker pa je verjetnost, da storilca deviantnega dejanja doletijo kakršne koli sankcije v kibernetnem prostoru, zelo majhna, koristi največkrat presežejo stroške, se posamezniki pogosto odločijo za deviantno delovanje. V primeru deviantnih dejanj v kibernetnem prostoru gre pogosto tudi za nepoznavanje pravnih norm, ki veljajo tako za fizični kot tudi za kibernetni prostor. Zaradi izredno lahkega in hitrega dostopa do najrazličnejših vsebin v kibernetnem prostoru pa posamezniki ob njihovi uporabi pogosto sploh ne pomislijo, da njihova uporaba pomeni kakršno koli kršenje pravnega reda.

Že klasične sociološke teorije, kot so funkcionalistična, interakcionistična in marksistična teorija, so se ukvarjale z dejstvom, da so nekatera dejanja, ki jih določeni posamezniki počnejo, zelo pogosto v nasprotju s početjem, ki ga drugi pripadniki družbe ocenjujejo kot sprejemljivo. V svojem življenju si posamezniki namreč

ustvarjajo sodbe o zaželenih oziroma nezaželenih oblikah vedenja. Svoje sodbe pa nato prevedejo v ugodne oziroma neugodne posledice za tiste, ki ta dejanja storijo. Katera pa so tista dejanja, ki so označena kot deviantna? To je odvisno od prostora, časa in družbene skupine, ki ji posameznik pripada (Vander Zanden, 1993: 129). Ker norme pogosto ne predstavljajo neke stroge razmejitev med deviantnim in sprejemljivim vedenjem, ampak vsebujejo poleg navodil za delovanje tudi določeno možno, še sprejemljivo odstopanje od t.i. pravilnega delovanja (Williams v Vander Zanden, 1993: 131), posamezniki pogosto napačno zaznavajo meje norm. Z drugimi besedami: posamezniki o svojem načinu delovanja oziroma ravnanja pogosto mislijo, da delujejo družbeno sprejemljivo (torej oni sami svoja dejanja dopuščajo prav zaradi zmotnega prepričanja o sprejemljivosti teh dejanj), čeprav v resnici temu ni tako. Emil Durkheim (v Haralambos in Holborn, 1999: 397) je menil, da je zaradi dejstva, da so posamezniki izpostavljeni različnim vplivom in okoliščinam, nemogoče, da bi bili vsi posamezniki enaki oziroma, da niso vsi posamezniki enako naklonjeni spoštovanju zakona, s tem pa tudi dopuščanju posameznih oblik deviantnosti.

Aktualnost obravnavane tematike se mi zdi v današnji informacijski družbi izrednega pomena, saj je potrebno poudariti, da je lahko potencialna žrtev kibernetских prestopnikov vsak uporabnik interneta in računalnika. Žrtev je lahko vsakdo izmed nas, zato je še posebej pomembno, da se tega zavedamo ter da proti temu tudi ukrepamo. Na drugi strani pa sami sebi ne smemo pustiti prestopiti mej pravnega reda le zato, ker bodo morda naša, v kibernetickem prostoru (v primerjavi s fizičnim) storjena, nelegalna dejanja zlahka ostala neopažena in nekaznovana.

1.1 Struktura naloge

V diplomski nalogi bom raziskovala, ali posameznikovo zaznavanje pravnih norm, ki ni v skladu z zakonodajo družbe, kateri posameznik pripada, ter izkušnja deviantnosti posameznika dejansko vplivata na toleriranje deviantnih dejanj. Raziskovanja te problematike se bom najprej lotila preko orisa teoretskega ozadja samega problema, in sicer predvsem na podlagi različnih teorij deviantnosti. Tu se bom dotaknila bioloških, psiholoških in socioloških teorij deviantnosti, med slednjimi pa bom orisala funkcionalistični, interakcionistični in marksistični vidik deviantnosti. Poleg omenjenih teorij pa se bom dotaknila še ekonomskih teorij deviantnosti, med katerimi bom nekoliko natančneje opisala teorijo racionalne izbire. V tretjem poglavju bom opisala, kako je z deviantnim vedenjem v kibernetnem prostoru. Najprej bom opisala zgodovinski razvoj samega pojma, nato pa opredelila pojem kibernetne kriminalitete ter prešla preko poglavja o kibernetnih prestopnikih in žrtvah kibernetnega kriminala do posameznih oblik kibernetnega kriminala in zakonodaje v zvezi z njim. V četrtem poglavju bo sledil raziskovalni okvir zaznavanja deviantnega vedenja na internetu, nato pa bom na podlagi analize ankete, ki sem jo izvedla med študenti, poskušala ugotoviti, ali percepcija pravnih norm in izkušnja deviantnosti dejansko vplivata na to, kako posameznik gleda na deviantnost – jo tolerira ali ne. Empiričnemu delu naloge pa sledita še razprava in zaključek.

2 TEORETSKI VIDIKI DEVIANTNEGA DELOVANJA

V vseh družbah nekateri ljudje od časa do časa prestopijo meje, ki jih določajo norme. *Norme* nam namreč povedo, kako naj bi v neki družbi delovali, ne pa tudi, kako ljudje v tej družbi dejansko delujejo (Vander Zanden, 1993: 129). Norme so torej vedenjski vzorci, ki jih pripadniki družbe ocenjujejo kot normalne v posameznih družbenih situacijah (O'Donnell, 1994: 8), in predstavljajo vedenjski standard, ki je skupen vsem pripadnikom neke družbe (O'Donnell, 1994: 373). Nekatera dejanja, ki jih določeni posamezniki počnejo, so zelo pogosto v nasprotju s početjem, ki ga drugi pripadniki družbe ocenjujejo kot sprejemljivo. Družbeno življenje torej ne označujejo družbeno ustrezna dejanja, marveč *deviantnost*, ki je oblika vedenja, katerega večina

pripadnikov neke družbe označuje za kaznivega in nad mejami sprejemljivega (Vander Zanden, 1993: 129). Deviantno vedenje ponavadi izzove formalne in neformalne kazni, omejitve in ostale kontrolne družbene mehanizme. Ti formalni oziroma neformalni družbeni mehanizmi pa silijo večino posameznikov neke družbe, da delujejo v skladu z družbenimi normami (Jeong-Yoo in Gang, 2001: 500).

Deviantnost ni prirojena vedenjska lastnost posameznikov, ampak je lastnost, ki je posameznikom dodeljena s strani nekih družbenih definicij (npr. pravnega reda). V času svojega življenja posamezniki ustvarjajo sodbe o zaželenih oziroma nezaželenih oblikah vedenja. Svoje sodbe nato prevedejo v ugodne oziroma neugodne posledice za tiste osebe, ki ta dejanja storijo. To pomeni, da je deviantnost to, kar posamezniki pravijo, da je. Katera pa so tista dejanja, ki so označena kot deviantna, pa močno variira glede na prostor, čas in družbeno skupino, ki ji posameznik pripada; torej družbeno občinstvo odloča o tem, ali je neko dejanje deviantno ali ne (Vander Zanden, 1993: 129).

V vsakdanjem življenju pogosto odkrivamo, da norme ne predstavljajo neke stroge razmejitve med deviantnim in sprejemljivim, ampak vsebujejo poleg navodil za delovanje tudi določeno stopnjo variacije v dejanjih. Kar pomeni, da določena oblika dejanja, ki je sicer označena kot deviantno, ni nujno takšna ali pa je celo popolnoma družbeno sprejemljiva (Williams v Vander Zanden, 1993: 131). »Zato norme ponavadi dovoljujejo za določene oblike vedenja nove oziroma drugačne oblike tega vedenja, ki pa še vedno ostajajo v mejah dovoljenega oziroma sprejemljivega vedenja« (Merton v Vander Zanden, 1993: 131). Deviantnega vedenja pa ne smemo enačiti s *kriminaliteto*, čeprav se oba pojma pogosto prekrivata. Deviantnost je namreč veliko obsežnejši pojem od kriminalitete, slednja se namreč nanaša le na ravnanja, ki kršijo pravne norme (Giddens, 2001: 203). *Kriminaliteta* so protipravna dejanja, ki jih zakon zaradi njihove nevarnosti določa kot kazniva dejanja in hkrati določa njihove znake in kazni zanje (Kazenski zakonik Republike Slovenije, 7. člen).

Pravna norma predstavlja vir prava in vir informacij. Pravna norma kot vir prava pomeni, da je neka norma razglašena za institucionalizirano vedenje, ki posameznikom, sodelujočim v določenih družbenih relacijah, zagotavlja določene pravice, poleg pravic pa jim nalaga tudi določene dolžnosti. Pravna norma kot vir

informacij pa pomeni, da pravna norma informira posameznike o tem, kakšna so pričakovanja normalnega delovanja v skladu s pravnim redom (*Sharankova*, 1999: 406). Glavna vloga pravnih norm je vzdrževanje družbene ureditve, saj norme vsebujejo zapovedi, prepovedi, napotke, dovoljenja in sankcije. Kazenski ukrepi, ki jih predvidijo državni organi, ki so pristojni na tem področju, pa zagotavljajo uresničevanje norm, in sicer s sredstvi prisile, ki jih uporablja nadzorstvo, ki je »nasploš zato, da bdi nad normami in pazi, kako se uresničujejo« (*Pečar*, 1988: 78). Z vidika prava je pravna norma pravilo o vedenju, ki vsebuje določbe o uporabi državne kazni v primeru kršitve te norme (v kolikor bo kršitelj prijet) (*Pečar*, 1988: 79). Pravo pa je sredstvo družbenega nadzorstva in je le ena izmed oblik družbenih norm. Posamezniki naj bi se, ko delujejo v družbi, vedli po pravnih normah, ki jih sprejemajo centri državne moči. Pravne norme so navadno merila za ocenjevanje vedenja in služijo nadzorovalcem pri določanju ukrepov za kršitelje. So torej ključno sredstvo ter instrument nadzorstva, saj postavljajo merila za ugotavljanje deviantnega delovanja posameznikov. Norme kazenskega prava so predvsem prisila v fizičnem in psihološkem smislu. Prisiljevanje opravljajo mehanizmi nadzorovanja s svojimi zastopniki preko različnih dejavnosti nadzorovanja: od ugotavljanja in odkrivanja, pregona in sojenja, do izvrševanja kazenskih sankcij (*Pečar*, 1988: 79–80).

Če želimo, da svet deluje po ustaljenih smernicah, morajo posamezniki spoštovati pravila, ki jim jih narekuje družba, v kateri živijo. Družbeni red narekuje ljudem smernice vedenja, ki se jih morajo držati oziroma se jih mora držati vsaj večina posameznikov (*Sagerin, Gibbs in Tyler v Vander Zanden*, 1993: 131). Družbe pa si zagotavljajo spoštovanje njihovega družbenega reda z že omenjenimi sredstvi družbenega nadzora. Obstajajo trije glavni načini družbenega reda, in sicer:

- *način, ki vodi posameznike k internalizaciji družbenih normativnih pričakovanj;*

Posamezniki so v življenju podvrženi nenehni socializaciji – procesu, v katerem ponotranjijo načine mišljenja, čutenja in primerne oblike delovanja v družbi. Ko se posamezniki »poglabljajo« v neko družbeno skupino, razvijejo samo-predstave, ki regulirajo njihovo delovanje v skladu z normami družbene skupine, ki ji pripadajo. Posamezniki, ki se vedejo na enak način kot drugi člani družbene skupine, ki ji pripadajo, si s takšnim načinom delovanja pridobijo lastne identitete in občutek

ugodja. Skupino, ki ji pripadajo, imajo za svojo, prav tako pa imajo za svoje tudi norme te družbene skupine. Na ta način družbena kontrola postane samo-kontrola (Vander Zanden, 1993: 132–133).

- *način, ki strukturira svet posameznikovih družbenih izkušenj;*

Tudi družbene institucije so tiste, ki oblikujejo naše izkušnje. V veliki meri posamezniki nezavedno gradijo na njihovem občutku realnosti na način, kot ga narekuje družba ter njene strukturne alternative, to pa pomeni, da posamezniki živijo v na nek način »omejenem« svetu (Vander Zanden, 1993: 133).

- *ter način, ki uporablja različne formalne in neformalne sankcije* (Vander Zanden, 1993: 131–132).

Vander Zanden (1993: 133–134) pravi, da se posamezniki prilagajajo družbenim normam predvsem zaradi zavedanja možne kazni v primeru, da bi te norme prekršili. Tisti posamezniki, ki kršijo pravila, se soočajo z neodobravanjem, sovražnostjo, preganjanjem in celo zapornimi kaznimi; medtem ko si posamezniki, ki se ravnavajo po družbenih pravilih, pridobijo hvalo, priljubljenost, prestiž ipd. Obstajajo torej slabe strani družbeno neprimerne vedenja ter dobre strani družbeno primerne vedenja, česar se zavedajo tudi posamezniki.

Becker (v Pečar, 1988: 153) pa pravi, da družba sama ustvarja deviantnost z izdelovanjem pravil, katerih kršitve pomenijo odklonskost, hkrati ko zoper kršilce uporablja norme in jih označuje kot deviantne, kriminalne ali nekonformne. Posameznik je torej v družbenem okolju vedno postavljen pred pričakovanja, ki jih o njegovem vedenju gojijo drugi, katerim se mora prilagajati. Če se ne, je deviant in v kolikor ne upošteva družbeno sankcioniranih norm, je kršitelj in zato objekt obravnavanja družbenih kontrolnih mehanizmov (Pečar, 1988: 371). »Sredstvo za doseganje poslušnosti, ubogljivosti in konformizma pa je predvsem kaznovanje« (Pečar, 1988: 138).

Z Beckerjevega vidika »deviantnost ni lastnost posameznikovega delovanja, ampak posledica »etikete«, ki jo družba ustvarja z izdelovanjem pravil in sankcij, ki se

nanašajo na prestopnike. Torej je deviant tisti, kateremu je bila etiketa uspešno pripeta, deviantno vedenje pa je vedenje, ki ga družba označuje kot takšnega« (Becker v Fulcher in Scott, 1999: 153). Na drugi strani pa po Vander Zandenevem mnenju zavedanje posameznikov o možnih kaznih za storjena deviantna dejanja ustvarja deviantnost.

2.1 Pregled različnih teorij deviantnega delovanja

Deviantnost so dejanja, ki odstopajo od ustaljenih družbeno sprejetih norm in vrednot oziroma družbeno sprejetih načinov delovanja. Deviantne osebe pa so tisti posamezniki, ki zavračajo življenje večine, ki deluje na podlagi nekih splošno sprejetih družbenih pravil (Haralambos in Holborn, 1999: 393). Predmet moje analize so deviantna dejanja, ki so storjena v kibernetnem prostoru in so v nasprotju s pravnimi normami, ki regulirajo to področje. Poglavje, ki sledi, predstavlja zgolj kratek oris posameznih teorij deviantnosti s poudarkom na teoriji racionalne izbire, saj le-ta najbolj označuje deviantna dejanja, ki so predmet moje analize.

2.1.1 Biološke oziroma fiziološke teorije deviantnosti

Biološke teorije izhajajo iz sklepanja, da so nekateri posamezniki zaradi svojega genskega zapisa mnogo bolj nagnjeni k deviantnosti kot drugi. Nekateri posamezniki imajo torej neko organsko napako ali patologijo, zaradi katere so nagnjeni k deviantnemu vedenju. Temelje biološkim teorijam je leta 1876 postavil italijanski zdravnik Lombroso, ki je v svojih raziskavah prišel do ugotovitve, da so ljudje po naravi dobri in ne počenjajo kaznivih dejanj, kar naj bi bil rezultat civilizacijskega razvoja. Nekoč pa so bili ljudje agresivni, vendar je civilizacija to agresivnost presegla. Med temi ljudmi pa obstaja manjšina, kjer so se obdržale agresivnosti iz preteklosti, kar se kaže v njihovih fizičnih pomanjkljivostih. To so t.i. »atavistični stigmati« (»atavistic features«). Gre za telesne pomanjkljivosti in po njegovem mnenju ima zločinec šibko sposobnost lobanje, močno čeljust, povezane obrvi, pomembni pa

sta tudi oblika lobanje in dolžina rok. Kdor ima teh pet telesnih pomanjkljivosti, je rojen hudodelec (Fulcher in Scott, 1999: 154–155; Macionis, 2005: 190).

Tudi Sheldon je prišel do podobnih ugotovitev. Na podlagi svojih raziskav je razlikoval med tremi glavnimi fiziološkimi tipi oz. strukturami človeka, ki se razvijejo že pred rojstvom, izmed katerih je eden direktno povezan z deviantnostjo (v Giddens, 2001: 205–206). Sheldon je namreč predvideval, da telesna struktura posameznika napoveduje njegovo deviantno delovanje. V svojih raziskavah je namreč ugotovil, da se deviantno delovanje najpogosteje pojavlja med moškimi, ki so mišičaste, atletske postave (v Macionis, 2005: 190). Po Sheldonovem mnenju so k deviantnosti najbolj nagnjeni tisti posamezniki, ki so močni, debeli in imajo agresiven, energičen, ambiciozen in vsiljiv temperament, iščejo razvedrilo, so egoistični, tvegajo in imajo potrebo po zadovoljstvu, so drzni v spopadu ter so zaradi omenjenih lastnosti bolj nagnjeni k storitvi kaznivih dejanj. Vendar pa to ne velja za športnike, ki imajo prav takšne značilnosti (Giddens, 2001: 205–206).

2.1.2 Psihološke teorije deviantnosti

Podobno kot biološke teorije tudi psihološke teorije iščejo razlage za deviantno vedenje v posameznikih samih in ne v družbi, vendar pa se za razliko od bioloških teorij osredotočajo na posameznikovo osebnost (Giddens, 2001: 206). Tako Hans Eysenck sklepa, da obstaja povezava med gensko pogojenimi značilnostmi in kriminalnim oz. deviantnim vedenjem. Trdi namreč, da posamezniki podedujejo različne osebnostne lastnosti, ki jih vodijo h kriminaliteti. Za primer si vzemimo ekstrovertirano osebo, ki naj bi po mnenju Eysencka še posebno rada kršila zakon. Ekstrovertirana oseba namreč potrebuje razburjenje, pogosto rada tvega, ravna brez premišljanja ter je na splošno izredno impulzivna. Poleg omenjenih značilnosti pa se ekstrovertirane osebe težje prilagodijo položaju v primerjavi z introvertiranimi. Korak naprej v psiholoških teorijah je naredil John Bawly, ki je trdil, da deviantnost ni podedovana, ampak izhaja iz otrokove zgodnje socializacije. Otrok, ki je v najzgodnejšem obdobju prikrajšan za materinsko ljubezen, se tako lahko razvije v psihopatsko osebnost (Haralambos in Holborn, 1999: 396).

2.1.3 Sociološke teorije deviantnosti

Za razliko od bioloških in psiholoških teorij se sociološke teorije deviantnosti osredotočajo na vpliv družbenih institucij in družbe, ki pogojujejo posameznikovo deviantno vedenje. Tako npr. funkcionalistična teorija deviantnosti išče izvor za deviantno vedenje posameznikov v naravi družbe, in sicer pravi, da je deviantnost nujen oziroma neizogiben del družbe. Z vidika funkcionalistov zločin v družbi ni samo neizogiben, ampak je lahko tudi funkcionalen. Za razliko od funkcionalistov pa interakcionisti poudarjajo pomembnost pomenov, ki jih različni akterji vnašajo in razvijajo znotraj interakcijske situacije, in sicer je definicija deviantnosti dogovorjena med vpletenimi akterji. Marksisti pa trdijo, da je kriminaliteta naraven »izrastek« kapitalistične družbe, ki jo generira kapitalistični ekonomski sistem.

Natančneje te teorije zastopajo naslednje ideje:

a) Funkcionalistični pogled

Funkcionalistična analiza deviantnosti izhaja iz družbe kot celote in išče izvor deviantnosti v naravi družbe. Tako je Emile Durkheim sklepal, da je kriminaliteta neizogiben in normalen pojav družbenega življenja ter »integralni del vseh zdravih družb«. Slednje je namreč neizogibno, ker vsak posameznik ne more biti enako predan kolektivnim občutkom. Zaradi dejstva, da so posamezniki izpostavljeni različnim vplivom in okoliščinam, je nemogoče, da bi bili vsi enaki, zaradi česar niso vsi posamezniki enako naklonjeni spoštovanju zakona (Haralambos in Holborn, 1999: 397).

Za Durkheima (1969: 62) je deviantnost pomemben, neizogiben in normalen pojav družbenega življenja, ki poziva moralne in pravne zakone, da delujejo enotno. Pravi, da »ne moremo reči, da neko dejanje razburi kolektivno zavest, ker je deviantno; ampak je deviantno, ker razburi kolektivno zavest. Torej nekega dejanja ne obsojamo zato, ker je deviantno, ampak je deviantno, ker ga obsojamo« (Durkheim, 1995: 123–124).

Deviantnost po Durkheimovem mnenju spodbuja tudi družbeno solidarnost. Pravi, da se najpogosteje zgodi, da deviantno delovanje posameznikov vzpodbudi družbo kot celoto, da združeno nastopi proti deviantom in na takšen način zagotovi ponovno vdanost (»adherence«) družbenim vezem. Deviantnost po Durkheimovem mnenju ustvarja družbene spremembe, tako da večina kršitev norm doživi nasprotovanje večine, nekatere takšne kršitve pa nasprotovanj večine ne doživijo. Pogosto tako nekatera dejanja, ki so bila še nedavno obravnavana kot deviantna, postanejo del norm, ker so doživela odobravanje s strani družbene večine. Ker je določena količina sprememb zdrava za družbo, saj lahko le tako družba napreduje in ne stagnira, je tudi deviantnost nujna (Durkheim, 1995: 127).

Z vidika funkcionalistov zločin v družbi ni samo neizogiben, ampak je lahko tudi funkcionalen. Disfunkcionalen pa postane takrat, ko je njegova stopnja nenavadno nizka ali pa previsoka. Durkheim namreč dokazuje, da se vse družbene spremembe začnejo z neko obliko deviantnosti, da pa bi se družbena sprememba dejansko zgodila, mora »včerajšnja deviantnost« postati »današnja normalnost«. Ker je določena količina sprememb zdrava za družbo, saj lahko le tako družba napreduje in ne stagnira, je tudi deviantnost nujna (Haralambos in Holborn, 1999: 397–398).

Cohen je analiziral dve pozitivni funkciji deviantnosti, in sicer pravi, da je deviantnost lahko (v Haralambos in Holborn, 1999: 398):

- *varnostni ventil*, ki zagotavlja razmeroma neškodljiv izraz nezadovoljstva, kar ščiti družbeni red;
- *koristen svarilni mehanizem*, ki kaže, da nek del družbe slabo funkcionira.

Durkheim (v Macionis, 2005: 192) v deviantnem vedenju posameznikov ne vidi ničesar abnormalnega, še več – pravi, da ima deviantnost štiri nujne funkcije:

1. *Deviantnost utrjuje kulturne vrednote in norme.* Kot moralna bitja dajejo posamezniki prednost nekaterim oblikam vedenja pred drugimi. Durkheim pravi, da dobro ne mora obstajati brez zlega, prav tako pa pravičnost ne mora obstajati brez kriminala. Tako je deviantnost potrebna, da določa in vzdržuje moralo.
2. *Reakcija na deviantnost razjasnjuje moralne meje.* Z označitvijo nekaterih posameznikov kot deviantnih so postavljene meje med dobrim in slabim.
3. *Reakcija na deviantnost pospešuje družbeno enotnost.* Posamezniki ponavadi reagirajo na posamezne oblike deviantnih dejanj s kolektivnim ogorčenjem.
4. *Deviantnost spodbuja družbeno spremembo.* Deviantni posamezniki predstavljajo moralne družbene meje, predlagajo alternative že obstoječim oblikam vedenja in na ta način spodbujajo spremembo.

b) Interakcionistični pogled

Interakcionistični pogled na deviantnost poudarja pomembnost *pomenov*, ki jih različni akterji vnašajo in razvijajo znotraj interakcijske situacije. Vendar pa ti pomeni niso ustaljeni in jasno izraženi, ampak se v interakcijskem procesu preoblikujejo in razvijajo. S tega vidika je definicija deviantnosti dogovorjena med vpletenimi akterji. Posamezniki se namreč ne odzivajo pasivno na zunanje sile, ampak pred odločitvijo, kako se odzvati, dogodkom pripišejo pomene (Haralambos in Holborn, 1999: 413).

Teorija etiketiranja se osredotoča na družbeno naravo procesov, v katerih družbene skupine označujejo nekatere posameznike kot deviantne (Doter, Roebuck, Gove in Walsh v Kemmayer in dr., 1994: 166).

Becker v teoriji etiketiranja trdi, da »družbene skupine ustvarjajo deviantnost s postavljanjem pravil, katerih kršitev tvori deviantnost, in z uporabo teh pravil na posameznih ljudeh in z njihovim etiketiranjem kot outsiderjev. S tega stališča deviantnost ni lastnost dejanja, ki ga oseba stori, temveč bolj posledica uporabe pravil in sankcij na prestopniku s strani ostalih. Deviantna oseba je nekdo, ki mu je bila etiketa uspešno prilepljena; deviantno vedenje pa je vedenje, ki ga ljudje tako etiketirajo« (Becker, 1963: 9). »Neko dejanje postane deviantno takrat, ko ga drugi posamezniki kot takega zaznavajo in označijo«. (Haralambos in Holborn, 1999: 413)

Becker je proučeval tudi možne posledice na posameznika, ki je javno etiketiran kot deviantna oseba. Če so posamezniki etiketirani kot kriminalci, jih drugi vidijo in se nanje odzivajo z vidika etikete ter praviloma predpostavljajo, da imajo negativne značilnosti, ki so normalno povezane s takšnimi etiketami. Ker posameznikovo pojmovanje samega sebe v glavnem izvira iz odzivov drugih nanj, pa tudi posameznik sam sebe pojmuje z vidika etikete, kar lahko povzroči *samoizpolnjujočo prerokbo*, zaradi česar postane deviantna identifikacija usmerjevalna (Becker, 1963: 25–34).

Možne stopnje v procesu etiketiranja pa so naslednje (Becker, 1963: 34–38):

- na začetku je posameznik javno etiketiran kot devianten, kar lahko vodi k temu, da ga mnoge družbene skupine pa tudi prijatelji in družina zavračajo, zaradi česar je prisiljen zapustiti svoje dosedanje bivalno okolje;
- slednje pa lahko spodbudi nadaljnjo deviantnost (poštene delodajalci jim lahko odklonijo službo);
- tudi uradni postopki do deviantnosti imajo lahko podobne posledice, in sicer »postopek do deviantnih oseb jim odreka običajna sredstva za nadaljevanje vsakodnevnega življenja, ki so dostopna večini ljudi. Ker ji to odrekajo, mora deviantna oseba nujno razviti nezakonite postopke«;
- deviantna kariera je popolna, ko se kot deviantje etiketirani posamezniki pridružijo organizirani deviantni skupini. Slednje pa kaže na dejstvo, da posamezniki potrdijo in sprejmejo svojo deviantno identiteto;

- znotraj te skupine pa se razvije deviantna subkultura, ki pogosto vključuje prepričanja in vrednote, ki racionalizirajo, opravičujejo in podpirajo deviantne identitete in delovanja.

Becker poudarja tudi pomembnost javne identifikacije deviantnosti z domnevo, da lahko etiketa deviantnosti vodi v nadaljnjo deviantnost, kar lahko celo spremeni posameznikovo pojmovanje jaza tako, da ima že od začetka samega sebe za deviantno osebo. Pripisana etiketa lahko torej na posameznika že od samega začetka deluje usmerjevalno (Becker, 1963: 31–32).

Becker poudarja tudi pomembnost subjektivnih pomenov, ki so pripisani izkušnjam. Posameznik namreč v interakciji z drugimi interpretira fizične izkušnje, ki so posledica deviantnega dejanja, npr. jemanja drog¹ (Becker, 1963: 31–32).

c) Marksistični in neomarksistični pogled

Z markstističnega vidika oblikuje zakone država, ki predstavlja interese vladajočega razreda. Chambliss trdi, da je »bistvo kapitalističnega ekonomskega sistema zaščita zasebne lastnine, ki je po definiciji temeljni kamen, na katerem funkcionirajo kapitalistične ekonomije. Torej ni presenetljivo ugotoviti, da kazenski zakoni odražajo to skrb« (Haralambos in Holborn, 1999: 422).

Marksisti trdijo, da je kriminaliteta naraven »izrastek« kapitalistične družbe, generira pa jo kapitalistični ekonomski sistem iz naslednjih razlogov (Haralambos in Holborn, 1999: 426):

- »ekonomska baza pomembno vpliva na družbene odnose, verovanja in vrednote, kapitalistični način proizvodnje pa poudarja maksimiziranje profitov in akumulacijo kapitala;
- vedenje motivira ekonomski interes, ne pa dolžnost do javnega interesa;

¹ Becker je izvedel svojo raziskavo na kadilcih marihuane.

- kapitalizem temelji na zasebni lastnini, spodbuja osebno korist, ne pa kolektivnega blagostanja;
- kapitalizem je tekmovalni sistem, ne spodbuja vzajemne pomoči in sodelovanja za dobrobit vseh, temveč podpira posameznikov uspeh na račun drugih«.

Chambliss prav tako trdi, da so pohlep, sebičnost in sovraštvo, ki jih generira kapitalistični sistem, motiv za kazniva dejanja na vseh nivojih družbe, in sicer pripadniki vseh slojev uporabljajo vsa sredstva in možnosti, ki jim jih daje njihov razredni položaj, da storijo kaznivo dejanje (Haralambos in Holborn, 1999: 426). »Tako v revnih četrtih nasilnež, majhen lopov, preprodajalec trdih drog, zvodnik in prostitutka uporabljajo to, kar imajo, da dobijo to, kar lahko. Ljudje z visokimi prihodki, poslovneži, pravniki in politiki pa imajo na razpolago bolj učinkovita sredstva, da si prigrabijo večji kos torte«. (Haralambos in Holborn, 1999: 426)

Tudi neomarksistični sociologi se strinjajo, da so za družbo značilne skupine, med katerimi obstaja tekmovanje in konflikti v interesih, vendar pa se od svojih marksističnih predhodnikov razlikujejo v dejstvu, da nihče med njimi ne misli, da obstaja preprost in jasen odnos med ekonomsko bazo družbe in deviantnostjo. Tako Taylor, Walton in Young trdijo, da se kriminalci sami odločijo za kršitev zakona, in ne kot je trdil Marx, da kriminalca v kriminaliteto potiska revščina, v katero kapitalizem sili določene skupine prebivalcev. Neomarksisti posameznikovo odločitev za kaznivo dejanje pojmujejo kot »smiselen poskus akterja, da bi oblikoval in razvil lastno pojmovanje samega sebe«. Poudarjajo, da so kazniva dejanja pogosto premišljena in zavestna dejanja s političnimi motivi (Haralambos in Holborn, 1999: 427–428). Na podoben način gleda na kriminaliteto tudi Gilroy (proučeval je odnos med raso in kriminaliteto), ki trdi, da so kazniva dejanja, ki jih storijo etične manjšine, pogosto zavestna in premišljena politična dejanja (v Haralambos in Holborn, 1999: 429).

2.1.4 Ekonomske teorije deviantnosti

V tem poglavju opisujem *teorijo racionalne izbire* nekoliko podrobneje v primerjavi z ostalimi predhodno orisanimi teorijami deviantnosti, saj omenjena teorija najbolje označuje vrsto deviantnih dejanj, ki so predmet moje analize.

Z ekonomske perspektive je kriminal oblika racionalnega delovanja oziroma odločitvena izbira, ki jo izberejo posamezniki, ko se odločajo, kako najbolje porabiti svoj čas. Pri oblikovanju izbire pa posamezniki tehtajo koristi in stroške v primerih uporabe njihovega časa v različnih situacijah:

- v primeru legalnega delovanja;
- v primeru ilegalnega delovanja;
- v primeru nedelovanja (Fadaei – Tehrani in Green, 2002: 781–782).

Jeremy Bentham – predstavnik klasične šole kriminologije – je razvil koncept »**hedonističnih kalkulacij**«, v sklopu katerega naj bi posamezniki tehtali potencialne užitke in na drugi strani bolečine, povezane z njihovim vedenjem, ter se na podlagi tega odločali za odločeno obliko vedenja (Geis, Jones in Taylor v Fadaei – Tehrani in Green, 2002: 782).

Podobno sliko deviantnega vedenja pa je orisala tudi **teorija racionalne izbire**, ki pravi, da prestopniki izberejo deviantno pot na podlagi »izračuna« tveganja in nagrad v primeru posameznega delovanja (Cornish in drugi v Fadaei – Tehrani in Green, 2002: 782). Ta teorija torej predpostavlja, da lahko deviantnost razumemo kot dejstvo, da posamezniki izberejo nelegalno delovanje za dosego svojih ciljev po enakem principu tehtanja stroškov in koristi, kakor tudi tehtajo stroške in koristi, kadar izberejo legalno delovanje. Na odločitev za deviantno delovanje vplivajo posameznikove preference, njegov odnos do rizika in časovne dostopnosti, prav tako pa tudi njegova ocena ilegalne priložnosti, stroškov in možnosti za samo realizacijo dejanja, v nasprotju z legitimno dostopnostjo, stroški in možnosti za realizacijo istega cilja (McCarthy, 2002: 422).

Teorija racionalne izbire predvideva, da imajo lahko posamezniki v različnih pogojih (v času in prostoru) različne spodbude za deviantno delovanje. Na primer posamezniki živeči v revnih četrtih so bolj nagnjeni k deviantnemu delovanju, prav tako pa je stopnja deviantnega delovanja višja v obdobju recesije kakor v obdobju gospodarske rasti (Jeong-Yoo in Gang, 2001: 500–501).

McCarthy v svojem pristopu k teoriji racionalne izbire temelji na delih ekonomistov in tudi na delih politologov in sociologov, in sicer pravi, da (McCarthy, 2002: 418-421):

- posamezniki težijo k določenim rezultatom, kot so premoženje, delo, preživetje;
- težnje posameznikov so celostne, tranzitivne in nespremenljive.

Celostnost tu pomeni, da lahko posamezniki naročijo vse možne kombinacije vseh možnih rezultatov od najbolj do najmanj zaželenega. Nekateri izmed teh rezultatov so neznani, spet drugi pa so z ostalimi neprimerljivi; vendar pa se celostnost ponavadi nanaša na točno določene rezultate, ne pa na vse možne rezultate.

Tranzitivnost in nespremenljivost pa težnjam določata koherenco in konsistenco. Tranzitivnost zahteva od posameznika v primeru, da preferira X pred Y in Y pred Z, potem preferira tudi X pred Z. Domneva o nespremenljivosti teženj oziroma preferenc posameznikov pa na eni strani pomeni, da morajo biti preference posameznikov eksogene in nespremenljive, s čimer se izključuje možnost, da na njih vplivajo dogodki in okoliščine (Usher v McCarthy, 2002: 419), na drugi strani pa morajo biti preference konsistentne v postopku odločitve, pri čemer je dovoljeno, da se v času zaradi novih informacij tudi spreminjajo (Becker in Frank v McCarthy, 2002: 419).

- Na izbire oziroma preference posameznikov vpliva njihova orientacija k sedanjim rezultatom v nasprotju z rezultati v prihodnosti. Posamezniki imajo lahko:
 - pozitivne časovne preference posameznih rezultatov, vendar pa bodo potrebovali v prihodnosti večje kompenzacije, da se bodo lahko odrekli sedanjim koristim;
 - negativne časovne preference, če so se pripravljene odreči sedanjim koristim zaradi manjših koristi v prihodnosti;

- nevtralne časovne preference, če so pripravljeni trgovati s sedanjimi in bodočimi koristmi v razmerju ena proti ena.
- Večina rezultatov je negotovih, kar pomeni, da ni nobenih zagotovil, da bodo realizirani, rezultat česar je dejstvo, da posameznikov odnos do rizika in negotovosti vpliva na njihove preference. Pomembnost slednjega odnosa reflektira Von Neumann-Morgensternova »funkcija pričakovane koristnosti« (»expected utility function«). Slednja odraža tri pomembne značilnosti preferenc rezultatov:

Prvič – na posameznikove preference vplivajo potencialne koristi, ki jih bo posameznik imel od določenih rezultatov, sorazmerno s stroški, ki jih bo posameznik imel s tem rezultatom.

Drugič – ekonomisti prepoznavajo več tipov potencialnih stroškov in koristi, kot so priložnostni in zunanji stroški, izmed katerih je večina nedenarnih.

In tretjič – izračun pričakovane koristi za posamezno dejanje vsebuje množenje posameznikove koristi pri vsakem možnem rezultatu z verjetnostjo, da se le-ta pojavi v izbranem dejanju, čemer sledi povzemanje vseh možnih rezultatov.

- Ugotovitve posameznikov o stroških in njihove izbire temeljijo na informacijah, ki jih le-ti zberejo. Vendar pa že zbiranje teh informacij samo po sebi za posameznika predstavlja stroške. Čeprav želijo imeti posamezniki, ko so v procesu odločanja, vse dostopne informacije o določenem cilju, so njihove odločitve ponavadi sprejete s pomanjkljivimi informacijami. Posamezniki lahko verjamejo, da imajo zadostne informacije, pa vendar jih nimajo; poleg tega pa imajo posamezniki nepopoln spomin in pogosto napačno presodijo stroške in koristi. Prav tako pa zbrane informacije še ne pomenijo, da bodo posamezniki racionalno izbrali, saj informacije preprosto predstavljajo gole podatke, racionalno odločanje pa pomeni veliko več kot le to (Lupia in McCubbins v McCarthy, 2002: 420). Te slabosti lahko ogrožajo posameznikovo sposobnost izbiranja rezultatov, skladnih z njihovimi preferencami.

- Racionalno delovanje je tisto delovanje, ki je skladno z zgornjimi predpostavkami. Gre torej za tisto delovanje, ki maksimizira koristi, ki jih ima posameznik. Maksimizacija koristi pa zahteva izbiro vedenja skladno s pričakovano funkcijo koristi, četudi vedenje samo po sebi ni »a priori« označeno kot racionalno. Označba nekega vedenja kot racionalnega je odvisna od poznavanja domnev o

posameznikovih informacijah, vrstnem redu preferenc ter rizičnem pristopu in časovni dosegljivosti. Racionalne izbire posameznikov lahko rezultirajo v različnih oblikah vedenja, četudi so ujeti v isto situacijo.

Vedenja posameznikov so lahko razumljena kot racionalna le za člane neke skupine, kolektiva ali populacije ob predpostavki, da ima večina posameznikov te skupine isto pričakovano funkcijo koristnosti.

Razlikujemo med dvema meriloma racionalnosti, in sicer med (Becker v McCarthy, 2002: 421):

- *lastno-interesnim merilom* (»self-interest standard«), ki je povezano z neoklasično Čikaško šolo in definira racionalno delovanje kot vedenje, ki reflektira posameznikovo ocenjevanje stroškov in koristi, ki zadevajo direktno njih same. To pomeni, da posamezniki zasledujejo predvsem svoje lastne ekonomske interese.
- *in merilom sedanjostnih ciljev* (»present-aim standard«), pri katerem gre za naravo posameznikovih preferenc. Torej gre za racionalno delovanje kot tisto vedenje, ki reflektira ocenjevanje stroškov in koristi za katere koli cilje v trenutku odločitve, ter pravi, da je posameznikovo delovanje racionalno, če je skladno z vrstnim redom posameznikovih preferenc.

Zgodnji ekonomistični modeli deviantnosti so se naslanjali na »*lastno-interesno merilo*« racionalnosti in so predvidevali, da posamezniki izberejo deviantno vedenje, ko le-to maksimizira njihove lastne interese. Becker (v McCarthy, 2002: 422) pravi, da je pogostost deviantnih dejanj določena s tremi faktorji, in sicer:

- s stroški, povezanimi z aretacijo, verjetnostjo obsodbe, kaznijo ter izgubo dohodka v primeru legalnega delovanja;
- koristi denarnega in psihološkega dobička, pridobljenega z deviantnim dejanjem;
- skupek variabel, ki predstavljajo pripravljenost posameznika za deviantno delovanje.

Poleg zgornjih dejavnikov, ki vplivajo na posameznikovo odločitev za deviantno delovanje, pa je njegovo delovanje tudi rezultat njegove nizke samokontrole, pritiska,

etiketiranja in drugih družbenih izkušenj, ki jih ima posameznik (McCarthy, 2002: 423).

Becker in drugi ekonomisti, kot sta npr. Schmidt in White, so državne sankcije predstavljali kot najpomembnejši strošek med izbiro, poleg tega pa so predpostavljali, da naj bi državne kazni zmanjševale stopnjo deviantnosti. Vendar pa mnogi avtorji, ki so raziskovali omenjeno hipotezo, ugotavljajo negativno povezavo med državnimi sankcijami in stopnjo deviantnosti. Kasnejše raziskave v zvezi s tem pa so pokazale svarilen učinek (»deterrence effect«) v povezavi med državnimi sankcijami in stopnjo deviantnosti za posamezna, ne pa za vsa deviantna dejanja (npr. Levitt, Lochner in Spelman v McCarthey, 2002: 425).

Teorija racionalne izbire tudi pravi, da denarni stroški, kot so npr. izguba legalnega dohodka v primeru deviantnega delovanja, prav tako vplivajo na posameznikovo odločitev za deviantno delovanje. Raziskave učinka zaposlenosti na dohodek, pridobljen z deviantnim delovanjem, so predvidevale, da se stroški deviantnega delovanja večajo z višino legalnega dohodka. Grogger (v McCarthey, 2002: 426) je odkril močno negativno povezanost legalnega dohodka na aretacijo in pozitivno povezanost med legalnim dohodkom in časom brezposelnosti. V modelih, ki jih je ocenjeval, je bila odločitev za delo neodvisna od odločitve za deviantno delovanje. Ugotovil je, da je znižanje plače vzpodbudilo posameznike k deviantnemu delovanju ter da je upadanje plač v 70-ih in 80-ih letih znatno prispevalo k povečanju deviantnega delovanja med mladimi. Pezzinova (v McCarthey, 2002: 426) je v svoji raziskavi ugotovila, da se odstotek deviantov, ki bodo prenehali z deviantnim delovanjem, povečuje z legalnim dohodkom in zmanjšuje z nelegalnim. Podobno sta Uggen in Thompson (v McCarthey, 2002: 426) ugotovila, da legalna zaposlitev zmanjšuje število povratnikov k deviantnim dejanjem. Vzorec prestopnikov, odvisnikov in mladoletnih prestopnikov sta spremljala v triletnem obdobju ter ugotovila, da sta zaposlitev in legalni dohodek negativno vplivala na nelegalne dohodke (zaposlitev posameznikov je zmanjšala nelegalne dohodke med 100 in 200 dolarji mesečno, prav tako pa je vsak prisluženi legalni dolar zmanjšal ilegalne dohodke za približno sedem centov).

Sociologi pa so prispevali še nekoliko več k ekonomskemu pristopu k deviantnosti. Predpostavljali so, da stroški vključujejo tudi stigmo in zavračanje s strani pomembnih drugih, ki spremljata državne sankcije, prav tako kot lahko kršenje norm povzroči krivdo in sramovanje s strani kršitelja (Graqsmick, Bursik in Paternoster v McCarthy, 2002: 426).

Nekatere raziskave ugotavljajo, da ima zaznavanje družbenih in državnih sankcij največji vpliv na posameznike, kar pomeni, da posamezniki internalizirajo norme, ki prepovedujejo deviantna dejanja, saj so vtikani v omrežja posameznikov, ki spoštujejo zakone večino svojega časa in katerih deviantne izkušnje so omejene na majhno število navadnih malenkostnih prekrškov (Stafford in Warr v McCarthy, 2002: 427). To pomeni, da ima lahko zaznavanje sankcij velikanski vpliv na tistih nekaj posameznikov, ki imajo motive ali priložnosti, da delujejo deviantno. Nasprotno pa Piliavin (v McCarthy, 2002: 427) ugotavlja, da ima ocena verjetnosti formalnih in neformalnih sankcij majhen vpliv na odločanje za deviantno delovanje. V raziskavi med mestnimi mladoletniki pa Foglia (v McCarthy, 2002: 427) ugotavlja, da zaznavanje verjetnosti za legalne sankcije in negativne reakcije prijateljev ne vplivajo na udeležbo v deviantnih dejanjih. Raziskave s področja odločanja za deviantno delovanje torej na eni strani ugotavljajo, da zaznavanje družbenih in državnih sankcij s strani posameznika vpliva na njegovo odločanje o deviantnem delovanju, na drugi strani pa so bile opravljene raziskave, ki temu nasprotujejo in ugotavljajo, da zaznavanje družbenih in državnih sankcij s strani posameznika nima pomembnega vpliva na njegovo odločanje za deviantno delovanje. To pa pomeni, da ne moremo trditi, da zaznavanje družbenih in državnih sankcij s strani posameznika pomembno vpliva na njegovo odločanje za ali proti deviantnemu delovanju.

Večina posameznikov torej internalizira pravne norme družbe, v kateri živijo. To pomeni, da večina posameznikov te norme tudi spoštuje in se izogiba deviantnim dejanjem. Pa vendar raziskave kažejo, da so med tistimi posamezniki, ki so internalizirali pravne norme, tudi takšni, ki pravnega reda ne spoštujejo. Internalizacija pravnih norm s strani posameznika in zaznavanje pravnih sankcij, ki jih družbena ureditev, v kateri živijo, nalaga za storilce deviantnih dejanj, delovanje večine posameznikov umeščata v meje legalnega. Vendar pa prav te sankcije na nekatere posameznike ne vplivajo na način, na kakršnega delujejo na večino pripadnikov neke

družbe – torej zaviralno v smislu storitve deviantnega dejanja – ampak jih spodbudijo k deviantnemu delovanju. Ker hujše pravne sankcije pogosto pomenijo manjšo možnost odkritja deviantnega dejanja, nekateri posamezniki tehtajo med možnimi stroški in koristmi ter verjetnostjo za aretacijo in v primeru pozitivnega izračuna oziroma pozitivnih koristi za njih same delujejo deviantno. Posameznikovo zaznavanje pravnih norm torej ne deluje na posameznika vedno v pozitivnem smislu, torej na način, da te norme spoštuje, ampak na nekatere posameznike, ki imajo motive ali priložnosti za deviantno delovanje, deluje tudi v negativnem smislu, da dejansko delujejo deviantno.

3 DEVIANTNOST V KIBERNETSKEM PROSTORU

Kibernetski prostor oziroma »cyberspace« je »virtualno, omrežno, elektronsko posredovani interesni prostor, skratka prizorišče za zagotavljanje različnih formalnih in neformalnih interesnih nagnjenj in potreb akterjev, ki poteka z interakcijo in transakcijo med akterji« (Trček, 2003: 13).

Kibernetski prostor je po Kitchinu sestavljen iz treh komponent, in sicer interneta, intraneta ter navidezne resničnosti (Kitchin, 1998: 2). »Lahko je del širšega okolja virtualne resničnosti, ki pa ni izključno pogojen s tehnologijo virtualne resničnosti. Za vstop v tako razumljen kibernetski prostor ne potrebujemo posebnih podatkovnih rokavic in simulacijskih čelad. Proučevanje kibernetskega prostora se ne osredotoča na njegovo tehnično strukturo, temveč na aktivnosti posameznih uporabnikov, ki vanj vstopajo. Dogajanja v tem prostoru niso navidezna, pač pa povsem realna. Lahko so fantazijska, nikakor pa niso neodvisna od akterjev, ki se v ta prostor iz takšnih ali drugačnih razlogov podajo«. (Oblak, 2000: 1057)

Poleg tradicionalnih oblik deviantnega vedenja, ki ga poznamo v fizičnem svetu (npr. ropi, umori, različne goljufije ipd.), se je domot deviantnega vedenja razširil tudi na območje kibernetskega prostora, kjer so te že omenjene tradicionalne oblike deviantnosti prevzele nove in naprednejše oblike, ki jih je v primerjavi s tradicionalnimi oblikami kriminala, storjenimi v fizičnem svetu, veliko težje odkriti.

Izmed vseh teorij, ki se ukvarjajo s pojmom deviantnosti z vidika kibernetnega kriminala, le-tega najbolj opisuje teorija racionalne izbire in pa Banthamov koncept »hedonističnih kalkulacij«, ki (kot sem omenila v poglavju o ekonomskih teorijah deviantnosti) poudarjata, da smo ljudje kalkulativna bitja. Torej vsak posameznik sam izračuna, kaj se mu najbolj izplača, in na podlagi teh izračunov nekateri posamezniki pridejo do ugotovitve, da se jim bolj izplača priti do želenega cilja po deviantni poti. Posameznik si torej sam racionalno izbira pot. Preverja stroške investicije ter dobiček. Ko nekateri posamezniki ugotovijo, da se investicija bolj izplača, če uporabijo deviantno pot, in da je dobiček večji na deviantni poti, se zato odločijo zanjo. Podobno se dogaja tudi v kibernetnem prostoru v primeru deviantnega vedenja posameznikov. Kalkulacija investicije in tveganja je predvsem zaradi pomanjkanja strukture pravil in sankcij v primeru deviantnosti v kibernetnem prostoru majhna, dobički pa so lahko enormi, kar posameznike prepriča v to, da delujejo deviantno ter ta deviantna dejanja tudi tolerirajo.

Ranljivost današnje informacijske družbe z vidika kibernetnega kriminala še vedno ni zadostno regulirana: gospodarstvo, administracija in celotna družba temeljijo na visoki stopnji učinkovitosti in varnosti modernih informacijskih tehnologij. V gospodarski skupnosti je večina denarnih transakcij izvršenih preko računalniških sistemov, elektronsko poslovanje pa je odvisno od varnosti sistemov denarnih transakcij in računalniških omrežij. Mnoga podjetja hranijo svoje največje skrivnosti v elektronskih bazah podatkov. Računalniki in internet pa igrajo tudi vedno večjo vlogo v izobraževanju in življenju mladih. Mednarodne računalniške mreže so živčna jedra gospodarstva, javnega sektorja in družbe, zato je varnost oziroma varovanje teh računalniških in komunikacijskih sistemov izrednega pomena (Sieber, 1998: 3).

Švedsko nacionalno ministrstvo za preiskovanje kriminala je leta 1998 ugotavljalo, da se z večanjem števila uporabnikov interneta večja tudi uporaba interneta za kriminalna dejanja. Ugotavljali so, da se je močno povečala uporaba interneta in drugih informacijskih tehnologij v kriminalnih dejanjih. Prav tako pa FBI ugotavlja, da predstavlja kibernetni kriminal v 21. stoletju temeljni izziv organom pregona, saj brezmejnost (»borderless«) kibernetnega prostora ponuja anonimnost in različne metode prekrivanja, poleg tega pa ponuja nova orodja za kriminalna dejanja (Armstrong in Forde, 2003: 209).

Kibernetski kriminal je postal velikanska grožnja današnji informacijski družbi. Razširjanje informacijske tehnologije v skoraj vse sfere življenja in povezovanje računalnikov v mednarodne računalniške mreže dela kibernetski kriminal vedno bolj raznovrstnejši, nevarnejši in mednarodno prisoten. Analiza relevantnih kriminogenih faktorjev kaže specifične karakteristike modernih računalniških in komunikacijskih omrežij, ki so v veliko pomoč vsiljivcem; potencialnim žrtvam in organom pregona pa pomenijo težave. Skupine, ki so vpletene v organizirani kriminal, gospodarski vohuni in tajne službe po svetu izkoriščajo nove oblike kibernetskega kriminala, na žalost pa se mnoge vladne, gospodarske in privatne organizacije ter uporabniki ne zavedajo napadov, ki se jim zgodijo v kibernetskem prostoru (Sieber, 1998: 3–4).

S pojavom interneta so se torej pojavile tudi nove oblike zlorab, za mnoge od njih pa dejansko povzročena škoda še ni znana, prav tako pa še niso znane poti za njihovo zatiranje. Med te oblike zlorab štejemo tudi t.i. črne kopije, pri katerih gre za neupravičeno razmnoževanje računalniških programov za lastno uporabo, in piratstvo, pri katerem gre za okoriščanje z nezakonito razmnoženimi računalniškimi programi. Obe omenjeni zlorabi predstavljata nezakonito izkoriščanje avtorskih del in imata posebej škodljive posledice za založnike programske opreme in končne uporabnike (Zupančič, 1997: 182).

Internet spreminja definicijo skupnosti in briše zemljepisne meje, spodkopava navade, pravila in zakone obnašanja ter ravnanja. S pravnega, zakonodajnega in policijskega vidika sta nevarni predvsem globalnost in univerzalnost interneta. Geografsko internet presega meje posameznih držav ter ne ločuje različnih vrednostnih sistemov in prepričanj, iz česar izhajajo naslednje pravne dileme in problemi (Zupančič, 1997: 186–187):

- »nepravosodnost interneta«;

»Internet kot tudi druga omrežja ne predstavlja otipljivega fizičnega objekta, ampak predstavlja skupek omrežnih protokolov, ki omogočajo prenos informacij po številnih posameznih mrežah. Z internetom se zato srečujejo mnoge mednarodne sodne oblasti, saj neko sporočilo lahko potuje kjerkoli v globalni mreži in je v kateri koli državi na vpogled kateremu koli uporabniku, ki je nanjo

priključen. Internet tako obstaja v okviru »več-pravosodnega sistema«, vendar pa je funkcionalno »nepravosoden«, saj ga ni mogoče fizično locirati ali omejiti«. (Zupančič, 1997: 186)

- »neoprijemljivost interneta«;

Fizično neoprijemljiv prostor je težko nadzorovati in še težje izvajati sankcije za morebitne kršitelje. Za komuniciranje v tem omrežju so na nek način odgovorne tudi družbene institucije, tako nevladne kot tudi vladne. Merila o tem, kaj pošiljati po kibernetnem prostoru, določa posameznik sam, na njegove odločitve pa lahko vplivajo predvsem splošne družbene norme in posameznikova osebna etika. Strokovnjaki in uporabniki interneta ugotavljajo, da je zakone težko postavljati v prostoru, ki je istočasno »povsod in nikjer«, da je težko varovati osebno lastnino, ki nima fizične oblike in jo je mogoče množično kopirati in poljubno reproducirati (Zupančič, 1997: 186). Posameznik v kibernetnem prostoru torej deluje na podlagi svoje lastne presoje o tem, kaj je prav in kaj ni.

- relativnost vrednot v kibernetnem prostoru;
- odgovornost sistemskih operaterjev;
- računalniški policisti;
- kazenski pregon.

3.1 Zgodovinski razvoj pojma kibernetne kriminalitete

Korenine pojma računalniški kriminal segajo v leto 1960, ko so bili v javnem tisku in strokovni literaturi objavljeni prvi članki o t.i. računalniškem kriminalu. Primarno so ti primeri vključevali računalniško manipulacijo, računalniško sabotažo, računalniško »špijonažo« oziroma vohunstvo in nelegalno uporabo računalniških sistemov. V sredini 70-ih let so bile o računalniškem kriminalu narejene prve empirične raziskave, ki so se sklicevale na znanstveno-kriminološke preiskave. Pogled javnosti in znanosti nanj pa se je drastično spremenil v 80-ih letih, ko so v tisku objavil osupljive primere o hekerjih, računalniških virusih in črvih. Ranljivost informacijske družbe je širši

javnosti razkril val programskega piratstva, manipulacij delitve denarja in zlorabe telekomunikacijskih sredstev (Seiber, 1998: 19–20).

Zaradi vedno novih in novih oblik računalniškega kriminala se je pojavila potreba po definiciji slednjega. Tako je že leta 1983 skupina strokovnjakov OECD² definirala termin »računalniški kriminal« (ali »kriminal v zvezi z računalniki«) kot »vsako ilegalno, neetično ali neavtorizirano vedenje, ki zajema avtomatsko obdelavo podatkov in/ali prenos podatkov« (Seiber, 1998: 20–21). Kasnejše razlage pojma pa so šle še dlje, z razvojem obsežnejšega pojma »podatkovni in/ali informacijski kriminal« (Seiber, 1998: 21).

3.1.1 Opredelitve pojma

Čeprav je večina razlag pojma kibernetске kriminalitete oziroma kriminalitete povezane z računalniki dokaj splošnih, pa je verjetno prav v njihovi splošnosti moč najti širok spekter kriminalnih dejanj, ki jih ta pojem obsega. Tako David Wall v svoji konceptualizaciji *kibernetске kriminalitete* (»*cybercrime-a*«) pravi, da je to pojem, ki obsega škodljivo vedenje, ki je na nek način povezano z računalnikom (Wall, 2001: 2). Armstrong in Forde pa za kibernetски kriminal pravita, da je to »kriminal, ki je zagrešen s pomočjo interneta« (Armstrong in Forde, 2003: 209). Grabosky in Smith definirata kibernetско kriminaliteto kot t.i. *digitalni kriminal*, to pa je kriminal, ki obsega informacijske sisteme kot sredstva ali tarče nezakonitega delovanja (Wall, 2001: 29).

Nekoliko bolj natančno je ta pojem definiral Brvar, ki je *kriminaliteto v zvezi z računalniki* definiral »kot kazniva dejanja, v katerih računalnik nastopa kot sredstvo (orodje), predmet ali objekt napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje iz računalništva in informatike« (v Martonoši, 1993: 498). Na tem mestu velja poudariti, da so v zahodnem svetu dolga leta uporabljali pojem računalniška kriminaliteta in ne pojma kriminaliteta v zvezi z računalniki. To namreč poudarjam zato, ker je prvi pojem v kriminološki in kazenskopravni tipologiji

² Organisation for Economic Co-operation and Development (Organizacija za ekonomsko sodelovanje in razvoj)

sporen, saj kriminaliteto klasificira glede na uporabljeno sredstvo in ne glede na to, da je računalnik le orodje v človeških rokah.

Obstajajo torej različne definicije kriminala, storjenega v kibernetnem prostoru. Nekateri (npr. Brvar) mu pravijo kriminal v zvezi z računalniki, spet drugi digitalni in informacijski kriminal (npr. Grabosky in Smith), nenazadnje pa se je splošno uveljavil pojem *kibernetška kriminaliteta* (»cybercrime«). Za slednjega Littlejohn Shinder (2002: 5) pravi, da je podkategorija računalniškega kriminala in se nanaša na kriminalna dejanja, storjena s pomočjo uporabe interneta ali kakega drugega računalniškega omrežja. Računalniki in računalniška omrežja so lahko uporabljeni za kriminalna dejanja na različne načine. Računalnik ali računalniško omrežje je lahko (Littlejohn Shinder, 2002: 5):

- orodje za izvedbo kriminalnega dejanja,
- tarča kriminalnega dejanja (torej žrtev kriminala),
- uporabljeno kot vmesnik v povezavi s kriminalnim dejanjem (npr. za shranjevanje ilegalnih vsebin ali prodajo ilegalnih drog).

V nadaljevanju naloge bom uporabljala pojem kibernetška kriminalitea. Na tem mestu pa velja poudariti, da je kibernetška kriminaliteta le ena izmed oblik deviantnega vedenja.

3.2 Kdo so kibernetški »kriminalci« in kdo so žrtve?

3.2.1 Kibernetški prestopniki

Kibernetški prestopniki so pogosto mladi, pametni in precej osamljeni posamezniki, pripadniki srednjega razreda, ki imajo ustrezno strokovno znanje in so pogosto motivirani z različnimi denarnimi in nedenarnimi cilji (Wall, 2001: 9). Glede na to, da je spekter kriminalnih dejanj v kibernetnem prostoru širok, je širok tudi spekter tistih posameznikov, ki ta dejanja zagrešijo.

Prvi kibernetiski prestopniki, ki so jih imenovali *telefonski friki*, so vdrlji v telefonski sistem z namenom, da jim bi bilo omogočeno medkrajevno klicanje, ne da bi bilo treba zanj plačati. Poleg telefonskih frikov pa so se pojavili tudi drugi kibernetiski prestopniki, in sicer *krekerji* («crackers») – to so posamezniki, ki razbijajo («crackajo») zavarovane informacijsko-komunikacijske sisteme. Dandanes se pojem kreker povezuje s posamezniki, ki so specializirani za razbijanje gesel (Littlejohn Shnider, 2002: 53). Na spletu je dostopnih mnogo informacij o »frikanju« (»phreaking«), vključno z natančnimi navodili za bodoče frike. Takšno vedenje telefonskih frikov pa je predstavljalo osnovo kasnejši hekerski subkulturi (Littlejohn Shnider, 2002: 55).

Med storilci kaznivih dejanj, ki nepooblaščno vdirajo v informacijsko-komunikacijske sisteme, torej ločimo *hekerje*, *kerekerje* in *telefonske frike*. *Hekerji* so »posamezniki, ki uživajo v raziskovanju programov; ki sami navdušeno, obsedeno programirajo in spoštujejo lastna etična pravila; ki pravijo, da naj bo dostop do računalnikov mogoč vsakomur; da morajo biti informacije svobodno dostopne; da nam računalniki izboljšujejo življenje in da oblasti (politiki, vojski in pravosodju) ne gre zaupati« (Zupančič, 1997: 182). *Krekerji* so posamezniki, ki »vdirajo in razbijajo («krekajo») zavarovane računalniške sisteme« (Zupančič, 1997: 182), *telefonski friki* pa so »umetniki vdiranja v telefonska omrežja« (Zupančič, 1997: 182). Young nadalje med hekerji in krekerji loči še (Wall, 2001: 4):

- *utopiste*³, ki naivno mislijo, da prispevajo k družbi z dokazovanjem njenih ranljivih mest;
- *kibernetiske pankerje*, ki so agresivno anti-ustanovni in namerno povzročajo škodo na stvareh, ki jih žalijo;
- *kibernetiske vohune*;
- *kibernetiske teroriste* – meja med slednjima je pogosto zabrisana, saj morajo biti po definiciji oboji izkušeni krekerji, da lahko dostopajo do različni spletnih mest.

Poleg teh najdemo med kibernetiskimi kriminalci še različne lovce na informacije, pirate in pa kriminalce, ki se dogovarjajo za kriminalne posle.

³ Ob vdoru v določen računalniški sistem ne naredijo ničesar, kar bi lahko onemogočilo sistem.

Primarna vloga hekerjev je temeljila na njihovem etičnem kodeksu, ki pravi, da »mora biti vsakršen dostop do računalnikov in vsega, kar bi jih lahko naučilo nekaj o tem, kako svet deluje, neomejen in skupen vsem« (Wall, 2001: 60). Torej z vidika primarne vloge hekerjev vdori v računalniške sisteme in podobna dejanja (npr. »spam«) pomagajo družbi, da odkrije svoje ranljive dele (hekerji v svoji primarni vlogi namreč v sistem le vdirajo in ne naredijo ničesar, kar bi lahko onemogočilo sistem). Prav tako se s podatki, ki jih morda vsebuje baza, v katero so vdrl, ne okoriščajo. To nadalje družbi omogoča boljšo zaščito pred novimi podobnimi dejanji (vdori ipd.), ki bodo morda zlonamerni (Wall, 2001: 60).

Hekerji uporabljajo internet za komuniciranje ter napade na različne sisteme na globalni ravni. Njihova filozofija je jasno dokumentirana, saj hekerji pravijo, da morajo biti informacije brezplačne, dostop do računalnikov in informacij pa naj bo neomejen. Hekerji delujejo v skupinah, izmed katerih so nekatere omejene le na hekersko elito, medtem ko so druge skupine medse pripravljene sprejeti še neizkušene posameznike z namenom, da jih izučijo. Mnogi hekerji so mentorji drugim hekerjem, še posebej tistim, ki mnogo obetajo, so entuzijastični ter imajo podobne vrednote. Hekerji si medsebojno delijo in izmenjujejo svoja orodja in informacije, vključno z metodami, kako se izogniti odkritju. Motivirani so s strani različnih dejavnikov, med katerimi so npr. vznemirjenost delovati ilegalno, izziv, užitek, znanje, priznanje, moč in prijateljstvo. Poleg že naštetih motivacijskih dejavnikov pa so tu še samozadovoljitev, odvisnost, vohunstvo, tatvina, dobiček, maščevanje, sabotaza in svoboda. Uporabljajo internetne pripomočke, vključno z internetnimi stranmi, spletnimi naslovi, »chat« sobami, FTP stranmi, »usenet« skupinami in forumi. Njihova programska orodja so shranjena na zasebnih in javnih internetnih straneh ter zavarovanih sistemih. Te spletne strani so visoko zavarovane, dostop do njih pa imajo le tisti posamezniki, ki so vredni zaupanja. Tako kot ostale kriminalne združbe tudi hekerji zavarujejo svoje komunikacijske kanale s sofisticiranimi enkripcijskimi orodji. Svojo anonimnost zagotavljajo z uporabo psevdonimov, anonimnih strežnikov in spletnih naslovov ter IP prevarami (kar pomeni, da svoj IP spremenijo, da izgleda, kot da prihajajo stvari z nekega drugega vira) (Armstrong in Forde, 2003: 211).

3.2.2 Žrtve kibernetkega kriminala

Pogosto nastajajo zmešnjave o tem, kdo so žrtve kibernetkega kriminala in kako posamezniki sploh postanejo žrtve. Potrebno je poudariti, da je lahko žrtev kibernetke kriminalitete vsak uporabnik interneta in računalnika. Med žrtvami kibernetkih kriminalcev so tako posamezniki kot tudi posamezne družbene skupine. V primerih kibernetkega zalezovanja in kraje kibernetkega denarja je viktimizacija najpogosteje osredotočena na posameznika. V primerih kibernetkega piratstva in kibernetkega vohunstva ali terorizma pa je viktimizacija ponavadi usmerjena proti korporacijam in družbenim skupinam (Wall, 2001: 8).

3.3 Vrste kaznivih dejanj v kibernetkem prostoru in odkrivanje kibernetkega kriminala

V kibernetkem prostoru ločimo štiri vrste kaznivih dejanj, in sicer (Konvencija o kibernetki kriminaliteti, 2002: 9–13):

1. kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov;
2. kazniva dejanja, povezana z računalnikom;
3. kazniva dejanja, povezana z vsebino;
4. kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic.

3.3.1 Kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov

a) Nedovoljen dostop do računalniških sistemov

V prvi fazi gre tu za vdore na daljavo z mikroračunalnikom ali modemom, običajno preko javne telekomunikacijske mreže v zavarovane informacijske in druge podatkovne sisteme različnih organizacij, z namenom, da bi pridobili računalniške podatke, ali pa s kakšnim drugim nepoštenim namenom (Konvencija o kibernetki kriminaliteti, 2002: 9). Tu gre tako za vdore v finančne organizacije, ki omogočajo

denarni prenos, kot tudi za vdore v različne državne organizacije ipd. (Zupančič, 1997: 183).

b) Onemogočanje in poškodovanje računalniških sistemov

V to kategorijo spadajo dejanja poškodovanja, izbrisa, poslabšanja, spreminjanja ali oviranja računalniških podatkov, s čimer je onemogočeno ali ovirano delovanje računalniškega sistema. Sem spadajo tudi različni napadi z računalniškimi virusi, zlorabe elektronske pošte (npr. onemogočanje komuniciranja preko elektronske pošte) ipd. (Konvencija o kibernetiski kriminaliteti, 2002: 9).

c) Izdelava in distribucija računalniških programov za storitev kaznivih dejanj

Gre za kazniva dejanja, ki obsegajo izdelavo, distribucijo naprav, računalniških programov, računalniških gesel in podobnih stvari z namenom onemogočanja in poškodovanja računalniških sistemov (Konvencija o kibernetiski kriminaliteti, 2002: 10).

3.3.2 Kazniva dejanja, povezana z računalnikom

V to kategorijo spadajo dejanja, s katerimi neka oseba ali skupina oseb naklepno povzroča premoženjsko škodo drugim osebam. Med slednje umeščamo tudi goljufije v zvezi z elektronsko trgovino. Vsak nakup ali uporaba drugih komercialnih storitev namreč v mreži pusti za seboj digitalne sledi in tako pri poslovanju s kreditnimi karticami obstaja veliko možnosti za njihovo zlorabo (Zupančič, 1997: 183). Poleg tega pa je velik delež dejanj, ki so povezana s trgom ukradenih komunikacijskih podpor. Stranke v teh dejanjih so tiste osebe, ki se izogibajo stroškom telefonskega klica ali iščejo popuste za te klice. Obstajajo pa tudi drugi, ki si prilastijo informacijska sredstva za upravljanje nezakonitih poslov, saj obstaja manjša verjetnost razkrinkanja. Sredstva za krajo telekomunikacijskih podpor so različna in obsegajo kloniranje mobilnih telefonov, ponarejanje telefonskih kartic ter tudi nepooblaščen vstop v organizacijsko telefonsko stikalno ploščo (»PBX«). Z dostopom do »PBX-a« si posamezniki ali kriminalne organizacije pridobijo dostop do obhoda »dail-in/dail-

out« ter tako opravljajo svoje klice ali pa klice prodajajo tretjim strankam (Grabosky in Smith v Wall, 2001: 30).

3.3.3 Kazniva dejanja, povezana z vsebino

Sem spada razširjanje otroške pornografije ter različne politične propagande skrajnežev, ki preko interneta širijo svoje propagandno gradivo. Tako »anarhistična kuhinja« spodbuja in napeljuje uporabnike k stanju družbenega kaosa ter posreduje navodila za izdelovanje nevarnih stvari in snovi (Zupančič, 1997: 183). Naslednja (in v zadnjem času zelo aktualna) tema političnih krogov je terorizem, ki je svoj domet razširil tudi v kibernetiski prostor. V primeru kibernetiskega terorizma gre za enkrat še bolj za spodbujanje k mednarodnemu terorizmu in terorističnim akcijam, v prihodnosti pa bo lahko že vse drugače, kajti prav terorizem predstavlja velikansko grožnjo informacijskim sistemom. Potem pa so tu še različni verski obračuni in rasne nestrpnosti, kjer posamezniki in skupine zlorablajo omrežje za širjenje svojih verskih in rasističnih prepričanj. Na internetu najdemo poleg že omenjenih dejanj tudi napeljevanja h kaznivim dejanjem in navodila za izvajanje le-teh, mogoče je najti tudi navodila, kako izdelati bombo, kako izvesti samomorilsko dejanje, napotke za gojenje marihuane ipd. (Zupančič, 1997: 183).

3.3.4 Kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic

Veliko informacij na mreži je namenjenih javni rabi. Zvok, slike, besedila, video ter multimedijske izdelke lahko prenesemo na svoj računalnik in jih poljubno uporabljamo, tu pa gre za novo obliko zlorabe intelektualne lastnine. Sem spada tudi nepooblaščen reprodukcija računalniških programov, torej kraja programske opreme (»software«) (Zupančič, 1997: 183).

3.3.5 Problematika odkrivanja kibernetiskega kriminala

Prvi problem, ki se pojavi v zvezi z raziskovanjem kibernetiskega kriminala, je ravnanje z računalniškimi sistemi in računalniško opremo. Gre namreč za to, da kompleksnost te vrste orodij laikom onemogoča spopadanje s to vrsto kriminala. Spopad pomeni predvsem veliko mero strokovnega znanja s področja računalništva in

informatike, potrebne pa so tudi druge psiho-analitične metode za odkrivanje kriminalcev, pri čemer gre na razne psihološke profile prestopnikov ipd. Prav zato je na tem področju najpomembnejše izobraževanje, predvsem v smeri uporabe določene računalniške opreme in računalniških programov ter védenje o tem, kako so oboji implementirani v informacijske sisteme. Pooblaščen osebe za boj proti kibernetickemu kriminalu pa morajo imeti tudi veliko mero iznajdljivosti; morajo biti bolj iznajdljive kot so kriminalci. Na žalost je pri nas pa tudi v svetu še vedno preveč pooblaščenih oseb za odkrivanje kibernetiskega kriminala, ki so računalniško nepismene in ki ne obvladajo niti osnovnih vprašanj, kot so identifikacija računalniške opreme, pravilen zaseg in uskladiščenje računalniške opreme. Zaradi tehnične narave te vrste kriminalitete so potrebne posebne policijske enote, specializirane za odkrivanje tovrstnih zlorab, t.i. kibernetiski policisti, potrebno pa je tudi tesno sodelovanje organov pregona z računalniškimi strokovnjaki (Vodušek, 1992: 116–117; Zupančič, 1997: 187).

Med zakonodajno oblastjo v različnih državah se pogosto pojavlja vprašanje, do kakšne mere lahko policija zakonito nadzoruje računalniška omrežja. Pogosto razumevanje večine držav je, da se lahko policisti vedejo tako, kot se vedejo navadni državljani, ko vstopajo v kibernetiski prostor, ter v njem raziskujejo in nato shranjujejo različne informacije, ki jih najdejo. V primeru, da policist sodeluje na internetu pod lažno identiteto samo z namenom zbiranja dokazov o kriminalnih aktivnostih, je take vrste aktivnost razumljena kot aktivnost pod krinko, katere pa naj bi se policisti lotili samo in izključno takrat, ko gre za prekršek obtoženega in drugih, ki je sorazmeren s pomembnostjo kriminalnega dejanja in verjetnostjo najdbe dokazov in storilca. Posebni problemi nastanejo, ko gre za trans-nacionalne policijske patrolje na internetu. Gre namreč za vprašanje, ali takšne aktivnosti kršijo suverenost vpletenih držav, saj se zakonodaja v zvezi s tem od države do države razlikuje, kar pomeni, da so raziskovalne prakse, ki so v eni državi ustaljene, v drugi glede na njihovo zakonodajo popolnoma nesprejemljive, pogosto gre namreč za kršenje varstva osebnih podatkov ipd. (Sieber, 1998: 104).

3.4 Zakonodaja v zvezi s kibernetško kriminaliteto

V Sloveniji področje kibernetške kriminalitete urejajo:

- Kazenski zakonik (Ur. l. RS, št. 95, 2004),
- Zakon o kazenskem postopku (Ur. l. RS, št. 96, 2004),
- Zakon o odgovornosti pravnih oseb za kazniva dejanja (Ur. l. RS, št. 98, 2004),
- Zakon o varstvu potrošnikov – 45. člen (regulira spam) (Ur. l. RS, št. 98, 2004),
- Zakon o avtorski in sorodnih pravicah (Ur. l. RS, št. 94, 2004);
- v določenem pogledu tudi Zakon o telekomunikacijah (Ur. l. RS, št. 30, 2001).

V spodnji tabeli so predstavljeni člani Kazenskega zakonika, ki neposredno ali posredno urejajo področje kibernetške kriminalitete:

Tabela 1: Člani, ki urejajo področje kibernetške kriminalitete, ter število kaznivih dejanj s področja kibernetške kriminalitete v letu 2002⁴

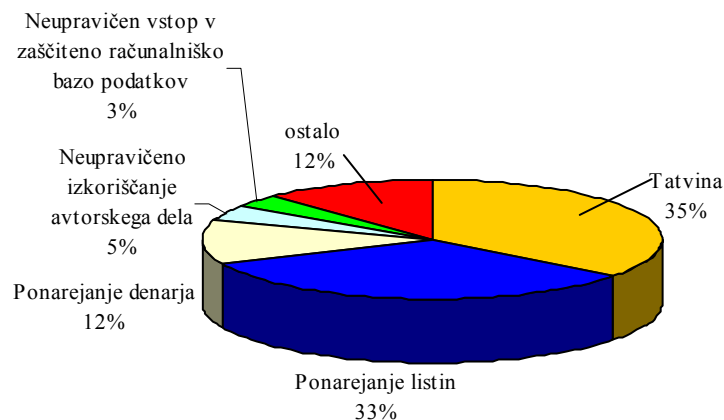
št. člena	Ime člena	Načini izvedbe dejanja	Št. kaznivih dejanj
148*	Neupravičeno prisluškovanje in zvočno snemanje	-	-
149*	Neupravičeno slikovno snemanje	-	-
150*	Kršitev tajnosti občil	-	-
151*	Nedovoljena objava zasebnih pisanj	-	-
154	Zloraba osebnih podatkov	Obdelava podatkov brez legalne podlage	1
158	Kršitev avtorske pravice	Sprememba/predelava programa	1
159	Neupravičena uporaba avtorskega dela	Piratstvo – »peka« CD-jev in prodaja	26
160*	Kršitev avtorski sorodnih pravic	-	-
187	Prikazovanje in izdelava pornografskega gradiva	Na internetu	1
211	Tatvina	Kraja telefonskih impulzov	200
212	Velika tatvina	Kraja telefonskih impulzov	8
217	Goljufija	Na internetu	10
225	Neupravičen vstop v informacijski sistem	Sprememba ali izbris	18
240	Ponaređitev ali uničenje poslovnih listin	Računalniško osnovane poslovne listine/dokumenti	4

⁴ Izpis vseh členov kazenskega zakonika, ki zadevajo področje kibernetške kriminalitete, je v prilogi

242	Vdor v informacijski sistem	Heking	7
249	Ponarejanje denarja	Uporaba računalnika kot orodja	66
250	Ponarejanje in uporaba ponarejenih vrednotnic ali vrednostnih papirjev	Uporaba računalnika kot orodja	15
256	Ponarejanje listin	Uporaba računalnika kot orodja	184
257	Posebni primeri ponarejanja listin	Uporaba računalnika kot orodja	2
260	Ponarejanje znamenj za zaznamovanje blaga, mer in uteži	Uporaba računalnika kot orodja	1
261	Zloraba uradnega položaja ali uradnih pravic	Uporaba računalnika kot orodja	16
265	Ponareditev ali uničenje uradne listine, knjige ali spisa	Računalniško osnovani uradni dokumenti	1
266	Izdaja uradne tajnosti	Uporaba računalnika kot orodja	1
309	Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje	Proizvodnja hekerskih orodij	1

Vir: Ministrstvo za informacijsko družbo

*Prenovljenji člani KZ (Ur. l. RS, št. 95, 2004)



Slika 1: Deleži kaznivih dejanj s področja kibernetike v letu 2002 (n=563)

V skrajno desnem stolpcu tabele 1 je navedeno število posameznih kaznivih dejanj s področja kibernetike v letu 2002. Izmed skupno 563 kaznivih dejanj na področju kibernetike je največ, in sicer 35.52 % tatvin, sledi ponarejanje listin (32.68 %), ponarejanje denarja (11.72 %), nepravilno izkoriščanje avtorskih del (4.62 %), nepravilni vstopi v zaščiteno računalniško bazo podatkov (3.20 %).

Ostalih posamičnih kaznivih dejanj s področja kibernetске kriminalitete je bilo v preteklem letu manj kot 3 %, skupaj pa 12.26 %.

3.4.1 Konvencija o kibernetски kriminaliteti

Pod okriljem Sveta Evrope je skupina strokovnjakov leta 1997 dobila nalogo oblikovati t.i. konvencijo o kibernetски kriminaliteti. Njen namen je bil določiti mednarodne pravne standarde v boju proti računalniški kriminaliteti. Skupina je s sodelovanjem držav opazovalk (ZDA, Kanada, Južnoafriška Republika in Japonska) sestavila prvi mednarodni pravni akt, ki obravnava sodobno kibernetско kriminaliteto. Sestavljena je z vidika priporočil državam podpisnicam, kako naj reformirajo svoje notranje pravo za boj proti računalniškemu kriminalu, in določa splošen okvir mednarodnega sodelovanja pri obravnavanju kibernetskega kriminala.

Konvencija o kibernetски kriminaliteti⁵ («Convention on Cybercrime») je mednarodna pogodba o boju zoper kriminal v kibernetskem prostoru in je bila sprejeta pod okriljem Sveta Evrope 23. 11. 2001 v Budimpešti, kjer jo je podpisalo 30 držav. Slovenija je konvencijo podpisala 24. 7. 2002, Državni zbor RS pa jo je sprejel 20. 5. 2004, v veljavo je stopila s 1. 1. 2005.

Glavni cilj konvencije je ustvariti skupno politiko, ki bo družbo ščitila pred kriminalom na svetovnem spletu, med drugim tudi s sprejetjem ustrezne zakonodaje in s spodbujanjem mednarodnega sodelovanja. Konvencija določa predvsem kaziva dejanja, povezana s kršitvami avtorskih pravic; prevare, povezane s kriminalom; otroško pornografijo in kaznivimi dejanji, povezanimi z varnostjo omrežij. Prav tako določa številne postopkovne pristojnosti, kot so iskanje in prestrežanje vsebine na računalniških omrežjih (<http://mid.gov.si/mid/mid.nsf>, 30. 5. 2005).

⁵ Povzetek konvencije o kibernetски kriminaliteti je v Prilogi C.

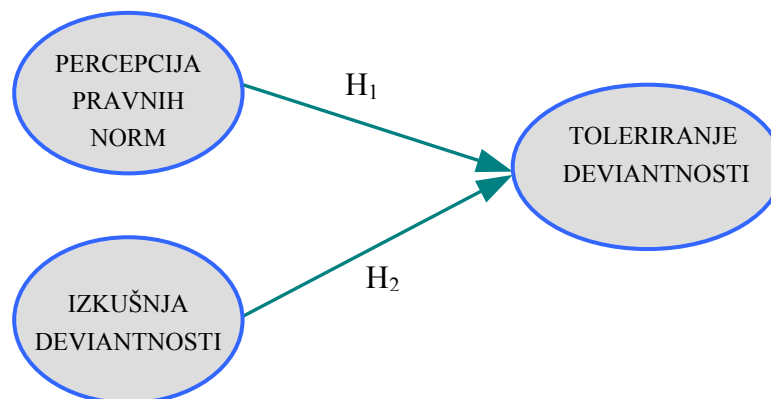
Po konvenciji se jurisdikcija posamezne države lahko nanaša samo na njen teritorij, ladje in letala ter njene državljane. Poleg tega pa konvencija ureja tudi mednarodno sodelovanje med državami, saj se računalniške mreže vedno bolj globalizirajo. Glavna načela v zvezi z mednarodnim sodelovanjem se po konvenciji nanašajo na:

- izročitev (ekstradicijo),
- medsebojno pomoč pri preiskovanjih, sodnih postopkih in zbiranju e-dokazov o kriminalnih dejanjih (Šercar, 2004: 18).

Republika Slovenija je konvencijo že delno upoštevala v svoji zakonodaji (v materialnem kazenskem pravu) pri zadnji spremembi Kazenskega zakonika, ki velja od 27. 8. 2004.

4 RAZISKOVALNI OKVIR ZAZNAVANJA DEVIANTNEGA VEDENJA NA INTERNETU

Na empirični ravni bom poskušala analizirati, *kako percepcija pravnih norm in izkušnja deviantnosti vplivata na dopuščanje deviantnih dejanj s strani posameznika*. Spodaj (slika 2) je grafično predstavljen ustrezen teoretski model s pojmi in hipotezami.



Slika 2: Teoretski model zaznavanja deviantnega vedenja na internetu

4.1 Definicije pojmov

Toleriranje deviantnosti je dopuščanje dejanj, ki odstopajo od ustaljenih družbeno sprejetih norm in vrednot oziroma družbeno sprejetih načinov delovanja (Haralambos in Holborn, 1999: 393), kot še sprejemljivih.

Percepcija pravnih norm je zaznavanje pravil o vedenju, ki vsebujejo določbe o uporabi državne kazni, v kolikor bo ta norma kršena in v kolikor bo kršitelj prijet (Pečar, 1988: 79).

Izkušnja deviantnosti je doživetje in spoznanje dejanj, ki odstopajo od ustaljenih družbeno sprejetih norm in vrednot oziroma družbeno sprejetih načinov delovanja (Haralambos in Holborn, 1999: 393).

4.2 Hipoteze

Na podlagi raziskovalnega vprašanja sem postavila dve hipotezi, ki ju bom med statistično analizo poizkušala potrditi ali pa ovreči. Hipotezi sta sledeči:

- **Hipoteza 1:** Večja napačna percepcija pravnih norm zvišuje toleriranje deviantnosti.

Sampson in Jeglum Bartucsh ugotavljata, da posameznikovo zaznavanje določenih dejanj kot primernih ni nujno zaznavanje primerne vedenja s stališča širše družbe oziroma družbenih mehanizmov, kot sta npr. pravo in policija, ki uravnavata to področje (Sampson in Jeglum Bartucsh, 1998: 782).

Posameznikovo vedenje in njegova dejanja pa niso nujno sama po sebi deviantna, kar pomeni, da niso v nasprotju z njegovo biološko naravo. Nekatera dejanja so lahko s stališča posameznika in s stališča njegove biološke osebnosti popolnoma normalna ali pa celo pozitivna. Tu so mišljena takšna pravno negativno ovrednotena posameznikova dejanja, ki pomenijo zanj sprostitev ali celo osvoboditev nekega pritiska, napetosti itd. Tako je krvno maščevanje za »Šiptarja«

in njegovo neposredno socialno okolje ne le pozitivno dejanje, temveč stvar njegovega ugleda in časti, še več, stvar njegove nadaljnje eksistence v ožjem okolju, medtem ko takšno vedenje njegovo širše okolje negativno vrednoti (Bavcon in drugi, 1964: 20). Posameznik torej lahko zaradi vpetosti v neko ožje družbeno okolje ali družbeno skupino napačno zaznava pravne norme širše družbe, v kateri živi; kar vodi v to, da posledično določena družbeno nesprejemljiva dejanja tolerira kot sprejemljiva.

Če pri argumentaciji zgornje hipoteze izhajam še iz socioloških teorij deviantnosti, se lahko oprem na Davida Matzo (v Haralambos in Holborn, 1999: 404), ki se je ukvarjal s problemom, kjer deviantni vseeno izpeljejo nelegalna dejanja, čeprav na splošno spoštujejo dogovorjene norme in vrednote. Trdil je namreč, da so posamezniki v določenih okoliščinah sposobni »nevtralizirati« moralno vez družbe. To pomeni, da so posamezniki sposobni prepričati sami sebe, da zakon za njih v določenem primeru ne velja. Deviantnost posameznikov postane torej mogoča, ko uporabijo *tehnike nevtralizacije*, ki jih začasno osvobodijo družbenega prijema (Matza v Haralambos in Holborn, 1999: 404).

Tehnike nevtralizacije pa po Matzi in Sykesu (v Becker, 1963: 28–29) vključujejo:

- zanikanje odgovornosti za deviantno dejanje;
- zanikanje škode, ki je posledica tega deviantnega dejanja;
- zanikanje, da je bilo dejanje v bistvu napačno;
- obsodba tistih, ki uveljavljajo pravila;
- poziv k večji lojalnosti, kar pomeni, da deviantje lahko trdijo, da ne kršijo zakona zaradi svojega lastnega interesa, temveč zaradi dejstva, da pomagajo npr. svoji družini ali prijateljem.

Po Matzi torej posamezniki določena nelegalna dejanja opravičujejo z različnimi tehnikami nevtralizacije. V teh primerih pravnih norm ne zaznavajo na način, kot jim ga nalagajo centri državne in pravne oblasti, marveč na način, na katerega ta dejanja zaznavajo oni sami (Matza v Haralambos in Holborn, 1999: 404–405).

- **Hipoteza 2:** Izkušnja deviantnosti zvišuje toleriranje deviantnosti s strani posameznika.

Hindelang je pri preučevanju Matzaovih in Sykesovih tehnik nevtralizacije ugotovil, da naklonjenost do deviantnosti zelo variira med posamezniki. Ugotovil je namreč, da tisti posamezniki, ki niso bili udeleženi v deviantnih dejanjih, bolj neodobravajo deviantna dejanja v primerjavi s posamezniki, ki so bili udeleženi v deviantnih dejanjih vsaj enkrat (v Sampson in Jeglum Bartusch, 1998: 779).

5 OPIS VZORCA IN ZBIRANJE PODATKOV

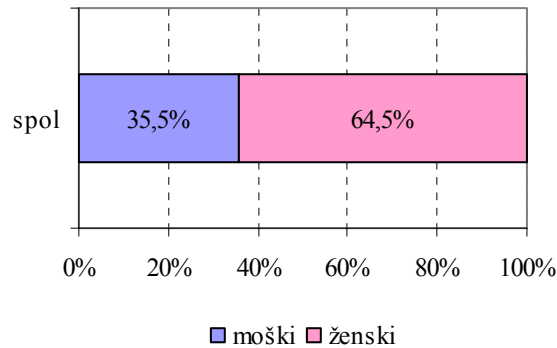
Zbiranje podatkov je potekalo konec aprila 2004 ter konec maja 2005, in sicer so bili podatki zbrani s pomočjo terenskega anketiranja. Anketirana populacija so bili naključno izbrani študentje, ki so se v času anketiranja nahajali na fakultetah, na katerih je anketiranje potekalo⁶. Anketiranje je potekalo v treh fazah. Prvi dve fazi sta potekali aprila 2004 na Filozofski fakulteti in Fakulteti za družbene vede, tretja faza pa je potekala maja 2005 na Fakulteti za Elektrotehniko ter Fakulteti za matematiko in fiziko⁷. Respondenti so odgovarjali na sedem vprašanj, ki so se nanašala na področje informacijsko-komunikacijskih tehnologij ter na tri demografska vprašanja.

V anketi je sodelovalo 334 študentov Fakultete za družbene vede in drugih fakultet, ki so bili v vzorec zbrani naključno.

⁶ Gre torej za vzorec študentov, ki so bili v trenutku anketiranja »pri roki«.

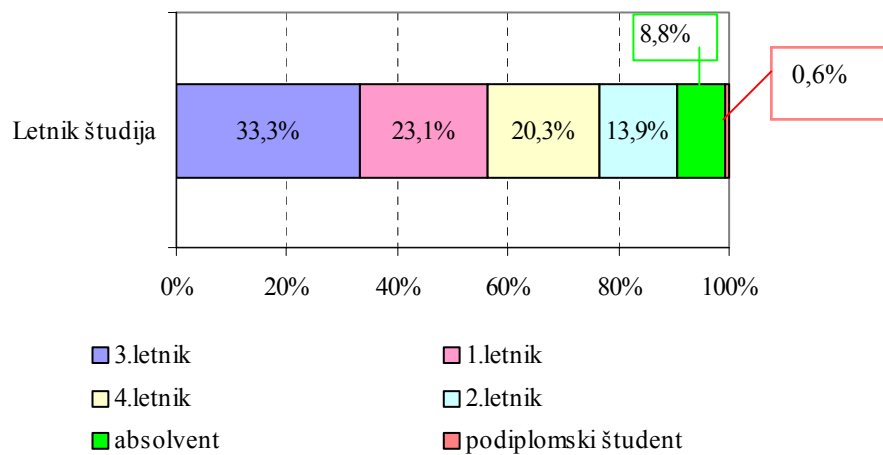
⁷ V anketiranje niso bili vključeni samo študentje omenjenih fakultet, ampak tudi študentje nekaterih drugih fakultet, ki so se v času anketiranja nahajali na omenjenih dveh fakultetah.

Slike, ki sledijo v nadaljevanju, prikazujejo demografske značilnosti anketiranih študentov:



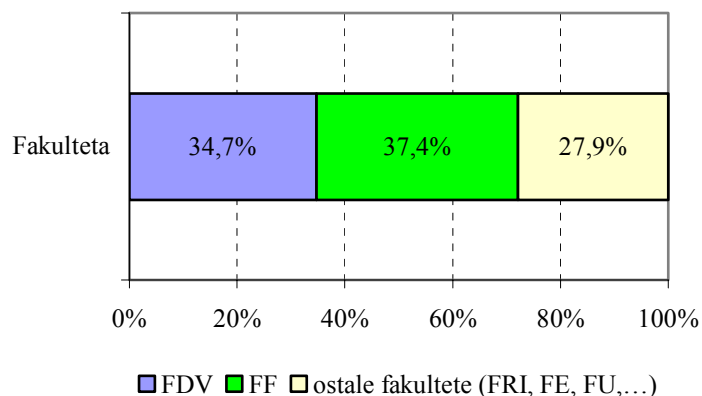
Slika 3: Grafični prikaz porazdelitve deležev anketiranih študentov glede na spol (n = 332)

Iz zgornje slike je razvidno, da v vzorcu prevladujejo ženske (64.5 %), saj fakultete, s katerih prihaja največje število respondentov, obiskuje veliko število deklet.



Slika 4: Grafični prikaz porazdelitve deležev anketiranih študentov po letniku študija (n = 330)

Največji delež anketiranih študentov obiskuje 3. letnik (33.3 %), sledijo pa jim študentje prvih in četrth letnikov. Najmanjši delež anketiranih je podiplomskih študentov (0.6 %).



Slika 5: Grafični prikaz porazdelitve deležev anketiranih študentov glede na fakulteto (n = 334)

Največji delež anketiranih študentov je vpisanih na Filozofsko fakulteto (37.4 %), sledijo študentje Fakultete za družbene vede (34.7 %), preostali delež anketiranih študentov pa predstavljajo študentje ostalih fakultet.

6 OPERACIONALIZACIJA

Operacionalni model je sestavljen tako, da je iz njega razvidno, kateri so posamezni indikatorji, ki merijo določeno spremenljivko. V nadaljevanju bom zato najprej predstavila indikatorje, ki merijo posamezne spremenljivke, nato pa še operacionalni model, iz katerega bom izhajala v nadaljnji analizi.

6.1 Indikatorji spremenljivk⁸

Spremenljivka *percepcija pravnih norm* je bila merjena s spodnjimi indikatorji označenimi od Y₇ do Y₁₂ in bo predstavljala seštevek posameznih indikatorjev. Večja vrednost dobljene spremenljivke bo pomenila večje pravilno zaznavanje pravnih norm s strani posameznika.

⁸ Indikatorje sem oblikovala na podlagi Kazenskega zakonika RS, in sicer iz členov, ki neposredno ali posredno urejajo področje kibernetске kriminalitete.

Spremenljivka *izkušnja deviantnosti* je bila merjena s spodnjimi indikatorji označenimi od Y₁₃ do Y₁₈ in bo prav tako predstavljala seštevek posameznih indikatorjev. Večja vrednost dobljene spremenljivke pa bo pomenila večjo izkušnjo deviantnosti s strani posameznika.

Spremenljivka *toleriranje deviantnosti* je bila merjena s spodnjimi indikatorji označenimi od Y₁ do Y₆, ki jih bom konstruirala v eno spremenljivko s pomočjo faktorске analize.

Posamezne spremenljivke sem merila z naslednjimi indikatorji⁹:

a. Če nekdo povzame del članka drugega avtorja in ga ne citira:

	popolnoma se NE strinjam	se ne strinjam	ni - ni	se strinjam	popolnoma se strinjam	
• To ni tako problematično.	1	4	5	4	5	y1
• Ali je to dovoljeno?	da		ne		ne vem	y7
• Ali ste to že kdaj naredili?		da			ne	y13

b. Če nekdo »skopira« mesečno vozovnico in jo nato uporablja:

• To ni tako problematično.	1	2	3	4	5	y2
• Ali je to zakonito?	da		ne		ne vem	y8
• Ali ste to že kdaj naredili?		da			ne	y14

c. Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal:

• To ni tako problematično.	1	2	3	4	5	y3
• Ali je to pravno sporno?	da		ne		ne vem	y9
• Ali ste to že kdaj naredili?		da			ne	y15

d. Kopiranje originalnega CD-ja z glasbo za lastno uporabo¹⁰:

• Ni tako problematično.	1	2	3	4	5
• Ali je to dovoljeno?	da		ne		ne vem
• Ali ste to že kdaj naredili?		da			ne

e. Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu:

• Ni tako problematična.	1	2	3	4	5	y4
• Ali je to pravno sporno?	da		ne		ne vem	y10
• Ali ste to že kdaj naredili?		da			ne	y16

⁹ V skrajno desnem stolpcu so predstavljene oznake posameznih indikatorjev.

¹⁰ Indikatorja ne bom uporabila v analizi, ker mi je predstavljal samo kontrolni indikator.

f. Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo:

• To ni tako problematično.	1	2	3	4	5	y5
• Ali je to zakonito?	da	ne	ne vem			y11
• Ali ste to že kdaj naredili?	da	ne				y17

g. Če nekdo prebere elektronsko pošto druge osebe, ne da bi le-ta vedela za to:

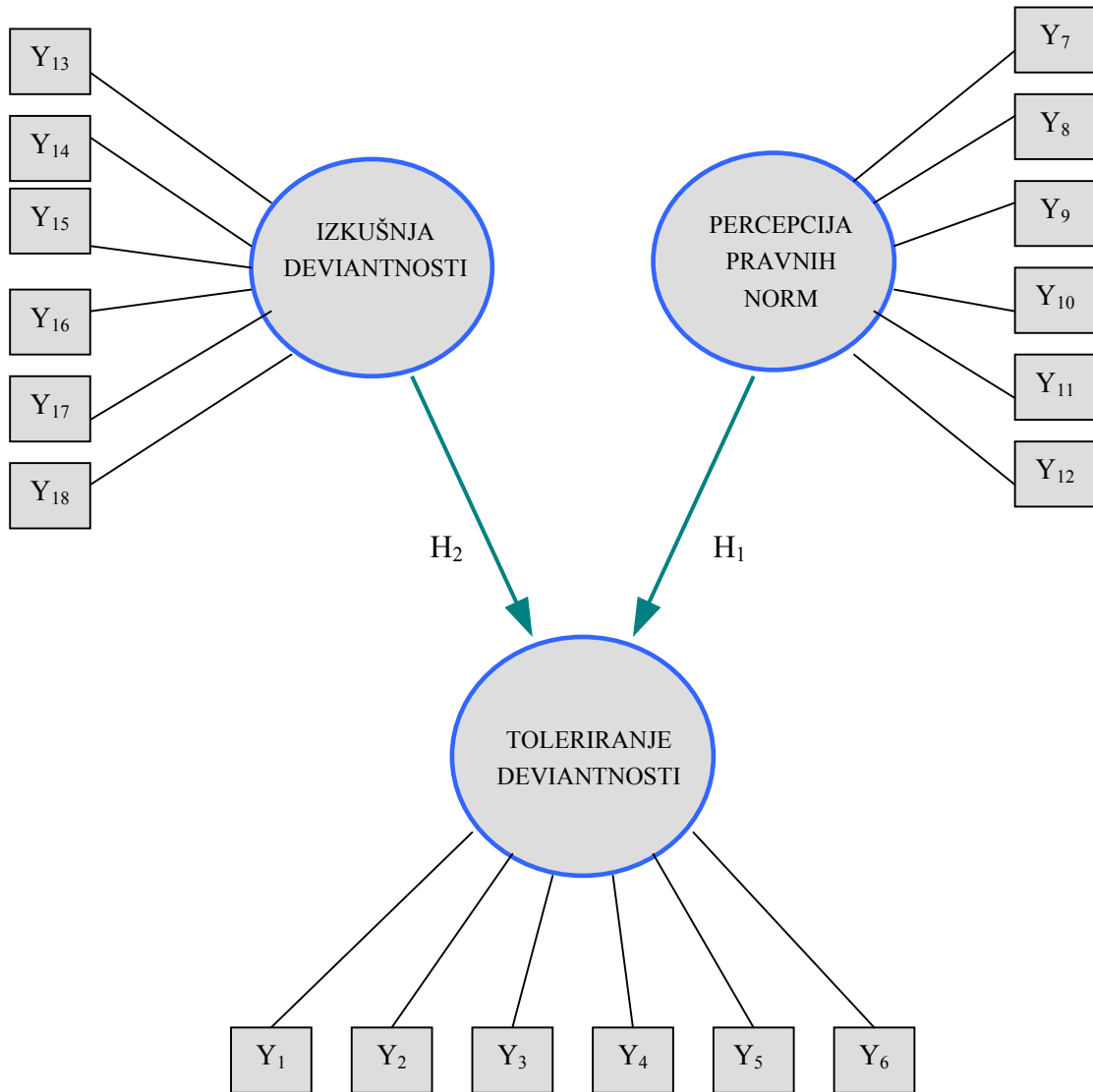
• To ni tako problematično.	1	2	3	4	5	y6
• Ali je to dovoljeno?	da	ne	ne vem			y12
• Ali ste to že kdaj naredili?	da	ne				y18

Tabela 2: Poimenovanje posameznih indikatorjev na podlagi Kazenskega zakonika

Indikator	Ime indikatorja – kaznivo dejanje
Če nekdo povzame del članka drugega avtorja in ga ne citira.	Kršenje avtorskih parvic 1
Če nekdo »skopira« mesečno vozovnico in jo nato uporablja.	Ponarejanje dokumentov
Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal.	Kršenje avtorskih parvic 2
Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu.	»crack-anje« računalniških programov – tudi kršenje avtorskih pravic
Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo.	»spam«
Če nekdo prebere elektronsko pošto druge osebe, ne da bi le-ta vedela za to.	Vdor v zaščiteno bazo podatkov

6.2 Operacionalni model

Spodnja slika predstavlja operacionalni model s posameznimi indikatorji merjenih spremenljivk.



Slika 6: Grafični prikaz operacionalnega modela

7 ANALIZE IN REZULTATI

7.1 Osnovne statistike posameznih indikatorjev in izvedenih spremenljivk

V nadaljevanju bom najprej predstavila analize posameznih indikatorjev vsake izmed merjenih spremenljivk, nato pa še analize izvedenih spremenljivk.

- Analiza posameznih indikatorjev neodvisne spremenljivke *percepcija pravnih norm*:

Tabela 3: Frekvenčne porazdelitve posameznih indikatorjev – deleži (spremenljivka percepcija pravnih norm)

	kršitev avtorskih pravic (1) – nepravilno povzemanje	ponarejanje dokumentov	kršitev avtorskih pravic (2) – »download-anje« filmov	»crack-anje« ¹¹ računalniških programov	»spam«	vdor v zaščiteno bazo podatkov
NE zaznava kot normo (%)	17.4	3.5	34.2	48.1	80.0	26.9
zaznava kot normo (%)	82.6	96.5	65.8	51.9	20.0	73.1
skupaj (%)	100.0	100.0	100.0	100.0	100.0	100.0

Iz zgornje tabele je razvidno, da večina respondentov zaznava kršenje avtorskih pravic (1) – nepravilno povzemanje člankov, ponarejanje dokumentov ter vdor v zaščiteno bazo podatkov kot nezakonito; nekoliko manjši delež respondentov pa zaznava kršenje avtorskih pravic (2) – »download-anje« filmov z interneta kot nezakonito. Na drugi strani se le pošiljanje »spama« večini respondentov ne zdi pravno sporno.

Posamezniki torej zaznavajo večino deviantnih dejanj kot nezakonitih, izjema je le eno izmed analiziranih deviantnih dejanj, in sicer »spam«, saj ta oblika deviantnega vedenja ni nujno kazniva.

¹¹ *Krekerji* (»crackers«) so posamezniki, ki razbijajo (»crack-ajo«) zavarovane informacijsko-komunikacijske sisteme. Dandanes se pojem kreker povezuje s posamezniki, ki so specializirani za razbijanje gesel (Littlejohn Shnider, 2002: 53).

- Analiza posameznih indikatorjev neodvisne spremenljivke **izkušnja deviantnosti**:

Tabela 4: Frekvenčne porazdelitve posameznih indikatorjev – deleži (spremenljivka izkušnja deviantnosti)

	kršitev avtorskih pravic (1) – nepravilno povzemanje	ponarejanje dokumentov	kršitev avtorskih pravic (2) – »download-anje« filmov	»crack-anje« računalniških programov	»spam«	vdor v zaščiteno bazo podatkov
Je že storil/-a deviantno dejanje (%)	41.5	7.1	58.4	40.2	8.5	12.1
Ni še storil/-a deviantnega dejanja (%)	58.5	92.9	41.6	59.8	91.5	87.9
skupaj (%)	100.0	100.0	100.0	100.0	100.0	100.0

Iz zgornje tabele je razvidno, da večina respondentov še ni ponaredila dokumentov, »skrekala« računalniškega programa, poslala »spama« ter vdrla v zaščiteno bazo podatkov. Velik delež respondentov pa je že kršil avtorske pravice (1 in 2), torej so nepravilno povzemali članke drugih avtorjev in tudi »download-ali« filme z interneta.

- Analiza posameznih indikatorjev odvisne spremenljivke **toleriranje deviantnosti**:

Tabela 5: Frekvenčne porazdelitve posameznih indikatorjev – deleži (spremenljivka toleriranje deviantnosti)

	kršitev avtorskih pravic (1) – nepravilno povzemanje	ponarejanje dokumentov	kršitev avtorskih pravic (2) – »download-anje« filmov	»crack-anje« računalniških programov	»spam«	vdor v zaščiteno bazo podatkov
popolnoma NE tolerira deviantnega dejanja (%)	46.3	40.7	5.0	13.1	35.7	58.2
NE tolerira deviantnega dejanja (%)	26.8	24.0	9.5	15.0	19.3	22.0
niti - niti (%)	12.4	18.7	19.8	38.1	19.6	10.1
tolerira deviantno dejanje (%)	10.3	10.1	28.7	18.4	13.7	5.3
popolnoma tolerira deviantno dejanje (%)	4.1	6.5	37.0	15.3	11.6	4.5
skupaj (%)	100.0	100.0	100.0	100.0	100.0	100.0

Iz zgornje tabele je razvidno, da velik delež respondentov ne tolerira kršenja avtorskih pravic (1) – nepravilno povzemanje člankov, ponarejanja dokumentov, »spama« ter vdora v zaščiteno bazo podatkov, medtem ko velik delež respondentov tolerira drug

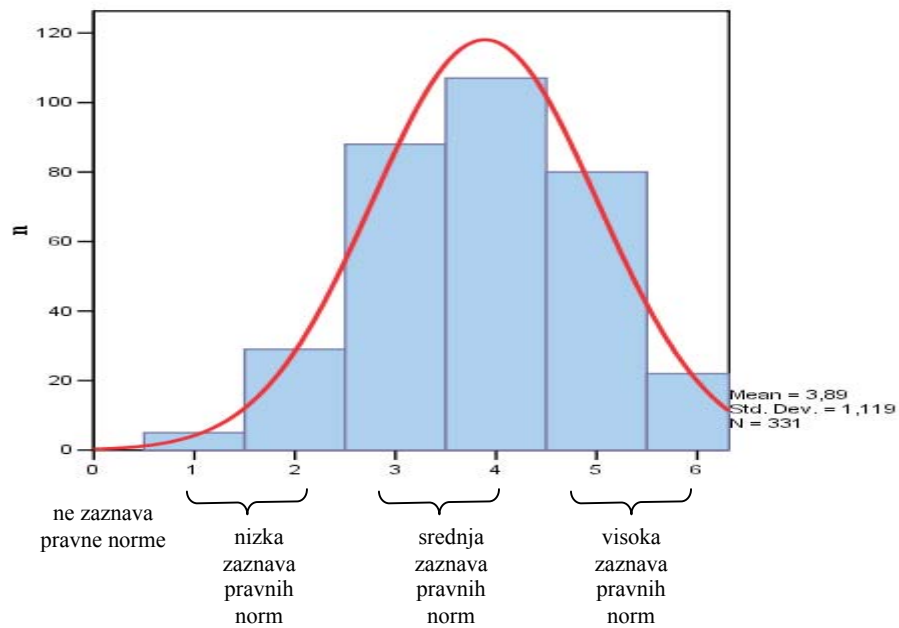
način kršenja avtorskih pravic (2) - »download-anje« filmov z interneta. Slednje je verjetno povezano z dejstvom, da je to obliko avtorskih pravic kršila že več kot polovica respondentov. Velik delež (38.1 %) respondentov pa niti tolerira niti ne tolerira »krekanja« računalniških programov.

Tabela 6: Spremenljivka toleriranje deviantnosti – osnovne statistike

Indikator	ime indikatorja	n	povprečje	st. odklon
Če nekdo povzame del članka drugega avtorja in ga ne citira ... to ni tako problematično.	kršitev avtorskih pravic (1)	339	1.99	1.17
Če nekdo »skopira« mesečno vozovnico in jo nato uporablja ... to ni tako problematično.	ponarejanje dokumentov	337	2.18	1.25
Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal ... to ni tako problematično.	kršitev avtorskih pravic (2)	338	3.83	1.17
Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu ... ni tako problematična.	»crack-anje« računalniških programov	320	3.08	1.21
Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo ... to ni tako problematično.	»spam«	336	2.46	1.39
Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to ... to ni tako problematično.	vdor v zaščiteno bazo podatkov	337	1.76	1.12

Izkaže se, da posamezniki nekaterih deviantnih dejanj ne tolerirajo, saj povprečja posameznih indikatorjev bistveno ne odstopajo od srednjih vrednosti po posameznih indikatorjih. Posamezniki ne tolerirajo naslednjih dejanj: kršenje avtorskih pravic (1) – nepravilno povzemanje člankov, ponarejanje dokumentov ter vdor v zaščiteno bazo podatkov. Ostala dejanja pa posamezniki tolerirajo oziroma se jim ne zdijo tako problematična. V povprečju se jim zdi najmanj problematično dejanje, ko posameznik »sname« film z interneta z namenom, da bi si ga ogledal (kršenje avtorskih pravic 2).

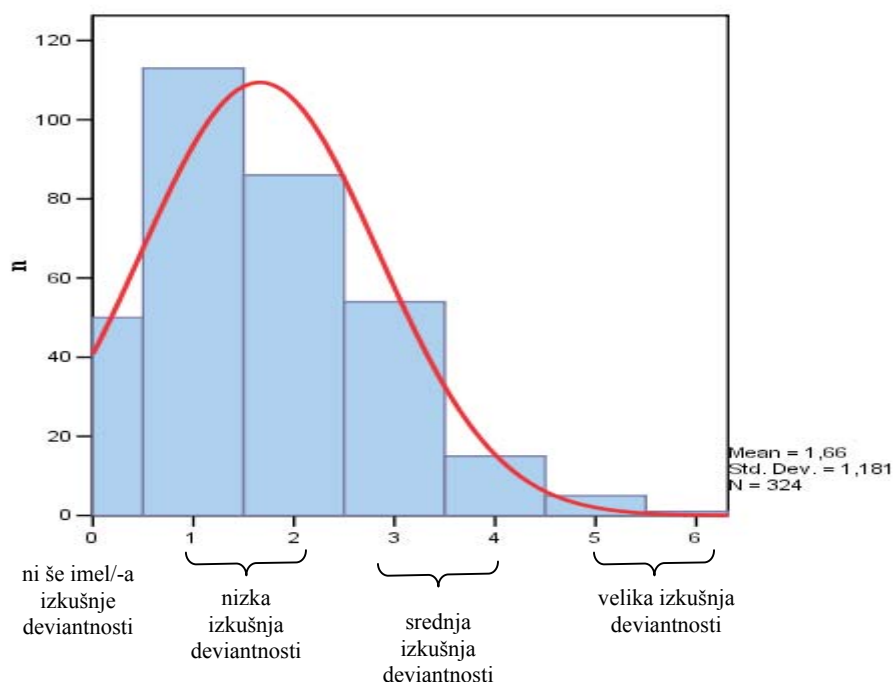
- Analiza izvedene spremenljivke **percepcija pravnih norm**:



Slika 7: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke percepcija pravnih norm (n=331)

Iz zgornje slike je razvidno, da največji delež respondentov zaznava večino pravnih norm (zaznavajo od 3 do 5 pravnih norm – skupaj – 83.09 %), majhen delež pa zaznava vse pravne norme (6.55 %). Vsi respondenti zaznavajo vsaj eno pravno normo.

- Analiza izvedene spremenljivke **izkušnja deviantnosti**:

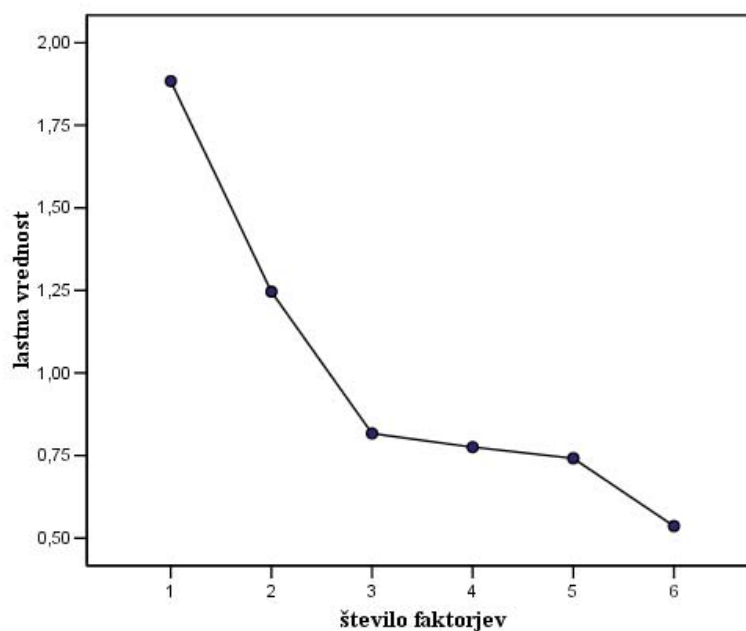


Slika 8: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke izkušnja deviantnosti (n=324)

Iz zgornje slike je razvidno, da je že več kot polovica respondentov imela majhno izkušnjo deviantnosti (storili so 1 do 3 deviantna dejanja – skupaj 78.09 %); 15.43 % respondentov še ni storilo nobenega izmed deviantnih dejanj; le 0.31 % respondentov pa je storilo že vsa našeta deviantna dejanja.

- Na strani, ki sledi, je prikazana analiza spremenljivke **toleriranje deviantnosti** na podlagi *faktorske analize*. Zaradi ugotovitve, da vrednosti posameznih indikatorjev niso približno normalno porazdeljene, sem uporabila metodo glavnih osi (»PAF«) ter poševno rotacijo z metodo »oblamin«.

"Scree" diagram



Slika 9: Faktorska analiza – »scree« diagram (n=324)

Iz »scree« diagrama je razvidno, da ima moj faktorski model dva faktorja. Na naslednji strani pa podajam še tabelo faktorskih uteži, iz katere sta prav tako razvidna dva faktorja ter kateri indikatorji tvorijo posamezen faktor.

Tabela 7: Faktorska analiza – »patteren« uteži¹² (n=324)

	»Patteren« uteži	
	F1	F2
Če nekdo povzame del članka drugega avtorja in ga ne citira ... to ni tako problematično	0.410	0.247
Če nekdo »skopira« mesečno vozovnico in jo nato uporablja ... to ni tako problematično	0.466	-0.036
Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal ... to ni tako problematično	0.699	-0.090
Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu ... ni tako problematična	0.645	-0.036
Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo ... to ni tako problematično	-0.043	0.411
Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to ... to ni tako problematično	-0.001	0.451
λ_i	1.884	1.246
% pojasnjene variance	31.395	20.769

¹² model je skonvergirala v štirih iteracijah

Uteži, predstavljene v tabeli 7, ki so večje od 0.40, sem poudarila s krepkim tiskom, tako je vidno, na katerem faktorju ima posamezna spremenljivka izrazite uteži. Rezultate podajam spodaj:

Tabela 8: 1. faktor – toleriranje »škodljive« deviantnosti

kršitev avtorskih pravic (1)	Če nekdo povzame del članka drugega avtorja in ga ne citira ... to ni tako problematično.
ponarejanje dokumentov	Če nekdo »skopira« mesečno vozovnico in jo nato uporablja ... to ni tako problematično.
kršitev avtorskih pravic (2)	Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal ... to ni tako problematično.
»crack-anje« računalniških programov	Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu ... ni tako problematična.

Tabela 9: 2. faktor – toleriranje »neškodljive« deviantnosti

»spam«	Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo ... to ni tako problematično.
vdor v zaščiteno bazo podatkov	Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to ... to ni tako problematično.

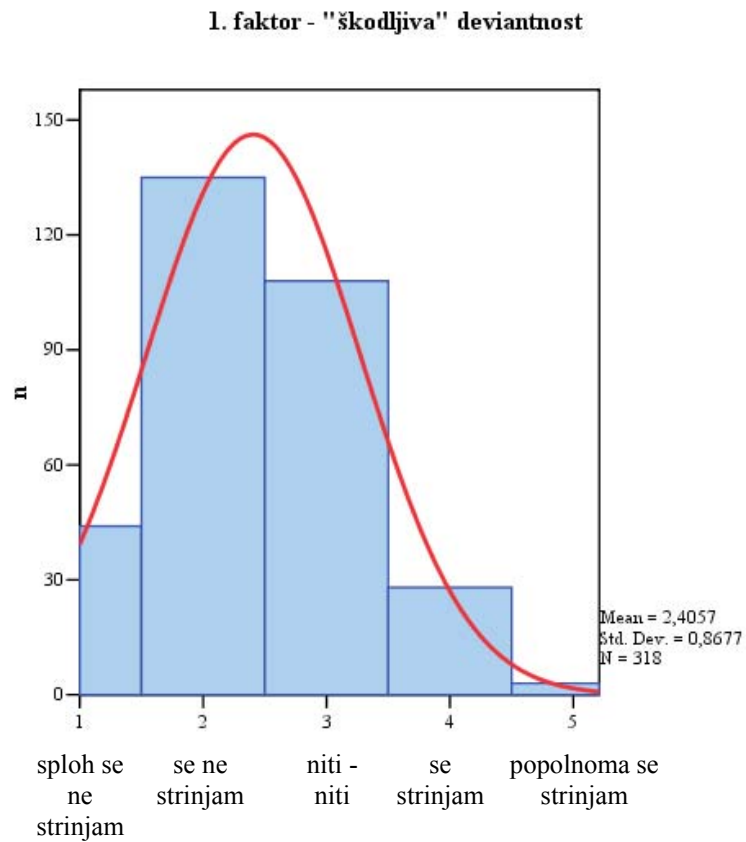
S pomočjo faktorjske analize sem v ozadju šestih indikatorjev spremenljivke toleriranje deviantnosti razkrila dva faktorja, in sicer toleriranje »neškodljive« deviantnosti ter toleriranje »škodljive« deviantnosti, ki ju bom v nadaljevanju uporabila tudi v bivariatni in regresijski analizi.

*Toleriranje »škodljive« deviantnosti*¹³ (v kibernetnem prostoru) je dopuščanje kaznivih dejanj, ki škodijo družbi. Tu gre predvsem za kazniva dejanja, storjena iz koristoljubja, kot je npr. okoriščanje z nepooblaščenim reproduciranjem avtorskih del drugih (Wall, 2001). *Toleriranje »neškodljive« deviantnosti*¹⁴ (v kibernetnem prostoru) pa je dopuščanje dejanj, ki ne škodijo družbi, ampak k njej pozitivno prispevajo, saj odkrivajo njene ranljive dele. Tu gre predvsem za vrsto kibernetnega kriminala, ki ga enačimo s prvotnim pojavom hekerstva – hekerji so bili namreč v svoji prvotni vlogi popolnoma »neškodljivi« za družbo. Še dandanes je ta vidik kibernetnega kriminala zelo pomemben, kajti dejansko lahko mnogo prispeva predvsem k izboljšanju zaščite pred drugo vrsto deviantnosti, ki jo razpoznamo v kibernetnem prostoru, in sicer »škodljivo deviantnostjo« (Wall, 2001).

¹³ Toleriranje »škodljive« deviantnosti oziroma toleriranje »škodljive« kibernetne kriminalitete.

¹⁴ Toleriranje »neškodljive« deviantnosti oziroma toleriranje »neškodljive« kibernetne kriminalitete.

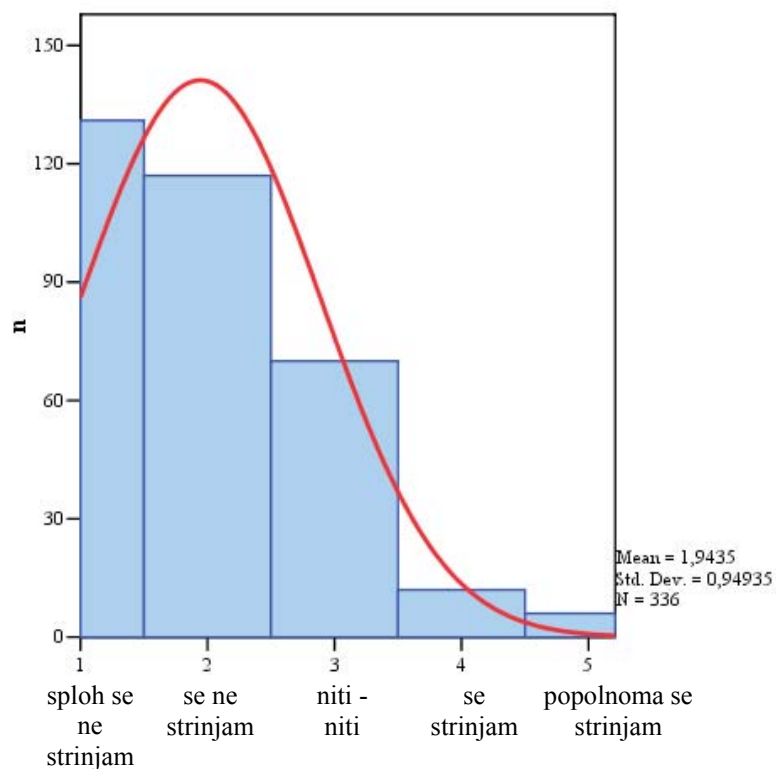
- Analiza izvedene spremenljivke **toleriranje deviantnosti**:



Slika 10: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke toleriranje deviantnosti – 1. faktor (n=318)

Iz zgornje slike je razvidno, da več kot polovica respondentov ne tolerira deviantnih dejanj, smatranih kot »škodljiva« deviantnost (56.3 %), le 9.7 % pa tolerira deviantna dejanja, smatrana kot »škodljiva« deviantnost.

2. faktor - "neškodljiva" deviantnost



Slika 11: Grafični prikaz frekvenčne porazdelitve izvedene spremenljivke toleriranja deviantnosti – 2. faktor (n=336)

Iz zgornje slike je razvidno, da več kot polovica respondentov ne tolerira deviantnih dejanj, smatranih kot »neškodljiva« deviantnost (73.8 %), le 5.4 % pa tolerira deviantna dejanja, smatrana kot »neškodljiva« deviantnost. Delež tistih, ki ne tolerirajo deviantna dejanja, smatrana kot »neškodljiva« deviantnost, je za 17.5 % višji v primerjavi s tistimi, ki ne tolerirajo deviantnih dejanj, smatranih kot »škodljiva« deviantnost.

Kako zanesljivo je merjenje, nam pokaže Crombachov α , katerega vrednost v primeru toleriranja »škodljive« deviantnosti znaša v primeru 0.621, kar kaže na to, da je izvedeno merjenje dokaj zanesljivo. V primeru toleriranja »neškodljive« deviantnosti pa vrednost Crombachovega α znaša le 0.291, kar pomeni, da merjenje v tem primeru ni bilo zanesljivo.

Na podlagi faktorске analize se je torej izkazalo, da sta v ozadju spremenljivke toleriranje deviantnosti dve dimenziji, ki sem ju na podlagi primarne hekerske etike poimenovala toleriranje »škodljive« in toleriranje »neškodljive« deviantnosti.

7.2 Povezanost izvedenih spremenljivk

Tabela 10: Korelacijska matrika izvedenih spremenljivk (n=332)

	»škodljiva« deviantnost	»neškodljiva« deviantnost	percepcija pravnih norm	izkušnja devinatnosti
»škodljiva« deviantnost	1			
»neškodljiva« deviantnost	0.081	1		
percepcija pravnih norm	-0.101*	-0.190***	1	
izkušnja devinatnosti	0.195***	0.098*	0.133**	1

*** Korelacija je značilna pri stopnji značilnosti manjši od 0.01

** Korelacija je značilna pri stopnji značilnosti večji od 0.01 in manjši od 0.05

* Korelacija je značilna pri stopnji značilnosti večji od 0.05 in manjši od 0.1

Na podlagi statističnih značilnosti Pearsonovega koeficienta korelacije je razvidno, da obstaja statistično značilna negativna povezanost med spremenljivko percepcija pravnih norm in spremenljivkama toleriranje »neškodljive« in »škodljive« deviantnosti ter statistično pozitivna povezanost med spremenljivko izkušnja deviantnosti in spremenljivkama toleriranje »škodljive« in »neškodljive« deviantnosti. Prav tako pa obstaja tudi statistično značilna pozitivna povezanost med spremenljivkama percepcija pravnih norm in izkušnjo deviantnosti.

Statistično značilna negativna povezanost med spremenljivko percepcija pravnih norm in spremenljivkama toleriranje »neškodljive« in »škodljive« deviantnosti pomeni, da se z večanjem pravilne percepcije pravnih norm manjša toleriranje »neškodljive« in »neškodljive« deviantnosti in obratno. Statistično značilna pozitivna povezanost med spremenljivko izkušnja deviantnosti in spremenljivkama toleriranje »škodljive« in »neškodljive« deviantnosti pa pomeni, da se z večanjem izkušnje deviantnosti veča tudi toleriranje »škodljive« in »neškodljive« deviantnosti in obratno.

7.3 Preverjanje modela in hipotez

7.3.1 Preverjanje modela

Za preverjanju modela in hipotez sem uporabila regresijsko analizo, ki sem jo morala v programu SPSS »zavrteti« dvakrat, ker sem v predhodni faktorski analizi dobila dve dimenziji spremenljivke toleriranje deviantnosti. Pri preverjanju prvega modela sem v analizo vključila obe neodvisni spremenljivki – percepcijo pravnih norm in izkušnjo deviantnosti ter neodvisno spremenljivko toleriranje »škodljive« deviantnosti. Pri preverjanju drugega modela pa sem v analizo prav tako vključila obe neodvisni spremenljivki ter odvisno spremenljivko toleriranje »neškodljive« deviantnosti.

Tabela 11: Regresijska analiza 1 – odvisna spremenljivka toleriranje »škodljive« deviantnosti – regresijski koeficienti (n=332)

	Nestandardizirani regresijski koeficient (B)		Standardizirani regresijski koeficient	t	Sig.
	B	Std. napaka	Beta		
percepcija pravnih norm	-0.089	0.042	-0.120	-2.131	0.034
izkušnja deviantnosti	0.141	0.040	0.201	3.554	0.000
konstanta	0.111	0.176		0.630	0.529

Tabela 12: Regresijska analiza 1 – odvisna spremenljivka toleriranje »škodljive« deviantnosti – vrednosti posameznih statistik (n=332)

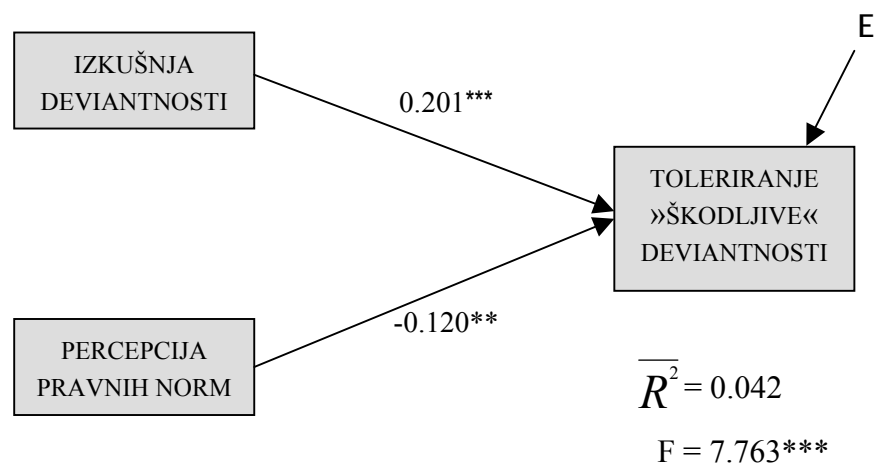
Statistika	Vrednost	Interpretacija stopenj značilnosti
R	0.221	$p < 0.01 \rightarrow ***$
R^2	0.049	$0.01 \leq p < 0.05 \rightarrow **$
$\overline{R^2}$	0.042	$0.05 \leq p < 0.1 \rightarrow *$
F	7.763 ***	$p \geq 0.10$

F-statistika nam pove, kako dobro se regresijski model v celoti prilega podatkom. V primeru prvega regresijskega modela znaša F-statistika 7.763, statistična značilnost F-statistike pa je manjša od 0.01, kar pomeni, da se prvi regresijski model dobro prilega podatkom.

Odstotek pojasnjene variance je samo 4.2 %, kar pomeni, da moje neodvisne spremenljivke odvisno spremenljivko le delno pojasnjujejo, vendar pa je to še vedno

zadovoljivo za razmere družboslovja, ker vpliva drugih dejavnikov na odvisno spremenljivko ne moremo odstraniti.

Na spodnji sliki je prikazan regresijski model, v katerem so grafično prikazani vplivi neodvisnih spremenljivk na odvisno spremenljivko. Vrednosti, zapisane na puščicah, predstavljajo standardizirane regresijske koeficiente, ki kažejo vpliv neodvisnih spremenljivk na odvisno spremenljivko brez vpliva ostalih spremenljivk.



Slika 12: Regresijski model 1 – odvisna spremenljivka toleriranje »škodljive« deviantnosti

Neodvisna spremenljivka izkušnja deviantnosti statistično značilno pozitivno močno vpliva na odvisno spremenljivko toleriranje »škodljive« deviantnosti. To pomeni, da se z večanjem izkušnje deviantnosti večja tudi toleriranje »škodljive« deviantnosti; medtem ko neodvisna spremenljivka percepcija pravnih norm statistično značilno negativno srednje močno vpliva na odvisno spremenljivko toleriranje »škodljive« deviantnosti, kar pomeni, da se z večanjem »pravilne« percepcije pravnih norm manjša toleriranje »škodljive« deviantnosti.

Tabela 13: Regresijska analiza 2 – odvisna spremenljivka toleriranje »neškodljive« deviantnosti – regresijski koeficienti (n=332)

	Nestandardizirani regresijski koeficient (B)		Standardizirani regresijski koeficient	t	Sig.
	B	Std. napaka	Beta		
percepcija pravnih norm	-0.111	0.031	-0.204	-3.624	0.000
izkušnja deviantnosti	0.066	0.031	0.129	2.279	0.023
konstanta	0.318	0.128		2.487	0.013

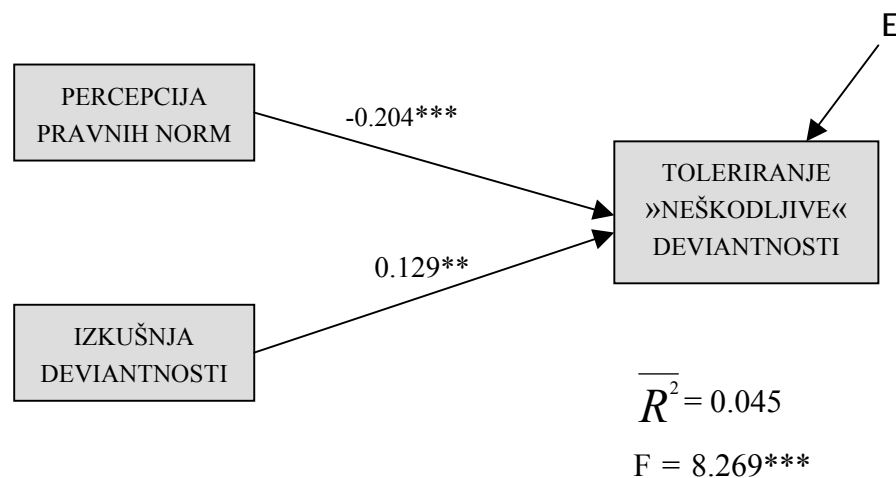
Tabela 14: Regresijska analiza 2 – odvisna spremenljivka toleriranje »neškodljive« deviantnosti – vrednosti posameznih statistik (n=332)

Statistika	Vrednost	Interpretacija stopenj značilnosti
R	0.227	$p < 0.01 \rightarrow ***$ $0.02 \leq p < 0.05 \rightarrow **$ $0.05 \leq p < 0.1 \rightarrow *$ $p \geq 0.10$
R^2	0.052	
$\overline{R^2}$	0.045	
F	8.261 ***	

V primeru drugega regresijskega modela znaša F-statistika 8.269, statistična značilnost F-statistike pa je tudi tu manjša od 0.01, kar pomeni, da se tudi drugi regresijski model dobro prilega podatkom.

Odstotek pojasnjene variance je samo 4.5 %, kar ponovno pomeni, da moje neodvisne spremenljivke odvisno spremenljivko le delno pojasnjujejo, vendar pa je to še vedno zadovoljivo za razmere družboslovja, ker vpliva drugih dejavnikov na odvisno spremenljivko ne moremo odstraniti.

Iz spodnje slike regresijskega modela je razvidno, da neodvisna spremenljivka percepcija pravnih norm statistično značilno negativno močno vpliva na odvisno spremenljivko toleriranje »neškodljive« deviantnosti, kar pomeni, da se z večanjem »pravilne« percepcije pravnih norm manjša toleriranje »neškodljive« deviantnosti; medtem ko neodvisna spremenljivka izkušnja deviantnosti statistično značilno pozitivno srednje močno vpliva na odvisno spremenljivko toleriranje »neškodljive« deviantnosti, kar pomeni, da se z večanjem izkušnje deviantnosti večja tudi toleriranje »neškodljive« deviantnosti.



Slika 13: Regresijski model 2 – odvisna spremenljivka toleriranje »neškodljive« deviantnosti

Na podlagi preverjanja obeh modelov s pomočjo regresijske analize se izkaže, da na toleriranje »škodljive« deviantnosti s strani posameznika vpliva predvsem njegova izkušnja te deviantnosti, nekoliko manj pa percepcija pravnih norm. Na posameznikovo toleriranje »neškodljive« deviantnosti pa vpliva predvsem njegova percepcija pravnih norm, nekoliko manj pa njegova izkušnja deviantnosti.

7.3.2 Preverjanje hipotez

S pomočjo rezultatov obeh regresijskih analiz lahko začnem obravnavati hipotezi, ki sem ju postavila na podlagi obstoječe teorije. Iz obeh regresijskih modelov je razvidno, da lahko potrdim postavljene hipotezi.

- **Hipoteza 1:** Večja napačna percepcija pravnih norm zvišuje toleriranje deviantnosti.

Hipotezo lahko potrdim, saj je na podlagi opravljenih regresijskih analiz razvidno, da spremenljivka percepcija pravnih norm statistično značilno negativno vpliva na spremenljivko toleriranje deviantnosti, kar pomeni, da se z večanjem pravilne percepcije pravnih norm manjša toleriranje deviantnosti. Torej način, na katerega posameznik zaznava pravne norme, vpliva na to, ali posameznik sprejema oziroma ne sprejema posamezna deviantna dejanja. Posameznikovo vedenje je lahko zaradi vpetosti v neko ožje družbeno okolje ali družbeno skupino v nasprotju s pravnimi merili in standardi širšega družbenega okolja. Oziroma, kakor ugotavljata Sampson in Jeglum Bartusch, posameznikovo zaznavanje določenih dejanj kot primernih ni nujno zaznavanje primerne vedenja s stališča širše družbe oziroma družbenih mehanizmov, kot sta npr. pravo in policija, ki uravnavata to področje (Sampson in Jeglum Bartusch, 1998: 782).

- **Hipoteza 2:** Izkušnja deviantnosti zvišuje toleriranje deviantnosti s strani posameznika.

Hipotezo lahko potrdim, saj je na podlagi opravljenih regresijskih analiz razvidno, da spremenljivka izkušnja deviantnosti statistično značilno pozitivno vpliva na spremenljivko toleriranje deviantnosti. To pomeni, da se z večanjem izkušnje deviantnosti večja tudi toleriranje deviantnosti oziroma, kakor ugotavlja Hindelang, da tisti posamezniki, ki niso bili udeleženi v deviantnih dejanjih, bolj neodobravajo deviantna dejanja v primerjavi s posamezniki, ki so bili udeleženi v deviantnih dejanjih vsaj enkrat (v Sampson in Jeglum Bartusch, 1998: 779).

8 ZAKLJUČEK

Različna dejanja posameznikov, ki so v nasprotju s početjem, ki ga drugi pripadniki družbe ocenjujejo kot sprejemljivega, so bila od vsega začetka rdeča nit moje diplomske naloge in prav zato se tudi v zaključni razpravi obračam na ta dejanja. Vander Zenden (1993: 129) ugotavlja, da si posamezniki v življenju ustvarjajo sodbe o zaželenih oziroma nezaželenih oblikah vedenja. Svoje sodbe pa nato prevedejo v ugodne oziroma neugodne posledice za tiste osebe, ki ta dejanja storijo. Katera pa so tista dejanja, ki so označena kot deviantna, pa močno variira glede na prostor, čas in družbeno skupino, ki ji posameznik pripada. Ko sociologi razpravljajo o normativnem vedenju, ugotavljajo, da družbene in pravne norme pogosto ne postavljajo jasne razmejitve med deviantnim in družbeno sprejemljivim vedenjem, torej, da med obema oblikama obstaja določena stopnja variacije (Williams v Vander Zenden, 1993: 131). To pa pomeni, da obstaja neke vrste siva cona, ki na eni strani pomeni še vedno določeno toleranco nekaterih dejanj posameznikov s strani družbenih institucij, na drugi strani pa le majhno odstopanje v vedenju od te t.i. sive cone že pomeni popolno netoleranco teh dejanj z vidika družbenih institucij. Posamezniki so torej ujeti v neke vrste zamejen svet, katerega mej pogosto ne poznajo dobro. To pomeni, da posamezniki pravnih omejitev družbe, v kateri živijo, pogosto ne zaznavajo na način, ki bi jim dal celovito sliko pravnega stanja družbene ureditve. Najsi gre tu za nepoznavanje pravnih norm s strani posameznika ali pa posamezniki zaradi vpetosti v določeno družbeno skupino zaznavajo norme te družbene skupine, ki so v neskladju s pravnim redom družbe, v kateri živijo. To nepoznavanje pravnih norm oziroma neskladje norm neke družbene skupine, ki ji posameznik pripada, s pravnimi normami družbe, v kateri živi, lahko povzroči, da posameznik določena deviantna dejanja sprejema kot popolnoma družbeno sprejemljiva.

Podobne tendence so se pokazale tudi na podlagi analize zbranih podatkov, kjer način, na katerega posameznik zaznava pravne norme, vpliva na posameznikovo sprejemanje ali zavračanje posameznih deviantnih dejanj. Posameznikovo vedenje je namreč zaradi vpetosti v neko ožje družbeno okolje ali družbeno skupino lahko v nasprotju s pravnimi merili in standardi širšega družbenega okolja, oziroma kakor ugotavljata Sampson in Jeglum Bartucsh, posameznikovo zaznavanje določenih dejanj kot

primernih ni nujno zaznavanje primernega vedenja s stališča širše družbe oziroma družbenih mehanizmov, kot sta npr. pravo in policija, ki uravnavata to področje (Sampson in Jeglum Bartucsh, 1998: 782).

Če se vrnem na nekatere sociološke vidike deviantnosti, kot je vidik Davida Matze, lahko ugotovim, da posamezniki določena nelegalna dejanja opravičujejo z različnimi tehnikami nevtralizacije. To pomeni, da posamezniki v primerih, ko določeno deviantno dejanje nevtralizirajo, pravnih norm ne zaznavajo na način, kot jim ga nalagajo centri državne in pravne oblasti, marveč na način, na katerega ta dejanja zaznavajo oni sami. Povedano drugače – posamezniki opravičujejo določena deviantna dejanja kot sprejemljiva, jih torej tolerirajo. Večja kot je torej stopnja nevtralizacije, bolj posamezniki opravičujejo svoja deviantna dejanja oziroma jih bolj zaznavajo kot družbeno sprejemljiva, saj se posamezniki začasno osvobodijo družbenega prijema, npr. z zanikanjem odgovornosti za določeno deviantno dejanje in zanikanjem škode, ki je posledica tega deviantnega dejanja (Matza v Haralambos in Holborn, 1999: 404–405).

Na drugi strani pa na posameznikovo toleriranje deviantnosti vplivajo tudi izkušnje, ki jih ima posameznik s posameznimi deviantnimi dejanji. Becker (1963: 25–34) je proučeval možne posledice na posameznika, ki je javno etiketiran kot deviantna oseba. Gre torej za posameznika, ki je že storil določeno deviantno dejanje in ki mu je na hrbet prilepljena etiketa deviant. Takšnega posameznika drugi pripadniki družbe vidijo, kot ga označuje etiketa, in praviloma predpostavljajo, da ima negativne značilnosti, ki so normalno povezane s takšno etiketo. Ker posameznikovo pojmovanje samega sebe v glavnem izvira iz odzivov drugih nanj, tudi posameznik samega sebe pojmuje z vidika etikete, kar lahko povzroči samoizpolnjujočo prerokbo, zaradi česar postane deviantna identifikacija usmerjevalna (Becker, 1963: 25–34). Posameznik, ki je že storil neko deviantno dejanje, je torej na nek način prisiljen, da prevzame to deviantno identiteto, kar nadalje pomeni, da je prisiljen v ponovno izvajanje deviantnih dejanj. Gre za neke vrste začaran krog. Posamezniku, ki je že storil neko deviantno dejanje, je na začetku prilepljena etiketa devianta, zaradi česar ga mnoge družbene skupine pa tudi prijatelji in družina zavračajo. To ponavadi posameznika prisili v to, da zapusti svoje bivalno okolje, kar lahko spodbudi nadaljnjo deviantnost, deviantna oseba pa mora zaradi uradnih postopkov do deviantnosti razviti nelegalne

postopke svojega delovanja. To pa nadalje vodi deviantno osebo v pridružitve določeni deviantni skupini, v kateri posamezniki potrdijo in sprejmejo svojo deviantno identiteto. Znotraj te deviantne skupine pa se razvije deviantna subkultura, ki pogosto vključuje prepričanja in vrednote, ki racionalizirajo, opravičujejo in podpirajo deviantne identitete in delovanja (Becker, 1963: 34–38). Posamezniki torej zaradi družbeno določenih etiket, ki so povezane z njihovimi izkušnjami deviantnosti, prevzemajo deviantne identitete ter nazadnje v sklopu vrednot, ki racionalizirajo, opravičujejo in podpirajo deviantne identitete in delovanja, deviantna dejanja tudi tolerirajo.

Podobne tendence so se pokazale tudi na podlagi analize zbranih podatkov, kar pomeni, da ima tudi posameznikova izkušnja deviantnosti določen vpliv na posameznikovo sprejemanje ali zavračanje deviantnih dejanj. Slednje ugotavlja v svoji raziskavi tudi Hindelang, in sicer, da tisti posamezniki, ki niso bili udeleženi v deviantnih dejanjih, pogosto ne odobravajo deviantnih dejanj v primerjavi s posamezniki, ki so bili udeleženi v deviantnih dejanjih vsaj enkrat (v Sampson in Jeglum Bartucsh, 1998: 779).

Ob koncu diplomske naloge želim poudariti, da predstavljen raziskovalni model ne vključuje vseh dejavnikov, ki morda vplivajo na zaznavanja deviantnega vedenja na internetu. V prihodnje bi bilo smiselno ugotoviti, kako (in če sploh) na toleriranje deviantnega vedenja s strani posameznika vplivajo tudi nekateri demografski dejavniki, ki v moji anketi niso bili zajeti (npr. velikost kraja bivanja, pogostost uporabe interneta, začetek uporabe interneta ipd.), ali pa kako na zaznavanje deviantnosti vplivajo množični mediji.

9 LITERATURA in VIRI

- Armstrong, H. L. in Forde, P. J. (2003): Internet anonymity practices in computer crime. *Information Management & Computer Security*. 11/5, str. 209–215.
- Bavcon, Ljubo, in drugi (1969): *Socialna patologija*. Mladinska knjiga, Ljubljana.
- Becker, Howard (1963): *Outsiders – Studies in the sociology of deviance*. Colloer-Macmillan Ltd., London.
- Durkheim, Emile (1969): *The Division of Labor in Society*. The Free Press, New York.
- Durkheim, Emile (1995): *Selected Writings*. Giddens, Anthony (ur). University Press, Cambridge.
- Fadaei – Tehrani, Reza in Green, Thomas M. (2002): Crime and Society. *International Journal of Social Economics*. Vol. 29, No. 10, str. 781–793.
- Fulcher, James in Scott, John (1999): *Sociology*. Oxford University Press, Oxford.
- Giddens, Anthony (2001): *Sociology*. Blackwell Publishers Ltd, Oxford.
- Haralambos, Michel in Holborn Martin (1999): *Sociologija – Teme in pogledi*. DZS, Ljubljana.
- Jeong-Yoo, Kim in Gang, Lee (2001): An Economic Theory of Deviance. *Journal of Institutional and Theoretical Economics*. Vol. 157, No. 4, str. 499–519.
- Kammeyer, Kenneth in dr. (1994): *Sociology*. Allyn in Bacon, Boston.
- (2004) Kazenski zakonik Republike Slovenije, Uradni list RS, št. 95, 27. 8. 2004.
- Kitchin, Rob (1998): *Cyberspace: The world in the wired wires*. John Wiley & Sons, Chichester.
- Littlejohn Shnider, Debra (2002): *Scene of the Cbercrime: Computer forensics Handbook*. Tittle, Ed (ur.). Syngress Publishing Inc. Rockland.
- Martonoši, Pavel (1993): »Kriminaliteta v zvezi z računalniki v novi slovenski kazenski zakonodaji«. *Podjetje in delo: revija za gospodarsko, delovno in socialno pravo*, št. 5/6, str. 489–500.

- Macionis, John J. (2005): *Sociology*. Pearson Prentice Hall, New Jersey.
- McCarthey, Bill (2002): New economics of sociological criminology. *Annual Rev. Sociol.*, 28, str. 417–442.
- Oblak, Tanja (2000): Mitske podobe o »življenju na mreži«: Od poljubnih identitet do izgubljenih skupnosti v kibernetskem prostoru. *Teorija in praksa*, let. 37, 6/2000, str. 1052–1068.
- O'Donnell, Gerard (1994): *Mastering Sociology*. The Macmillan Press Ltd, London.
- Pečar, Janez (1988): *Formalno nadzorstvo – Kriminološki in kriminalnopolitični pogledi*. Delavska enotnost, Ljubljana.
- Sampson, Robert J. in Jeglum Bartuchsh, Dawn (1998): Legal cynicism and (subcultural?) tolerance of deviance: The neighborhood context of racial differences. *Law and Society Review*, Vol. 32, No. 4, str. 777–804.
- Schwartz, Alan and Garfinkel, Simson (1998): *Stopping spam*. Sebastopol, O'Reilly & Associates, Inc., Beijing.
- Sharankova, Jeana (1999): Semiotic Aspects of the Transformation of Legal Systems. *AS/SA*, No. 6/7, str. 402–412.
- Seiber, Ulrich (1998): *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME - Study*. Prepared for the European Commission by University of Würzburg.¹⁵
- Streck, John (1998): PULLING THE PLUG ON ELECTRONIC TOWN MEETINGS v Tolouse in Luke (ur.) *The Politics of Cyberspace*, str. 18–47.
- Šercar, Tvrtno (2004): Kiberangelčki umazanega obraza. *Organizacija znanja*. Let. 9, zv. 1, str. 14–19.
- Trček, Franc (2003): Problem informacijske (ne)dostopnosti. *Zbirka Kiber 1*, Ljubljana.
- Vodušek, Mojca (1992): Računalniški kriminal. *Varnost – strokovni bilten*, št. ½, str. 110–117.
- Zupančič, Maja (1997): Kriminaliteta v globalni komunikacijski mreži (internet). *Revija za kriminalistiko in kriminologijo*, Let. 48, št. 2, str. 179–188.

¹⁵ Študijo sem dobila na nekdanjem Ministrstvu za informacijsko družbo v elektronski obliki.

- Vander Zanden, James W. (1993): Sociology: The core. McGraw-Hill Book Co., Singapore.
- Wall, S. David (2001): Crime and the internet. Routledge, London.
- (2004) Zakon o avtorski in sorodnih pravicah, Uradni list RS, št. 94, (26. 8. 2004).
- (2004) Zakon o kazenskem postopku, Uradni list RS, št. 96, (30. 8. 2004).
- (2004) Zakon o odgovornosti pravnih oseb za kazniva dejanja, Uradni list RS, št. 98, (9. 9. 2004).
- (2001) Zakon o telekomunikacijah, Uradni list RS, št. 30, (26. 4. 2001).
- (2004) Zakon o varstvu potrošnikov, Uradni list RS, št. 98, (9. 9. 2004).

Viri:

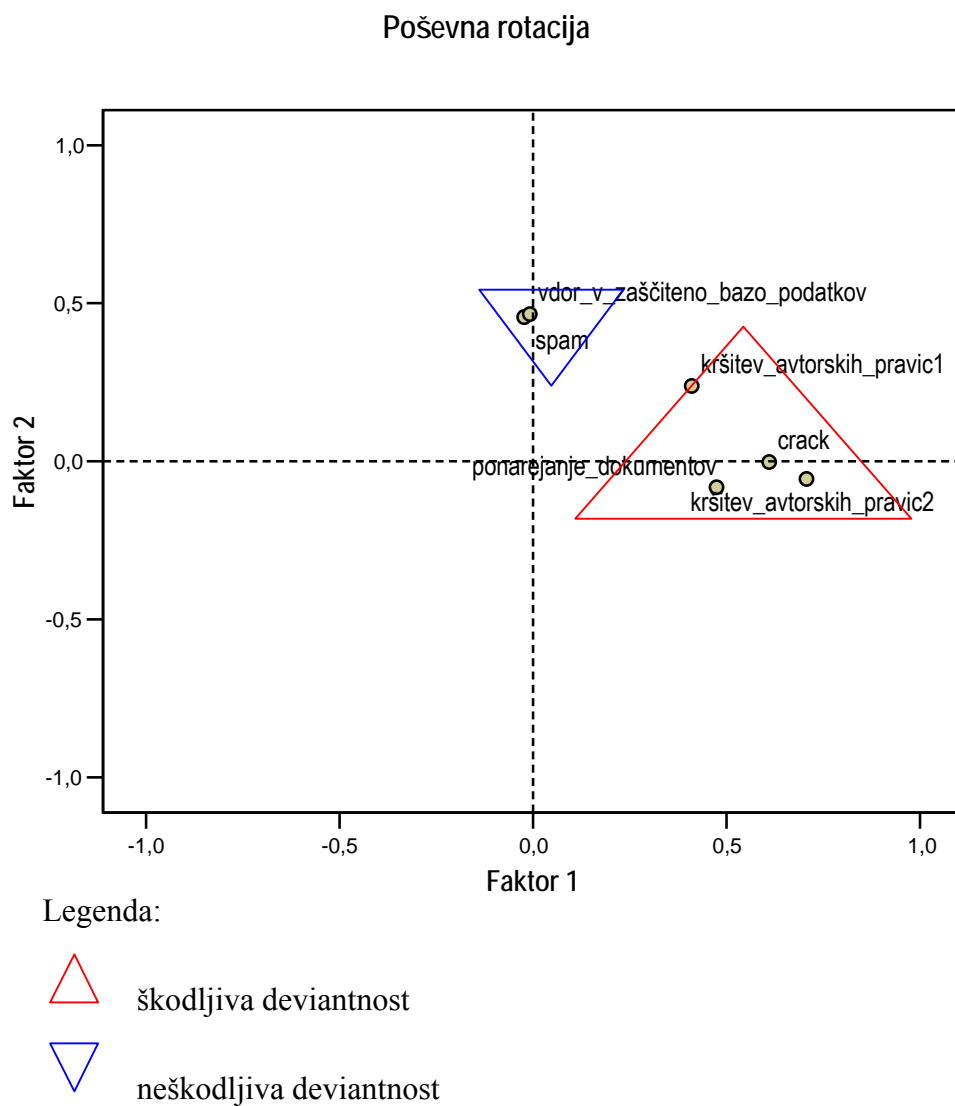
- Konvencija o kibernetiski kriminaliteti (2002), št. 792-03/2002-1, <http://mid.gov.si/mid/mid.nsf/konvencija-CyberCrime.pdf>, 30. 5. 2005.
- <http://mid.gov.si/mid/mid.nsf>, 30. 5. 2005.

10 PRILOGE

Priloga A - Statistična analiza - dodatek

Tabela 15: Korelacije med faktorji pri poševni rotaciji:

Faktor	1	2
1	1.000	0.073
2	0.073	1.000



Slika 14: Grafični prikaz faktorjev po poševni rotaciji

Tabela 16: Korelacijska matrika posameznih indikatorjev spremenljivke percepcija pravnih norm

	Če nekdo povzame del članka drugega avtorja in ga ne citira...ali je to dovoljeno?	Če nekdo "skopira" mesečno vozovnico in jo nato uporablja...ali je to zakonito?	Če nekdo "sname" film z interneta z namenom, da bi si ga ogledal...ali je to zakonito?	Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu...ali je to zakonito?	Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo...ali je to zakonito?	Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to...ali je to dovoljeno?
Če nekdo povzame del članka drugega avtorja in ga ne citira...ali je to dovoljeno?	1	0.094	0.007	0.105	-0.023	-0.001
Če nekdo "skopira" mesečno vozovnico in jo nato uporablja...ali je to zakonito?	0.094	1	0.023	0.001	-0.055	0.162**
Če nekdo "sname" film z interneta z namenom, da bi si ga ogledal...ali je to zakonito?	0.007	0.023	1	0.329**	0.083	-0.008
Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu...ali je to zakonito?	0.105	0.001	0.329**	1	0.122*	-0.050
Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo...ali je to zakonito?	-0.023	-0.055	0.083	0.122*	1	0.017
Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to...ali je to dovoljeno?	-0.001	0.162**	-0.008	-0.050	0.017	1

Tabela 17: Korelacijska matrika posameznih indikatorjev spremenljivke izkušnja deviantnosti

	Če nekdo povzame del članka drugega avtorja in ga ne citira...ali ste to že kdaj naredili?	Če nekdo "skopira" mesečno vozovnico in jo nato uporablja...ali ste to kdaj že naredili?	Če nekdo "sname" film z interneta z namenom, da bi si ga ogledal...ali ste to že kdaj naredili?	Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu...ali ste to že kdaj naredili?	Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo...ali ste to že kdaj naredili?	Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to...ali ste to že kdaj naredili?
Če nekdo povzame del članka drugega avtorja in ga ne citira...ali ste to že kdaj naredili?	1	0.006	0.038	0.084	0.010	0.025
Če nekdo »skopira« mesečno vozovnico in jo nato uporablja...ali ste to kdaj že naredili?	0.006	1	0.158**	0.048	0.115	0.125*
Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal...ali ste to že kdaj naredili?	0.038	0.158**	1	0.361**	0.096	0.077
Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu...ali ste to že kdaj naredili?	0.084	0.048	0.361**	1	0.114	0.129*
Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo...ali ste to že kdaj naredili?	0.010	0.115	0.096	0.114	1	0.236**
Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to...ali ste to že kdaj naredili?	0.025	0.125*	0.077	0.129*	0.236**	1

Tabela 18: Korelacijska matrika posameznih indikatorjev spremenljivke toleriranje deviantnosti

	Če nekdo povzame del članka drugega avtorja in ga ne citira...to ni tako problematično	Če nekdo "skopira" mesečno vozovnico in jo nato uporablja...to ni tako problematično	Če nekdo "sname" film z interneta z namenom, da bi si ga ogledal...to ni tako problematično	Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu...ni tako problematično	Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo...to ni tako problematično	Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to...to ni tako problematično
Če nekdo povzame del članka drugega avtorja in ga ne citira...to ni tako problematično	1	0.219***	0.270***	0.238***	0.082	0.104
Če nekdo »skopira« mesečno vozovnico in jo nato uporablja...to ni tako problematično	0.219***	1	0.302***	0.273***	-0.051	-0.029
Če nekdo »sname« film z interneta z namenom, da bi si ga ogledal...to ni tako problematično	0.270***	0.302***	1	0.461***	-0.007	-0.022
Uporaba serijskih števil računalniških programov, ki jih lahko najdemo na internetu...ni tako problematično	0.238***	0.273***	0.461***	1	0.027	0.003
Če nekdo pošlje isto elektronsko pošto 30 osebam, ki pošiljatelja ne poznajo...to ni tako problematično	0.082	-0.051	-0.007	0.027	1	0.196***
Če nekdo prebere elektronsko pošto druge osebe, ne da bi ta vedela za to...to ni tako problematično	0.104	-0.029	-0.022	0.003	0.196***	1

Priloga B - Členi kazenskega zakonika RS, ki neposredno ali posredno rešujejo vprašanje kibernetске kriminalitete

Neupravičeno prisluškovanje in zvočno snemanje

148. člen

(1) Kdor neupravičeno s posebnimi napravami prisluškuje pogovoru ali izjavi, ki mu nista namenjena, ali ju zvočno snema, ali kdor takšen pogovor ali takšno izjavo neposredno prenaša tretji osebi, ali ji takšen posnetek predvaja ali kako drugače omogoči, da se z njim neposredno seznaní, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

(2) Enako se kaznuje, kdor zvočno snema njemu namenjeno zaupno izjavo drugega brez njegove privolitve z namenom, da bi takšno izjavo zlorabil, ali kdor takšno izjavo neposredno prenaša tretji osebi ali ji takšen posnetek predvaja ali ji kako drugače omogoči, da se z njim neposredno seznaní.

(3) Če stori dejanje iz prvega ali drugega odstavka tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic ali poskusi to storiti, se kaznuje z zaporom od treh mesecev do petih let.

(4) Pregon za dejanje iz prvega odstavka tega člena se začne na predlog, za dejanje iz drugega odstavka pa na zasebno tožbo.

Neupravičeno slikovno snemanje

149. člen

(1) Kdor neupravičeno slikovno snema ali naredi slikovni posnetek drugega ali njegovih prostorov brez njegove privolitve in pri tem občutno poseže v njegovo zasebnost, ali kdor takšno snemanje neposredno prenaša tretji osebi ali ji takšen posnetek prikazuje ali ji kako drugače omogoči, da se z njim neposredno seznaní, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

(2) Če stori dejanje iz prejšnjega odstavka uradna oseba z zlorabo uradnega položaja ali uradnih pravic ali poskusi to storiti, se kaznuje z zaporom od treh mesecev do petih let.

(3) Pregon za dejanje iz prvega odstavka tega člena se začne na predlog.

Kršitev tajnosti občil

150. člen

(1) Kdor neupravičeno odpre tuje pismo, tujo brzojavko ali kakšno drugo tuje zaprto pisanje ali pošiljko, se kaznuje z denarno kaznijo ali z zaporom do šestih mesecev.

(2) Z denarno kaznijo ali z zaporom do enega leta se kaznuje:

1) kdor se z uporabo tehničnih ali kemičnih sredstev, ne da bi odprl tuje pismo, tujo brzojavko ali kakšno drugo tujo zaprto pošiljko, neupravičeno seznanil z njihovo vsebino;

2) kdor se z uporabo tehničnih sredstev neupravičeno seznanil s sporočilom, ki se prenaša po telefonu ali s kakšnim drugim telekomunikacijskim sredstvom;

3) kdor neupravičeno odpre zaprt predmet, ki varuje sporočilo, in se neupravičeno seznanil s sporočilom v njem.

(3) Enako se kaznuje, kdor s katerim izmed dejanj, ki so navedena v prvem in drugem odstavku tega člena, omogoči drugemu, da se neposredno seznanil z vsebino sporočila ali pošiljke.

(4) Kdor neupravičeno obdrži, skrije, uniči ali komu drugemu izroči tuje pismo, brzojavko ali kakšno drugo pošiljko, preden se je prejemnik seznanil z njeno vsebino, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, poštni ali drug delavec, ki mu je zaupano prevzemanje, prenos ali predaja tujih pisem, tujih brzojavk ali kakšnih drugih pisanj ali pošiljk, se kaznuje z zaporom od treh mesecev do petih let.

(6) Pregon za dejanja iz prvega do četrtega odstavka tega člena se začne na predlog.

Nedovoljena objava zasebnih pisanj

151. člen

- (1) Kdor brez dovoljenja pooblaščen osebe v primerih, kadar je tako dovoljenje potrebno, objavi dnevnik, pismo ali kakšno drugo zasebno pisanje, se kaznuje z denarno kaznijo ali z zaporom do enega leta.
- (2) Pregon se začne na zasebno tožbo.

Zloraba osebnih podatkov

154. člen

- (1) Kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali z zaporom do enega leta.
- (2) Enako se kaznuje, kdor vdre v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.
- (3) Če stori dejanje iz prvega ali drugega odstavka tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let.

Kršitev avtorske pravice

158. člen

- (1) Kdor s svojim imenom ali z imenom koga drugega objavi, prikaže, izvede ali prenese tuje avtorsko delo ali njegov del, ali dovoli to storiti, se kaznuje z denarno kaznijo ali z zaporom do enega leta.
- (2) Kdor skazi, okrni ali kako drugače neupravičeno poseže v tuje avtorsko delo, se kaznuje z denarno kaznijo ali z zaporom do šestih mesecev.
- (3) Pregon se začne na predlog.

Neupravičena uporaba avtorskega dela

159. člen

- (1) Kdor neupravičeno uporabi eno ali več avtorskih del ali njihovih primerkov, katerih skupna tržna cena pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let.
- (2) Če tržna cena avtorskih del iz prejšnjega odstavka pomeni veliko premoženjsko vrednost, se storilec kaznuje z zaporom do petih let.
- (3) Če je bila z dejanjem iz prvega ali drugega odstavka tega člena pridobljena velika protipravna premoženjska korist in je šlo storilcu za to, da sebi ali komu drugemu pridobi takšno premoženjsko korist, se kaznuje z zaporom od enega do osmih let.
- (4) Primerki avtorskih del in naprave za njihovo reproduciranje se vzamejo.

Kršitev avtorski sorodnih pravic

160. člen

- (1) Kdor neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, RTV oddaj ali podatkovnih baz, katerih skupna tržna cena pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let.
- (2) Kdor neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, RTV oddaj ali podatkovnih baz, katerih skupna tržna cena pomeni veliko premoženjsko vrednost, se kaznuje z zaporom do petih let.
- (3) Če je bila z dejanjem iz prvega ali drugega odstavka tega člena pridobljena velika protipravna premoženjska korist in je šlo storilcu za to, da sebi ali komu drugemu pridobi takšno premoženjsko korist, se kaznuje z zaporom od enega do osmih let.
- (4) Primerki izvedb, fonogramov, videogramov, RTV oddaj ali podatkovnih baz in naprave za njihovo reproduciranje se vzamejo.

Prikazovanje, izdelava, posest in posredovanje pornografskega gradiva

187. člen

- (1) Kdor osebi, mlajši od štirinajst let, proda, prikaže ali z javnim razstavljanjem ali kako drugače omogoči, da so ji dostopni spisi, slike, avdiovizualni ali drugi predmeti pornografske vsebine, ali ji prikaže pornografsko predstavo, se kaznuje z denarno kaznijo ali zaporom do dveh let.
- (2) Kdor zlorabi mladoletno osebo za izdelavo slik, avdiovizualnih ali drugih predmetov pornografske vsebine, ali jo uporabi za pornografsko predstavo, se kaznuje za zaporom od šestih mesecev do petih let.
- (3) Enako se kaznuje kdor proizvede, razširi, proda, uvozi, izvozi ali drugače ponudi pornografsko gradivo, ki prikazuje mladoletne osebe, ali kdor poseduje tako gradivo z namenom proizvodnje, razširjanja, prodaje, uvoza, izvoza ali drugačnega ponujanja.
- (4) Če je bilo dejanje iz drugega ali tretjega odstavka tega člena storjeno v hudodelski združbi za izvrševanje takih kaznivih dejanj, se storilec kaznuje z zaporom od enega do osmih let.
- (5) Pornografski material iz drugega, tretjega in četrtega odstavka tega člena se vzame ali njegova uporaba ustrezno onemogoči.

Tatvina

211. člen

- (1) Kdor vzame komu tujo premično stvar z namenom, da si jo protipravno prilasti, se kaznuje z zaporom do treh let.
- (2) Če je vrednost ukradene stvari majhna in je šlo storilcu za to, da si prilasti stvar take vrednosti, se kaznuje z denarno kaznijo ali z zaporom do enega leta.
- (3) Pregon za dejanje iz prejšnjega odstavka se začne na predlog.
- (4) Če je storilec vrnil oškodovancu ukradeno stvar, preden je zvedel, da je uveden kazenski postopek, se mu sme kazen odpustiti.

Velika tatvina

212. člen

(1) Storilec tatvine iz prvega odstavka prejšnjega člena se kaznuje z zaporom do petih let:

- 1) če je storil tatvino tako, da je z vlomom, vdorom ali z drugačnim premagovanjem večjih ovir prišel v zaprto stavbo, sobo, blagajno, omaro ali v druge zaprte prostore;
- 2) če je storilo tatvino dvoje ali več oseb, ki so se združile zato, da bi kradle;
- 3) če je storil tatvino na posebno predrzen način;
- 4) če je imel pri sebi kakšno orožje ali nevarno orodje za napad ali obrambo;
- 5) če je storil tatvino ob požaru, povodnji ali podobni naravni nesreči;
- 6) če je storil tatvino tako, da je izrabil nemoč ali nesrečo drugega.

(2) Enako se kaznuje storilec tatvine, če je ukradena stvar posebnega kulturnega ali zgodovinskega pomena ali naravna vrednota ali če je ukradena stvar velike vrednosti in je šlo storilcu za to, da si prilasti takšno stvar ali stvar take vrednosti.

(3) Če je bila z dejanjem iz prvega odstavka tega člena pridobljena stvar posebnega kulturnega ali zgodovinskega pomena ali stvar velike vrednosti in je šlo storilcu zato, da si prilasti takšno stvar ali stvar take vrednosti, se kaznuje z zaporom od enega do osmih let.

Goljufija

217. člen

(1) Kdor z namenom, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist, spravi koga z lažnivim prikazovanjem ali prikrivanjem dejanskih okoliščin v zмотo ali ga pusti v zmoti in ga s tem zapelje, da ta v škodo svojega ali tujega premoženja kaj stori ali opusti, se kaznuje z zaporom do treh let.

(2) Če je storilec z dejanjem iz prejšnjega odstavka povzročil veliko premoženjsko škodo, se kaznuje z zaporom od enega do osmih let.

(3) Če je z dejanjem iz prvega odstavka tega člena povzročena majhna premoženjska škoda in je šlo storilcu za to, da pridobi majhno premoženjsko korist, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

(4) Kdor z namenom, da bi drugega oškodoval spravi koga z lažnim prikazovanjem ali prikrivanjem dejanskih okoliščin v zмотo ali ga pusti v zmoti in ga s tem zapelje, da ta v škodo svojega ali tujega premoženja kaj stori ali opusti, se kaznuje z denarno kaznijo ali zaporom do enega leta.

(5) Pregon za dejanje iz tretjega in četrtega odstavka tega člena se začne na predlog.

Neupravičen vstop v informacijski sistem

225. člen

(1) Kdor neupravičeno vstopi v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v ali iz informacijskega sistema, se kaznuje z denarno kaznijo.

(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

(3) Poskus dejanja iz prejšnjega odstavka je kazniv.

(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

Ponareditev ali uničenje poslovnih listin

240. člen

(1) Kdor v poslovne knjige, spise ali druge poslovne listine, ki jih mora voditi po zakonu ali na podlagi drugih predpisov, izdanih na podlagi zakona, in so pomembne za poslovni promet z drugimi pravnimi ali fizičnimi osebami ali so namenjene za odločitve v zvezi z gospodarsko ali finančno dejavnostjo, vpiše lažne podatke ali ne vpiše kakšnega pomembnega podatka, ali s svojim podpisom potrdi takšno knjigo, listino ali spis z lažno vsebino ali omogoči sestavo knjige, listine ali spisa z lažno vsebino, se kaznuje z zaporom do dveh let.

(2) Enako se kaznuje, kdor lažno poslovno knjigo, listino ali spis uporabi kot resnično ali kdor uniči, skrije, precej poškoduje ali kako drugače napravi nerabne poslovne knjige, listine ali spise iz prejšnjega odstavka.

(3) Poskus dejanj iz prvega in drugega odstavka tega člena je kazniv.

Vdor v informacijski sistem

242. člen

(1) Kdor pri gospodarskem poslovanju neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen svoj podatek, ovira prenos podatkov ali delovanje informacijskega sistema, ali kako drugače vdre v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let.

(2) Če je bila z dejanjem iz prejšnjega odstavka pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda in je šlo storilcu za to, da sebi ali komu drugemu pridobi tako premoženjsko korist ali drugemu povzroči tako premoženjsko škodo, se kaznuje z zaporom do petih let.

Ponarejanje denarja

249. člen

(1) Kdor napravi kriv denar z namenom, da bi ga spravil v obtok kot pravega, ali kdor predrugači pravi denar z namenom, da bi ga spravil v obtok, ali kdor tak ponarejen denar spravi v obtok, se kaznuje z zaporom od šestih mesecev do osmih let.

(2) Enako se kaznuje, kdor si preskrbi ponarejen denar z namenom, da bi ga spravil v obtok kot pravega.

(3) Če zaradi dejanja iz prvega ali drugega odstavka tega člena nastanejo motnje v gospodarstvu države, se storilec kaznuje z zaporom od enega do desetih let.

(4) Kdor da v obtok ponarejen denar, ki ga je prejel kot pravega, ali kdor ve, da je bil denar ponarejen ali da je bil tak denar spravljen v obtok, pa tega ne naznani, se kaznuje z denarno kaznijo ali z zaporom do šestih mesecev.

(5) Ponarejeni denar se vzame.

Ponarejanje in uporaba ponarejenih vrednotnic ali vrednostnih papirjev

250. člen

- (1) Kdor napravi kolke ali poštne znamke ali druge krive vrednotnice, ali kdor predružači kakšno tako pravo vrednotnico z namenom, da bi jo uporabil kot pravo ali jo dal v uporabo komu drugemu, ali kdor ponarejene vrednotnice uporabi kot prave ali si jih s tem namenom pridobi, se kaznuje z zaporom do treh let.
- (2) Če so vrednotnice iz prejšnjega odstavka velike vrednosti, se storilec kaznuje z zaporom od šestih mesecev do petih let.
- (3) Kdor napravi krive vrednostne papirje, ali kdor predružači kakšen tak pravi vrednostni papir z namenom, da bi ga uporabil kot pravega ali ga dal v uporabo komu drugemu, ali kdor take ponarejene vrednostne papirje uporabi kot prave ali jih s tem namenom pridobi, se kaznuje z zaporom od enega do osmih let.
- (4) Če zaradi dejanja iz prejšnjega odstavka nastanejo motnje v gospodarstvu države, se storilec kaznuje z zaporom od enega do desetih let.
- (5) Kdor odstrani žig, s katerim se vrednotnice iz prvega odstavka tega člena uničujejo, ali kdor si kako drugače prizadeva napraviti te vrednotnice, kakor da ne bi bile uporabljene, ali kdor že uporabljene take vrednotnice znova uporabi ali proda, kakor da bi bile veljavne, se kaznuje z denarno kaznijo ali z zaporom do enega leta.
- (6) Ponarejene vrednotnice in ponarejeni vrednostni papirji se vzamejo.

Ponarejanje listin

256. člen

- (1) Kdor napravi krivo listino ali predružači pravo listino z namenom, da bi se taka lista uporabila kot prava, ali kdor krivo ali predružačeno listino uporabi kot pravo, se kaznuje z zaporom do dveh let.
- (2) Poskus je kazniv.
- (3) Kdor napravi krivo javno listino, oporoko, javno ali uradno knjigo ali kakšno drugo knjigo, ki se mora voditi na podlagi zakona, predružači tako pravo listino ali kdor tako krivo ali predružačeno listino spravi v obtok ali hrani z namenom uporabe ali jo uporabi kot pravo, se kaznuje z zaporom do treh let.

Posebni primeri ponarejanja listin

257. člen

Za ponarejanje listin se kaznuje po določbah prejšnjega člena:

- 1) kdor kakšen papir, golico ali kakšno drugo listino, ki jo je kdo podpisal, neupravičeno izpolni s kakšno izjavo, ki ima pomen za pravna razmerja;
- 2) kdor koga preslepi o vsebini kakšne listine in jo ta podpiše, misleč, da se podpisuje pod kakšno drugo listino ali pod kakšno drugo vsebino;
- 3) kdor izda listino v imenu kakšne osebe brez njenega pooblastila ali v imenu osebe, ki je ni;
- 4) kdor kot izdajatelj listine doda k svojemu podpisu kakšen položaj ali naziv, čeprav nima takega položaja ali naziva, pa to bistveno vpliva na dokazilno moč listine;
- 5) kdor napravi listino tako, da neupravičeno uporabi pravi pečat ali znamenje.

Ponarejanje znamenj za zaznamovanje blaga, mer in uteži

260. člen

- (1) Kdor z namenom, da bi jih uporabil kot prave, napravi kriva znamenja za zaznamovanje domačega ali tujega blaga, kakor so pečati, žigi, znamke ali druge predpisane označbe, s katerimi se zaznamuje zlato, srebro, živina, les ali kakšno drugo blago, ali prava taka znamenja predrugači ali odstrani, ali kdor uporabi ponarejena znamenja kot prava, se kaznuje z denarno kaznijo ali z zaporom do dveh let.
- (2) Enako se kaznuje, kdor ponaredi mere ali uteži, ali kdor jih uporabi pri merjenju kot prave.
- (3) Kdor neupravičeno izdelava, si pridobi, proda ali da v uporabo pripomočke za izdelovanje znamenj za zaznamovanje ali označevanje blaga, kakor tudi krivih mer in uteži, se kaznuje z zaporom do enega leta.
- (4) Ponarejena znamenja, mere in uteži, kakor tudi pripomočki za njihovo ponarejanje se vzamejo.

Zloraba uradnega položaja ali uradnih pravic

261. člen

(1) Uradna oseba, ki z namenom, da bi sebi ali komu drugemu pridobila kakšno nepremoženjsko korist ali da bi komu prizadejala škodo, izrabi svoj uradni položaj ali prestopi meje uradnih pravic ali ne opravi uradne dolžnosti, se kaznuje z zaporom do enega leta.

(2) Če storilec z dejanjem iz prejšnjega odstavka povzroči večjo škodo ali huje prekrši pravice drugega, se kaznuje z zaporom do treh let.

(3) Uradna oseba, ki z namenom, da bi sebi ali komu drugemu pridobila protipravno premoženjsko korist, izrabi svoj uradni položaj ali prestopi meje uradnih pravic, ali ne opravi uradne dolžnosti, pa pri tem niso podani znaki drugega kaznivega dejanja, se kaznuje z zaporom od treh mesecev do petih let.

(4) Če je storilec z dejanjem iz prejšnjega odstavka pridobil veliko protipravno premoženjsko korist in mu je šlo za to, da si pridobi tako korist, se kaznuje z zaporom od enega do osmih let.

Ponareditev ali uničenje uradne listine, knjige ali spisa

265. člen

(1) Uradna oseba, ki v uradno listino, knjigo, ali spis vpiše lažne podatke, ali ne vpiše kakšnega pomembnega podatka, ali s svojim podpisom oziroma pečatom potrdi uradno listino, knjigo ali spis z lažno vsebino, ali s svojim podpisom oziroma uradnim pečatom omogoči sestavo uradne listine, knjige ali spisa z lažno vsebino, se kaznuje z zaporom do treh let.

(2) Enako se kaznuje tudi uradna oseba, ki uradno listino, knjigo ali spis z lažno vsebino uporabi v službi kot resnične ali ki uradno listino, knjigo ali spis uniči, skrije, jih precej poškoduje ali kako drugače napravi nerabne.

Izdaja uradne tajnosti

266. člen

(1) Uradna oseba ali druga oseba, ki v nasprotju s svojimi dolžnostmi varovanja uradne tajnosti sporoči ali izroči komu podatke, ki so uradna tajnost, ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke z namenom, da jih izroči nepoklicani osebi, se kaznuje z zaporom do treh let.

(2) Enako se kaznuje, kdor z namenom, da jih neupravičeno uporabi, na protipraven način pride do podatkov, ki se varujejo kot uradna tajnost, kakor tudi kdor take podatke brez dovoljenja javno objavi.

(3) Če je dejanje iz prvega odstavka tega člena storjeno iz koristoljubnosti ali z namenom objave ali uporabe podatkov v tujini, se storilec kaznuje z zaporom do petih let.

(4) Če je dejanje iz prvega odstavka tega člena storjeno iz malomarnosti, se storilec kaznuje z zaporom do enega leta.

(5) Ne glede na določbe drugega odstavka tega člena se ne kaznuje, kdor uradno tajnost, katere vsebina je v nasprotju z ustavnim redom Republike Slovenije, posreduje za objavo ali objavi z namenom, da javnosti razkrije nepravilnosti pri organiziranju, delovanju in vodenju službe, če objava za državo nima škodljivih posledic.

(6) Za uradno tajnost se štejejo podatki, ki so z zakonom, z drugim predpisom, splošnim aktom ali s sklepom pristojnega organa, ki so izdani na podlagi zakona, razglašeni za uradno tajnost in so tako pomembni, da so z njihovo izdajo nastale ali bi lahko nastale hujše škodljive posledice za službo.

Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje

309. člen

(1) Kdor orožje, razstrelilne snovi ali pripomočke, s katerimi se lahko napravijo, ali strupe, za katere ve, da so namenjeni za kaznivo dejanje, izdelata ali si jih pridobi ali jih hrani ali komu omogoči, da pride do njih, se kaznuje z zaporom do treh let.

(2) Kdor napravi ali komu odstopi ponarejen ključ, odpirač ali kakšen drug pripomoček za vlom, čeprav ve, da je namenjen za kaznivo dejanje, se kaznuje z zaporom do enega leta.

(3) Enako se kaznuje, kdor z namenom izvršitve kaznivega dejanja poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali na drug način zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem.

Priloga C - Povzetek konvencije o kibernetiski kriminaliteti

»Konvencija o kriminalu v kibernetnem prostoru celovito obravnava kazenskopravno problematiko v kibernetnem prostoru, ki se je v preteklih letih, zaradi posameznih temeljnih značilnosti modernih informacijsko komunikacijskih tehnologij (IKT), še posebej pa interneta, razvila v povsem specifično vejo kazenskega prava. Specifično zato, ker zaradi nekaterih temeljnih značilnosti modernih IKT, predvsem pa zaradi izjemne anonimnosti in geografske nedoločnosti interneta ter hitrosti prenosa in vsakršne obdelave podatkov, kaznivih dejanj v tem (beri: kibernetnem) prostoru, ni več moč ustrezno preganjati s sedanjimi kazenskopravnimi instituti. Z vidika pregona kaznivih dejanj v kibernetnem prostoru je nujno potrebno zagotoviti predvsem dvoje: spremembo, dopolnitev in prilagoditev veljavne kazenske materialne in procesne zakonodaje ter zagotovitev ustreznih instrumentov za hitro in učinkovito mednarodno sodelovanje, ki so zaradi geografske nedoločnosti interneta, še posebej ključnega pomena. Konkretnih rešitev omenjene problematike sama konvencija sicer ne določa, daje pa državam podpisnicam dovolj natančne in konkretne smernice, glede bodoče ureditve na področju kriminala v kibernetnem prostoru. Z vidika Slovenije to pomeni, da bo, v kolikor bo konvencijo podpisala in ratificirala, v skladu s sedaj veljavno ustavno ureditvijo, pri sprejemanju vsakršnih ukrepov na področju kriminala v kibernetnem prostoru, zavezana področje urediti v skladu z določbami konvencije (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Konvencija je vsebinsko razdeljena na štiri poglavja: v prvem je opredeljen pomen nekaterih, za razumevanje konvencije ključnih izrazov, drugo poglavje kompleksno obravnava tako materialno kot procesno kazenskopravno problematiko, tretje precej

natančno opredeljuje posamezne smernice mednarodnega sodelovanja, končne določbe v četrtem delu pa določajo modalitete podpisa, sprejema in veljavnosti konvencije (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Ker terminologija na omenjenem področju ni mednarodno usklajena, kar utegne zaradi podobnosti izrazov, ki lahko v posameznih primerih označujejo povsem različne zadeve, povzročati zmedo in negotovost, je za zagotovitev enakega razumevanja na določila konvencije, potrebno natančno določiti pomen posameznih ključnih pojmov, čemur je namenjeno prvo poglavje. Tovrstna fiksacija učinkuje predvsem kot varovalni instrument, ki naj onemogoči "frauduloznost" s strani pogodbenic pri udejanjanju določil konvencije. Tako so v prvem poglavju natančno definirani pojmi računalniškega sistema, računalniških podatkov, ponudnika storitev in podatkov v prometu (1. člen) (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Drugo poglavje se nanaša na ukrepe, ki jih je potrebno sprejeti na nacionalni ravni in je smiselno razdeljeno na dva oddelka; prvi obravnava kazensko materialno, drugi pa kazensko procesno problematiko. Kazensko materialni del opredeljuje posamezna kazniva dejanja, ki morajo biti v luči konvencije inkriminirana, pri čemer način inkriminacije prepušča podpisnicam. Države podpisnice lahko pregon zagotovijo bodisi z že veljavno zakonodajo, v kolikor le-ta slednje dopušča, bodisi s spremembo veljavne zakonodaje, bodisi na področju kriminalitete v kibernetnem prostoru posebej uredijo. Države podpisnice se skratka zavezujejo, da je na njihovem ozemlju zagotovljen pregon za vsa kazniva dejanja, opredeljena v prvem oddelku drugega poglavja konvencije. Smiselno lahko kazniva dejanja v konvenciji razdelimo na štiri sklope: kazniva dejanja zoper zaupnost, integriteto in dostopnost računalniških podatkov in sistemov med katera sodijo vdor v računalniški sistem, protipravno prestrezanje in motenje podatkov in sistemov ter zloraba naprav (2. – 6. člen); kazniva dejanja, povezana z samim računalnikom kot sta računalniško ponarejanje in računalniška goljufija (7. in 8. člen); kazniva dejanja, povezana s prenašano vsebino med katerimi gotovo izstopajo kazniva dejanja povezana z otroško pornografijo (9. člen) in kazniva dejanja povezana s kršitvijo avtorske in njej sorodnih pravic (10. člen) (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Konvencija tudi posebej določa odgovornost za poskus, pomoč ali napeljevanje k omenjenim kaznivim dejanjem, odgovornost pravnih oseb in okvirne smernice sankcioniranja v konvenciji opredeljenih kaznivih dejanj (11. – 13. člen) (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Oddelek, ki obravnava kazensko procesno problematiko, je precej pomembnejši od materialnega, saj, medtem ko je na eni strani veliko večino v konvenciji opredeljenih kaznivih dejanj moč preganjati v okviru veljavne kazenske materialne zakonodaje, so po drugi strani sedaj veljavne določbe kazenskega postopka, ki se nanašajo na preiskovanje, zagotavljanje, zaseg podatkov in dokumentov, zaradi izjemne hitrosti prenosa in obdelave vsakršnih računalniških podatkov, neprimerne za analogno uporabo v kibernetnem prostoru. Procesno gledano gre za povsem nov sklop posebnih metod in sredstev, ki jih je v luči pregona kaznivih dejanj v kibernetnem prostoru potrebno zagotoviti, pri čemer pa je potrebno seveda vsaj enako pozornost posvetiti varovalnim instrumentom, ki bodo kar seda učinkovito onemogočili njihovo zlorabo. Kazensko procesne določbe lahko tako razdelimo na: splošne, ki od države podpisnice zahtevajo določitev pristojnih organov in postopkov, kazniva dejanja iz materialnega dela, na katera se morajo nanašati ter spoštovanje človekovih pravic in temeljnih svoboščin, v skladu z veljavno zakonodajo in sprejetimi mednarodnimi obveznostmi s tega področja (14. in 15. člen); določbe, ki opredeljujejo hitro zagotavljanje in razkrivanje računalniško shranjenih podatkov in so v luči omenjenih značilnosti kibernetnega prostora, še posebej ključnega pomena (16. in 17. člen); določbe, ki se nanašajo na zahtevanje, preiskovanje in zaseg računalniško shranjenih podatkov (18. in 19. člen); določbe glede zbiranja računalniških podatkov v dejanskem času (20. in 21. člen) in določbe, ki opredeljujejo nekatere smernice za določitev sodne pristojnosti (22. člen) (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Mednarodno sodelovanje, ki ga obravnava tretje poglavje konvencije je v luči omenjenih temeljnih značilnosti kibernetnega prostora, še posebej ključnega pomena. Zaradi njegove anonimnosti in geografske nedoločnosti države pogosto trčijo ob meje svoje jurisdikcije, kar jim v praksi, v odsotnosti ustreznih mednarodnih sporazumov, onemogoča učinkovit pregon kaznivih dejanj v kibernetnem prostoru in kaznovanje storilcev. Določila konvencije so uperjena prav v odpravljanje te problematike, z velikim poudarkom na poglobljenem in precej natančno opredeljenem mednarodnem

sodelovanju, predvsem pa hitri in učinkoviti vzajemni pomoči med državami podpisnicami. Poglavje lahko razdelimo na naslednje sklope: temeljna načela mednarodnega sodelovanja (23. člen); načela, povezana z izročitvijo (24. člen); določbe, povezane z vzajemno pomočjo, ki jih lahko razdelimo na načela vzajemne pomoči (25. in 26. člen), postopke v zvezi z vzajemno pomočjo (27. in 28. člen) ter posebne določbe glede vzajemne pomoči pri začasnih ukrepih (29. in 30. člen) in glede preiskovalnih pristojnosti (31. – 34. člen) in določbe, ki se nanašajo na neprestano (24 ur na dan in 7 dni na teden) in učinkovito delovanje omrežja (35. člen) (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).

Zadnje (četrt) poglavje je namenjeno končnim določbam in določa modalitete podpisa (36. člen), pristopa (37. člen), teritorialne uporabe (38. člen), učinkov (39. člen) in odpovedi konvencije (47. člen), kakor tudi obsega in dopustnosti uporabe pridržkov (42. in 43. člen), deklaracij (40. člen) in amandmiranja konvencije (44. člen). Posebej zanimiva je morda le federalna klavzula (41. člen), ki v okviru končnih določb deluje kot nekakšen tujek, kar gre najbrž pripisati dejstvu, da je bila konvencija sprejeta na pobudo Združenih držav Amerike v luči dogodkov 11. septembra 2001, ki kot »federalna« država najbrž nočejo pregloboko poseči v kazenskopravne specifike posameznih zveznih držav. Končne določbe vsebujejo tudi nekatera načela reševanja sporov med strankami in določila namenjena posvetovanju med pogodbenicami (45. in 46. člen)« (<http://mid.gov.si/mid/mid.nsf>, 30.5.2005).