

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Barbara Kuhar

**ODNOS DO VARNE UPORABE INTERNETA :
primerjava med evropskimi državami**

Diplomsko delo

Ljubljana 2007

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Barbara Kuhar

Mentor: asist. dr. Matej Kovačič

**ODNOS DO VARNE UPORABE INTERNETA:
primerjava med evropskimi državami**

Diplomsko delo

Ljubljana 2007



IZJAVA O AVTORSTVU diplomskega dela

Spodaj podpisani/-a BARBARA KUCHAR, z vpisno številko 21019363,
rojen/-a 08.07.1983 v kraju PTUJ, sem avtor/-ica diplomskega dela z naslovom:
ODNOS DO VARNOSTI UPORABE INTERNETA :
PRIMERJAVA MED EVROPSKIMI DRŽAVAMI

S svojim podpisom zagotavljam, da:

- je predloženo diplomsko delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel/-a, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel/-a, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil/-a vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisal/-a v predloženem delu;
- se zavedam, da je plagiatstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu in sorodnih pravicah, Uradni list RS št. 21/95), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo diplomskega dela v zbirki »Dela FDV«.

V Ljubljani, dne 4. 9. 2007

Podpis avtorja/-ice: Kuchar B.

ODNOS DO VARNE UPORABE INTERNETA: primerjava med evropskimi državami

Širjenje in uporaba novih tehnologij v evropskih državah sta še vedno v porastu; zato pri vseh ugodnostih in prednostih, ki nam jih ta napredna tehnologija prinaša, ne smemo pozabiti na negativne lastnosti, na nevarnosti in zlorabe, ki se lahko ob uporabi pojavijo. Informacijska družba se širi na vse aspekte družbenega in ekonomskega življenja, zato je potrebno pod drobnogled vzeti ne samo razvoj tehnološke infrastrukture, temveč tudi vpliv na posameznike. Kot smo si ljudje med seboj različni, so tudi države vsaj tako, ali nemara celo bolj kompleksne; zato bomo med seboj primerjali dobljene rezultate v zvezi z odnosom do varne uporabe interneta. Osredotočili se bomo predvsem na vprašanja zavedanja nevarnosti, ki smo jih lahko ob uporabi interneta deležni; na zaskrbljenost nad varnostjo, zasebnostjo in zaupnostjo podatkov, ki se prenašajo preko interneta; in nenazadnje tudi, na pripravljenost (anonimne ali javne) prijave kršitve, v kolikor bi do le-te prišlo. Za lažje razumevanje, kaj je sploh (ne)varna uporaba interneta, pa bomo predstavili tudi potencialne nevarnosti, s katerimi se ob uporabi lahko srečamo.

Ključne besede: uporaba interneta, varnost, prijava kršitev, Evropa, mednarodna analiza.

ATTITUDE TO SAFE USE OF INTERNET: comparing European countries

In European countries the use of new technologies is still growing. Even though it brings us many benefits, we have to be aware of its negative sides, of dangers and misuses, which can emerge during our use. Information society is broadening on all aspects of social and economic life and that is one of the reasons why we have to consider not only technological infrastructures, but influence on individuals too. Likewise people differ from each other, the states are maybe even more complex, so we will be comparing collected results in considering relation to safe use of Internet. We will focus mostly on questions of realizing dangers, which we can be exposed to during use of Internet; on concerning about security, privacy and confidentiality of data, that is transferred on Internet; and never the less about readiness of (anonymous or public) reporting of violations, if they emerge. For easier understanding, what (un)safe use of the internet is, we will also define potential dangers, which we can encounter while using Internet.

Key words: Internet use, safety, reporting violations, Europe, multinational analysis.

KAZALO

1. UVOD	5
2. OSNOVNI POGOJI ZA VZPOSTAVITEV (KRITIČNEGA) ODNOSA DO (VARNE) UPORABE INTERNETA	7
3. OPREDELITEV (NE)VARNE UPORABE INTERNETA	9
3.1 Nadloge na internetu	9
3.1.1 Vohunsko programje	9
3.1.2 Oglaševalska programska oprema	10
3.1.3 Parazitsko programje	10
4. ZNAČILNOSTI IN AKTIVNOSTI EVROPSKIH DRŽAV	11
4.1 Bolgarija	11
4.2 Češka	14
4.3 Estonija	16
4.4 Latvija	20
4.5 Litva	21
4.6 Madžarska	22
4.7 Poljska	25
4.8 Romunija	26
4.9 Slovaška	27
4.10 Slovenija	29
5. SKRIB ZA VARNOST	31
6. METODOLOGIJA	33
6.1 Predmet in cilji proučevanja	33
6.2 Uporabljene metode	34
6.2.1 Empirična raziskava – SIBIS	35
6.2.1.1 Internetni kazalci - vpliv dostopnosti interneta na vzpostavitev vzpostavitev kritičnega odnosa do uporabe	36
6.2.1.2 Varna informacijska infrastruktura – vpliv občutka varnosti in zanesljivosti na vzpostavitev kritičnega odnosa do uporabe ...	37
6.3 Povzetek hipotez	38
7. REZULTATI	39
7.1 Zavedanje nevarnosti	39
7.2 Zaskrbljenost nad varnostjo, zasebnostjo in zaupnostjo	42
7.3 Prijava kršitev	45
8. ZAKLJUČEK	48

LITERATURA
PRILOGE

1. UVOD

Živimo v moderni, potrošniški družbi in se vse bolj uklanjamo vedno hitrejšemu tempu življenja, kjer je ključnega pomena, da so (posredovani, iskani, želeni) podatki in informacije dostopni v čim krajšem možnem času. To je tudi eden od razlogov, da si danes težko predstavljamo ljudi, ki pri svojem delu ali v svojem prostem času ne bi uporabljali informacijsko-komunikacijskih tehnologij (v nadaljevanju IKT), pri čemer še posebej ciljamo na internet. Gre za ogromno mrežo, sestavljeno iz še več manjših mrež; za mrežno infrastrukturo, ki med seboj povezuje milijone računalnikov po vsem svetu.

Širjenje in uporaba novih tehnologij v Sloveniji in nekaterih ostalih evropskih državah sta še vedno v porastu; zato pri vseh ugodnostih in prednostih, ki nam jih ta napredna tehnologija prinaša, ne smemo pozabiti na negativne lastnosti, na nevarnosti in zlorabe, ki se lahko ob uporabi pojavijo. Informacijska družba se širi na vse aspekte družbenega in ekonomskega življenja, zato je potrebno pod drobnogled vzeti ne samo razvoj tehnološke infrastrukture, temveč tudi vpliv na posameznike.

Zaupanje uporabnikov v kakršnekoli infrastrukturo, organizacije, podjetja in nenazadnje tehnologije, izvira iz politike države. Če nam le-ta stvari vedno znova prikazuje v korektni luči, si jih znamo lažje, predvsem pa boljše predstavljati, zato se jih posledično ne bojimo in jih tolerantno sprejemamo takšne kot so. V nalogi bom zato na podlagi podatkov o osveščenosti posameznih držav, o problemu rabe IKT, najprej predstavila osnovne pogoje za vzpostavitev kritičnega odnosa do varne uporabe interneta. S pomočjo podatkov iz SIBIS-ovega poročila bom podrobneje opredelila politike, oziroma politična prizadevanja posameznih držav, za obravnavo problemov informacijske družbe.

V tretjem poglavju bomo opredelili (ne)varno uporabo interneta in tako opisali nadloge, s katerimi se srečujemo na internetu. Gre za t.i. vohunsko programje, oglaševalsko programsko opremo in parazitsko programje.

Sledil bo del, kjer bomo spoznali še značilnosti in aktivnosti posameznih evropskih držav, za izvedbo uspešnega pronicanja interneta v vse pore družbe (e-izobrazba, e-zdravstvo, e-uprava, ipd.).

Za lažje razumevanje bom v petem poglavju nekoliko podrobneje predstavila metodologijo komparativnega raziskovanja, ki sem ga uporabila v nalogi, vas seznanila z različnimi pogledi na tovrstno raziskovanje in predstavila še nekaj pozitivnih in negativnih lastnosti le-tega.

V nadaljevanju bomo preučili še razlike v podatkih za posamezne na novo pridružene članice evropske unije, kako jih skrbi za varnost. Kot smo si ljudje med seboj različni, so tudi države vsaj tako, ali nemara celo bolj kompleksne; zato bom med seboj primerjala dobljene rezultate v zvezi z odnosom do varne uporabe interneta. Osredotočila se bom predvsem na vprašanja zavedanja nevarnosti, ki smo jih lahko ob uporabi interneta deležni; na zaskrbljenost nad varnostjo, zasebnostjo in zaupnostjo podatkov, ki se prenašajo preko interneta; in nenazadnje tudi, na pripravljenost (anonimne ali javne) prijave kršitve, v kolikor bi do le-te prišlo.

V zadnjem delu bom torej zbrane rezultate analizirala in jih skušala interpretirati na podlagi naših teoretskih izhodišč; ter z njimi preveriti zastavljene hipoteze. Na kratko bom omenila še možno povezavo med odnosom do varne uporabe interneta, ter pripravljenostjo sodelovati v spletnem anketiranju.

Naj bo moje pisanje v opozorilo in pomoč tistim, ki se ne zavedajo kaj vse nam internet prinaša. Nikakor ni moj namen prestrašiti uporabnike, ampak poudariti, da sta že znanje in zavedanje o potencialnih nevarnostih dovolj, da se kot uporabniki zaščitimo pred pastmi in tako uživamo sadove te velike mreže.

2. OSNOVNI POGOJI ZA VZPOSTAVITEV (KRITIČNEGA) ODNOSA DO (VARNE) UPORABE INTERNETA

Največja prednost interneta je v tem, da lahko kjerkoli in kadarkoli dostopamo do informacij z najrazličnejših področij, z raznovrstno tematiko; v obliki besedila, slikovnih predlog, celo v avdio in video obliki. Omogoča nam nakupovanje, klepetanje s prijatelji, spoznavanje novih ljudi, vključevanje v razprave na forumih. S tem imamo omogočen nov pristop k pridobivanju znanja (Vurušič 2006). Če smo še do nedavnega morali v knjižnici taboriti, da smo končno izbrskali potrebovani podatek, pa danes doma sedemo za računalnik, odpremo internetno stran, ki nam zagotavlja želene podatke, vtipkamo ključne besede in že smo na cilju, v hipu in z informacijami v rokah. Število virov na internetu je praktično neomejeno in ni primerljivo z nobenim drugim orodjem, ki je kadarkoli obstajalo. Dostopamo lahko do raznih strokovnih revij, atlasov, podatkovnih baz in nenazadnje do zvrhanega koša zabavnih vsebin.

Osnovni pogoj, da si ustvarimo mnenje v zvezi z internetom pa je predvsem njegova dostopnost ter uporaba. Prva slabost, oziroma prva težava na katero naletimo je, da neizkušen uporabnik težko razlikuje med pravimi in napačnimi podatki in zaman bi bilo pričakovati, da bo do njih kritičen. Za spletnimi stranmi namreč ne stojijo več le podjetja in zanesljivi viri, saj lahko dandanes spletno stran ustvari kdor koli in na njej objavlja podatke, ki jih želi – izvzete niso niti izmišljene, niti zavajajoče informacije. Poleg vprašljivosti podatkov pa obstaja tudi nevarnost njihove zlorabe. S klikanjem po nezaščitenih spletnih straneh ali s klikom na spletno stran, katerega okno se samodejno pojavi (angl. pop-up okno), lahko uporabnik svoj računalnik okuži z virusom.

Pri tem igrajo veliko vlogo tudi država, državni uradi, institucije, ki bi ob preplavljanju držav z informacijsko komunikacijskimi tehnologijami morali opozarjati tudi na slabosti, ki ji le-te prinašajo, kadar za njihovo uporabo nismo ustrezno podučeni (namestitve požarnega zidu, obvezna uporaba in posodabljanje protivirusnih programov, redno posodabljanje operacijskega sistema in nameščenih aplikacij; izdelava varnostnih kopij podatkov, močna gesla¹, previdnost pri nameščanju in zaganjanju programov, ipd.).

¹ vsebujejo črke in številke, so težka za pomnjenje; za primerjavo: šibka gesla se ponavadi nanašajo na imena sorodnikov, rojstne datume ipd. (Vurušič 2006)

Odgovornost bi nenazadnje morali prevzeti tudi proizvajalci programske opreme, ki pa se temu na vso moč izogibajo. Znan je primer gigantskega podjetja programske opreme Microsoft, ki si je skozi leta izboril monopol na področju programja, si tako povečeval tržni delež, ni pa želel prevzeti skrbi za varnost. Že res, da nobena programska oprema ni popolna, vendar je varnost še dodatno ogrožena, kadar so v ospredje postavljeni drugi (predvsem finančni) cilji. Mikrosoftovi operacijski sistemi so znani kot izjemno kompleksni in prav zapletenost je prvi sovražnik varnosti². Posledice čutimo uporabniki. Delna rešitev problema bi lahko bila zamenjava operacijskega sistema Windows, vendar ljudje raje posegamo po kombinaciji Microsoftovih izdelkov z uporabo dodatnih programov. Tako si na primer zraven požarnega zidu, ki nam ga sam operacijski sistem sicer ponuja (vendar je nezadosten) nameščamo še različne antivirusne programe, ki jih pridno posodabljam, da se izognemo morebitnim nevarnim vdorom; ki smo jim preko povezave računalnika z internetom vsakodnevno izpostavljeni.

² Geer, Dan et.al. (2007): Cyber Insecurity: The Cost of Monopoly. Dostopno na http://securityforest.com/wiki/index.php/Cyber_Insecurity:_The_Cost_of_Monopoly (september 2007)

3. OPREDELITEV (NE)VARNE UPORABE INTERNETA

3.1 Nadloge na internetu

Kot uporabniki interneta, se soočamo z različnimi nadlogami. Pogosto so le-te povezane z operacijskimi sistemi Windows podjetja Microsoft, ki so še vedno najbolj razširjeni med uporabniki (seveda tudi ostali operacijski sistemi niso izjema, le da so manj razširjeni in nekateri med njimi bolje zaščiteni) (Vurušič 2006).

Nevarnosti, s katerimi se srečujemo delimo v več kategorij:

- vohunske,
- oglaševalne,
- parazitske, ipd.

3.1.1 Vohunsko programje

Gre za tehnologijo, ki pomaga zbirati podatke o uporabnikih ali organizacijah mimo njihove vednosti; nato pa jih posreduje spletnim oglaševalcem ali drugim zainteresiranim strankam (angl. spyware). V računalnik lahko pride kot virus ali kot posledica namestitve novega programa. Pogosto je nameščeno brez uporabnikove vednosti (kot dodatek pri prenosu (angl. download) ali kot rezultat pri klikanju opcij pri pojavnih oknih (angl. pop-up window).

Vohunsko programje pa nima vedno negativnega predznaka. Velikokrat se namreč uporablja za razne oblike nadzora otrok oziroma njihove uporabe interneta, v pomoč pa je lahko tudi preiskovalcem pri nadzoru kriminalcev (oz. pri odkrivanju kriminalnih dejanj). Ponekod ga uporabljajo državne tajne službe, čeprav je to v večini držav z zakonom prepovedano (Vurušič 2006).

Vedeti je potrebno še, da programi za zbiranje podatkov, ki so nameščeni z uporabnikovo vednostjo, pravzaprav izgubijo status vohunskega programja, če uporabnik razume, kateri podatki bodo zbrani in komu bodo poslani, ter se s tem strinja.

3.1.2 Oglaševalska programska oprema

Oglaševalne programe (angl. adware) lahko pogosto imenujemo tudi vohunsko programje, ker poleg tega, da oglašuje različne izdelke ali storitve, vsebuje tudi komponente za zbiranje podatkov o uporabnikovih potrebah in navadah. Na osnovi teh podatkov nato na spletnih straneh prikazujejo oglase, ki so izbrani posebej za uporabnika. Pogosto se srečujemo tudi z neželenimi oglasi v pojavnih oknih, ki se prikazujejo med običajnim delom.

3.1.3 Parazitsko programje

Programi se namestijo na uporabnikov računalnik in na primer preprišejo oglaševalske povezave s svojimi ter tako kradejo zaslužek tistim, ki so za oglaševanje plačali (angl. parasiteware). Med zlonamerno programje (angl. malware) spadajo na primer tudi virusi in trojanski konji, ki onemogočajo normalno delo, saj pogosto obremenjujejo sistem. Njihov namen je, vrniti se v računalniški sistem in ga poškodovati ali zlorabiti. Velik problem predstavlja dejstvo, da se jih je zelo težko znebiti, ko se jim uspe namestiti; njihovo delovanje pa lahko povzroči nepopravljivo škodo (izguba podatkov in ponovno nameščanje vseh programov).

Naslednja zelo nadležna oblika programja so t.i. dialerji. Njihova naloga je, da prekinejo obstoječo internetno povezavo in/ali vzpostavijo novo povezavo na komercialno telefonsko številko, običajno v oddaljene kraje sveta. S tem lahko uporabnikom povzročijo veliko stroškov pri njegovem ponudniku telefona (če uporablja klicni način dostopa do interneta), ki pa jih je po naši zakonodaji dolžan poravnati, čeprav uslug dejansko ni koristil - vsaj ne namerno in zavedno.

Ker je človeška iznajdljivost neomejena, nas najbrž ne preseneča dejstvo, da je novih nadlog vsak dan več. Nanje lahko uporabniki naletimo med brskanjem po internetu ali že ob pregledovanju elektronske pošte. Glede na nekatere statistike je na 80% računalnikov nameščena vsaj ena vrsta nevarnega programja (Vurušič 2006), zaradi katerih si nenazadnje tudi računalniški servisi manejo roke. Naj bo to še en razlog več, da se pri uporabi interneta spomnimo na morebitne nevarnosti, se jih zavedamo in se jim ne izpostavljam; oziroma se skušamo o njih dobro podučiti, da bomo znali primerno ravnati, kadar se z njimi srečamo.

4. ZNAČILNOSTI IN AKTIVNOSTI EVROPSKIH DRŽAV

4.1 Bolgarija

Leta 2002 se je, s ponovnim osnovanjem pomembnejših političnih in ekonomskih institucij, končala prva faza tranzicije v Bolgariji. Soočiti so se morali s pritiski tekmovalnosti in silami trga znotraj evropske unije. Da bi lahko sledili tem izzivom pa inovacije igrajo veliko vlogo. Kljub temu, da gre za eno vodilnih držav (ki še vedno ohranja visok nivo) ko gre za izobrazbo specializiranih ljudi v IKT, je njen položaj enak le povprečju na novo pridruženih članic evropske unije³ (v nadaljevanju NAS – angl. Newly Associated States). Za to obstaja več razlogov. Največji je prenizek nivo zahtev v zvezi z investicijami in dejstvo, da je hkrati tudi vodilna država glede odstotka »bega možganov« (SIBIS 2003d).

Da bi bili kos razvoju informacijske družbe in zahtevam skupnega evropskega tržišča, je vlada, kot osnovo za vzdrževanje ekonomske rasti države, dala direktive za razvoj komunikacij in tehnologij.

Program vlade je bil zgrajen na osnovi naslednjih ciljev:

- široka izvedba novodobnih tehnologij, povečanje tekmovalnosti in števila inovacij z zagotavljanjem visokih standardov izobraževanja, modernizacijo ekonomije in gradnjo modernih infrastruktur, še posebej na področjih informacijskih tehnologij in telekomunikacij;
- vlaganja v IKT, preko česar generalno gledano posledično vlagamo tudi v ostala področja;
- IKT postaja glavno gonilo ekonomske rasti.

Vlada pa je prav tako oznanila naslednje strateške cilje:

- promovirati vlaganja v IKT in razvoj R&D⁴ mrež,
- narediti tekmovalno in v izvoz usmerjeno industrijo računalniške programske opreme,
- ohraniti močno bolgarsko izobraževalno tradicijo,
- podpirati mala in srednja podjetja v sektorju IKT,
- vzpodbujati mlade diplomante, da gradijo svojo kariero doma.

³ Bolgarija, Češka, Estonija, Latvija, Litva, Madžarska, Poljska, Romunija, Slovaška in Slovenija

⁴ Research and Development nets – mreže za raziskovanje in razvoj

Slednje nameravajo izpeljati z gradnjo raziskovalnih in razvojnih centrov v Bolgariji, preko katerih bodo zmožni delati na daljavo in sodelovati pri velikih korporativnih projektih po vsem svetu. Ponudili jim bodo dobre profesionalne priložnosti in poštene nagrade za njihovo delo (SIBIS 2003d: 5).

Kot znak pomembnosti razvoja IKT, so se posamezna ministrstva zavezala k izvedbi teh strategij, za vzpodbudo omenjenega sektorja. Da bi bili bolj usklajeni pri akcijah ministrstev, pa je glavni urad tisti, ki prevzema vso odgovornost pri koordinaciji državnih ambicij in ciljev.

Pri nadgraditvi in razširitvi IKT v Bolgariji, so glavne ugotovitve naslednje:

- nivo prodiranja informacijskih tehnologij v vsakdanjike življenj je relativno nizek, računalniški dostop je zgoščen le v večjih mestih (Sofia ipd.),
- tamkajšnji uporabniki interneta običajno dostopajo v virtualni prostor iz treh večjih razlogov: uporablja interneta kot vir informacij, v zabavne namene, in za delo in izobraževanje.

Možnosti finančnih poslovanj in kupovanja preko spleta se še vedno zelo malo izkoriščajo. Glavni razlogi so: (ne)zanesljivost povezav, nizek nivo zavedanja zmogljivosti teh tehnologij in nizka stopnja zaupanja v elektronsko bančništvo (npr. samo tri banke⁵ sploh nudijo e-usluge).

Gre za državo, ki ima veliko število kvalificiranih znanstvenikov in tehnikov v poslovnem sektorju (izučeni elektroniki in mehanični inženirji), kar posledično pomeni, da kvantiteta ljudi podpira razvoj IKT (SIBIS 2003d). Kljub temu pa so na ministrstvu za izobraževanje in znanost sprejeli mere za dodatno izboljšanje stanja v informacijskem sektorju. Že leta 1998 se je pričela izvajati državna strategija za izobraževanje v IKT, sledil je program za dodatno izboljšanje nivoja izobrazbe v IKT (1999), 30.8.1999 pa je bil izdan še ukaz za uvedbo informatike in informacijskih tehnologij v šole. Izobraževanje se je tako začelo 1. septembra 1999, maja naslednjega leta (2000) pa so bila objavljena tudi vsa priporočila za učne programe.

⁵ United Bulgarian Bank, First Investment Bank, Union Bank

Kot enega glavnih vplivov, na zagotovitev virov za tehnološki razvoj v državi, naj omenim visoko zanimanje mladih za izobraževanje v IKT. Razloge za to gre iskati v bolgarski tradicionalni naklonjenosti izobraževanju; hitremu razvoju trgov informacijskih tehnologij v EU in ZDA, in nenazadnje v dejstvu, da so njihovi strokovnjaki spretni in izkušeni, tako pri fizični kot pri programski opremi.

Tuje povpraševanje za izurjene človeške vire v sektorju IKT pa je vodilo k t.i. »begu možganov«, ko so strokovnjaki začeli odhajati na tuje. Po podatkih državnega statističnega urada je v zadnjem desetletju; zaradi minimalnih zahtev državnega trga (visokih zahtev v EU), slabega praktičnega znanja mladih o razvoju poslovnih poti znotraj države in šibkega sodelovanja univerz, raziskovalnih ustanov in poslovnega sveta; državo zapustilo okrog 300.000 strokovnjakov iz področja informacijskih tehnologij.

Izobrazba in uporaba IKT ter razvoj državnih mrež za izobraževanje in znanost, so naloge državne strategije za razvoj informacijske družbe in pobude za vzpostavitev e-Evropske. Načrt za leto 2005 je vseboval prizadevanja za elektronsko pismenost učencev v srednjih šolah, in zagotovitev dobrega dostopa do interneta, šolam, univerzam in ostalim institucijam.

Bolgarija ima torej dobro raven usposobljenih v IKT, vendar so zahteve in povpraševanje v tem sektorju premajhne in premalo mikavne, zato z odhodom strokovnjakov na tuje prihaja do izgube tega potenciala. V glavnem je država odgovorna za vzpodbujanje šol k informacijskemu izobraževanju; vendar v zadnjih letih prihaja do teženj k zmanjševanju sredstev za tovrstna področja, pobudo pa prevzemajo podjetja, ki želijo razširiti in pospešiti pokritost in hitrost tehnologij, informacij in znanj. Pri tem pa niso preveč uspešni, saj se soočajo s finančnimi problemi in omejenostjo potreb oziroma povpraševanj ljudi.

4.2 Češka

Vodstvo države se je prvič spoprijelo s problemom informacijske družbe leta 1998. Nameravali so ustvariti primerne zakonodajne pogoje in ustvariti okolje, ki bi vzpodbujalo razvoj. Maja 1999 je bil izdan tudi prvi⁶ uraden dokument (State Information Policy), ki govori o sistematičnem obravnavanju omenjenega problema. V njem se država zavezuje k podpori za dosego informacijsko usmerjene družbe in obljublja pomoč k uresničevanju računalniške pismenosti. Dejanski izraz tega zapisa se odraža v projektu »Action Plan for Implementation of the State Information Policy (akcijski načrt za izvedbo državne informacijske politike), ki so ga uvedli v marcu 2002 in dokončno izvedli konec leta 2003 (SIBIS 2003d).

Januarja 2003 je bil z ustanovitvijo ločenega ministrstva za informiranje izveden zadnji institucionalni korak Češke države, kar zadeva skrb za informacijsko družbo. Splošno stališče v zvezi s tem je, da zasebne pobude in spontan razvoj na ravni državnih administrativnih institucij in lokalne vlade, igrajo še večjo in bolj pozitivno vlogo, kot centralizirana državna podpora informacijske družbe. Tudi zato Češka pripada vodilnim državam v sektorju informacijsko-komunikacijskih tehnologij med osrednjimi in vzhodnimi članicami EU; saj je bil tu razvoj teh tehnologij (osebni računalniki, internet, mobilni telefoni) izredno hiter. Kot zanimivost naj navedem še podatek, da država porabi več sredstev za IKT (glede na BDP), kot v povprečju države EU; vsako leto pa imajo približno 5.000 diplomantov in veljajo za populacijo, ki ima približno 10% prebivalstva visoko računalniško pismenega.

Posledično se sicer zdi, da osrednja politika države vzpodbuja razvoj tega sektorja, vendar je realna slika drugačna, saj z realnim stanjem nikakor ne dohajajo dejanskih pogojev zakonodaje. To se na primer kaže v pozni liberalizaciji telekomunikacijskega sektorja (ki se je začela že v 90.letih 20.stoletja) in neenaki ravni izvedbe rešitev fizične in programske opreme v javnih institucijah, kar je vodilo k ne-združljivosti in težavam pri medsebojnem povezovanju. Glavni cilj je torej doseči harmonizacijo z zakoni EU in vzpostaviti zakonodajne pogoje za učinkovitejšo in širšo uporabo in izkoriščanje modernih IKT.

⁶ Čeprav so se te problematike rahlo dotaknili že leta 1994, v dokumentu z naslovom »The Main Principles of Telecommunication Policy«; nova verzija izdana 1999 (SIBIS 2003d)

V glavnih listinah o informacijski družbi so obravnavana naslednja področja: varstvo osebnih podatkov (z zakonom stopilo v veljavo junija 2000), dostop do informacij javnega značaja, o telekomunikacijah, elektronskem podpisu (zakon sprejet oktobra 2000) in javnem vodenju informacijskega sistema.

Na češkem obstajajo tako interesne skupine, ki jih podpira vlada (the Czech Forum for the Information Society); kot ostale privatne skupine (npr. zveza petdesetih vodilnih podjetij v sektorju informacijskih tehnologij – the Association for the Information society (dostopno na <http://www.spis.cz>); ali BMI, zasebna zveza, ki organizira in oglašuje projekt »March-Internet Month«, ki razpravljajo o vprašanih informacijske družbe.

Od 1. januarja 2003 je na novo ustanovljeno ministrstvo za informiranje tisto, ki usklajuje dogodke, ki vodijo k informacijski družbi. Povezalo je dve neodvisni strukturi – urad za javni informacijski sistem in ministrstvo za transport in komunikacije, ter od urada za varstvo osebnih podatkov prevzelo vprašanja elektronskega podpisa. V svojih ciljih so zapisali, da si želijo vzpostaviti take pogoje, da bo njihova država postala vodilna v sektorju IKT. Za to se borijo na treh frontah: najprej želijo osnovati e-vlado, ki bo državljanom omogočala hitro in lahko komunikacijo z državo, kar bo vodilo k varčevanju državnega proračuna. Oblikovali bodo pogoje enakovrednega tekmovanja na trgu telekomunikacij in pomagali razviti ekonomski trg. Nenazadnje pa želijo ponuditi še rešitve, da bi večjemu številu ljudi omogočili širok dostop in znanja o KT. Bistvo celotnega projekta je torej omogočiti Češki enakovreden položaj z ostalimi državami, da bo uspešno prenesla svetovno/globalno tekmovanje v 21. stoletju. Ostale naloge ministrstva vključujejo pripravo strateških konceptov, osnutkov zakonov IKT in usklajevanje državnih teles na področju IKT. Tudi ostali organi države so odgovorni za uresničitev ciljev o IKT, glavno vlogo pa igrajo: ministrstvo za izobrazbo in mladino (dostopno na <http://www.msmt.cz>), ministrstvo za delo in družbene zadeve (dostopno na <http://www.mpsv.cz>), ministrstvo za notranje zadeve (dostopno na <http://www.mvcr.cz>) in češki statistični urad (dostopno na <http://www.czso.cz>).

4.3 Estonija

Prvi državni program za informacijsko tehnološki razvoj je bil pripravljen leta 1994 (The Estonian Way to the Information Society). Malo kasneje je nastal začetni dokument v zvezi z razvojem informacijske družbe (Principles of Estonian Information Policy), ki ga je odobrila vlada v letu 1998. Vladna informacijska politika je vzela na znanje cilje, ki so nastali pri ureditvi različnih krogov družbenega življenja in omogočila priložnosti za predstavitev novih rešitev (SIBIS 2003d: 20).

Načrt informacijske politike (Information Policy Action Plan) je osnova za natančno opredeljene predloge (načrti, viri financiranja in odgovornosti vsakoletne izvedbe programov informacijske politike), ki jih vsi vladni uradi želijo posredovati vladi.

Njihova politika je bila v naslednjem okviru, na temelju štirih področij: modernizacije zakonodaje, pomoč pri razvoju privatnega sektorja, razvoj komunikacij med državo in državljani, in prepoznavanje problemov v zvezi z informacijsko družbo (SIBIS 2003d).

Vsako leto se je načrt nadalje razvijal, zato je vlada podala osnovne prednosti, ki jih je pri izvajanju le-tega treba upoštevati: razvoj uslug za državljane, poslovni sektor in javno administracijo; izboljšanje veščin, spretnosti in dostopa družbenih skupin v neenakem položaju, do uporabe elektronsko posredovanih uslugah; izpopolnjenje in predstavitev sistemov za upravljanje digitalnih dokumentov in procesov arhiviranja; razvoj sistema in infrastrukture državnih registrov, (vključno z razvojem sistemov, ki zagotavljajo vzdrževanje baz podatkov); boljša preskrbljenost šol z računalniki (doseganje končnega cilja – imeti en računalnik na 20 študentov); izvedba programa »Tiger« na univerzah, ki bi omogočil podporo razvoju infrastrukture IKT in visokošolskemu osebju IKT ter infrastrukturi za po-diplomante.

V ozadju teh nalog, ki so v glavnem v zvezi z razvojem infrastrukture IKT, je po navedbah SIBIS-ovega poročila (2003d) namen države razviti in dopolniti tudi infrastrukturo državnih in lokalnih vladnih IKT v splošno, uporabniku prijazno okolje IKT, kjer bi se poudarjala načela in priporočila za razvoj demokracije.

Vlada je decembra 1999 sestavila strateški dokument imenovan »Knowledge-based Estonia« (na znanju temelječa Estonija), ki ga je 6.12.2001 odobril tudi estonski parlament – in v zvezi s tem takrat podal tudi strategijo razvoja v letih od 2001 do 2006 (SIBIS 2003d). Izhaja iz dejstva, da ima znanje, kreativnost in inovativnost veliko vlogo v dolgoročnih spoprijemanjih s problemi njihove ekonomije in utrjuje vladne želje za izboljšanje estonske inovacijske politike. Podpirajo torej nova znanja, uporabo spretnosti, znanj in razvoja človeških virov, ki jih vidijo kot vir ekonomske in delovne konkurenčnosti, kot kvaliteto življenja. Poudarjajo uporabniku prijazne IKT in razvoj informacijske družbe kot enega ključnih področij razvoja.

Zavedanje ljudi, o informacijski družbi, je sunkovito naraslo s sodelovanjem med različnimi organizacijami in z organiziranjem aktivnosti v večjem merilu. V javnem sektorju je ministrstvo za izobraževanje aktivno pri razvoju osnove informacijskih tehnologij estonskih šol (preko že omenjenega programa Tiger Leap Foundation).

Estonski informacijski center objavlja računalniški časopis »Arvutimaailm« (v estonskem jeziku), ki je namenjen širokemu občinstvu in pokriva različne vidike informacijske družbe.

Glavna organizacija v ozadju (t.i. tretji razred), ki poudarja zavedanje ljudi o posledicah, ki nam jih IKT prinaša, je »Open Estonia Foundation«, ki je financirala več projektov informacijske družbe (npr. vzpostavitev javnih možnosti dostopa do interneta, razvoj on-line informacijskih uslug, organizacija seminarjev in konferenc ipd.). Ostale tretje razredne profesionalne organizacije pa so še: Estonian Computer Association in Estonian Information Technology Association.

Estonski (državni) koordinacijski urad, ki vzpodbuja zavest in kritičnost ljudi do novih tehnologij; ter si hkrati prizadeva tudi za rast informacijske družbe, je njihov informacijski center, ki je bil pod vodstvom državnega kanclerstva, z nalogo rešiti glavne probleme v zvezi informacijsko tehnologijo v nekaj državnih organizacijah, ustanovljen leta 1997.

Številni programi javnega in projekti privatnega sektorja (e-vlada, e-okrožje, e-državljan, e-poslovanje itd.) podpirajo tudi politično zavedanje.

Eden takšnih je na primer »Look@World«, ki je bil narejen aprila 2002, v njegovem programu pa so si prizadevali za brezplačne računalnike in internetno poučevanje za stotisoče oseb (Progress Report 2002. V SIBIS 2003d).

Poudariti velja še izjemen dosežek Estonije na področju parlamentarnih volitev, saj je 4.marca 2007 kot prva država v zgodovini omogočila državljanom, da so glasovali preko interneta. Okoli 3.2 % volilnih upravičencev (30.000 od 940.000) je uporabilo možnost elektronske oddaje glasu na predčasnem glasovanju. Volitve je spremljala Organizacija za varnost in sodelovanje v Evropi (OVSE). To je bil sicer drugi poskus z e-volitvami v Estoniji. Leta 2005 je namreč na lokalnih volitvah elektronsko glasovalo okrog 10.000 volilnih udeležencev (dostopno na <http://www.agencijanet.si>).

Država sodeluje z različnimi tujimi organizacijami, kot so:

- Joint High Level Committee,
- International Council for Information Technology in Government Administration,
- Baltic Council of Ministers,
- European Environment Information and Observation Network ipd.

Hkrati pa se tudi sama pridružuje številnim mednarodnim projektom, npr.:

- e-Europe+⁷ 2003,
- Northern eDimension,
- European Survey of Information Society (SIBIS 2003d).

V dokumentu projekta eEuope+ 2003, kot enega mnogih projektov za uresničitev informacijske družbe v Evropi, se omenja problem e-ustreznosti. Junija 2001 je zato bil, iz strani držav kandidatk, s podporo evropske komisije, sestavljen akcijski načrt za informacijsko družbo. Z njegovo izvedbo naj bi dosegli kriterije, navedene v poročilu za razvoj informacijske družbe v obdobju 2000-2006 (SIBIS 2003:d).

⁷ je akcijski načrt za države kandidatke EU, pri izvedbi katerega naj bi jim pomagala evropska komisija

Vlada je aprila 1997, za raziskovalne programe, za potrebe koordinacije in izvedbe različnih evropskih programov in uresničitve pobud na področju raziskovanja in izobraževanja, ustanovila sklad za izobraževanje ljudi v evropski uniji, ki prav tako vključuje dejavnosti povezane z razvojem informacijske družbe. Leta 2000 se je vlada odločila preseliti naloge koordinacije razvoja informacijskih tehnologij, ki so bile dotlej vodene iz strani javnih administracij, preusmeriti na področje ministrstva za transport in komunikacije (e-policy 2002). Prav tako se je zasebni sektor vse bolj vključeval v delo mednarodnega sodelovanja na področju informacijske družbe in v aktivnosti različnih delovnih skupin. Pozitiven primer sodelovanja je delovna skupina, ki se je ukvarjala z izvedbo digitalnega podpisa in je pri iskanju ustreznih rešitev pogosto vključevala predstavnike različnih bank in ponudnikov telekomunikacij.

4.4 Latvija

Potrebe za razvoj informacijske družbe je vlada naznanila marca 1999, ko je ministrstvo sprejelo državni program informatizacije (prodiranje IKT na različna področja družbe), ki naj bi se preko več kot 120 manjših projektov (za uresničitev e-Evropske) izvajal med leti 1999 in 2005. Glavni cilj programa je bil po navedbah SIBIS-ovega poročila (2003d) integracija Latvije v globalni razvojni proces in oblikovanje informacijske družbe.

Danes so navodila za strategijo vključena v mnogih dokumentih, od katerih naj omenim najpomembnejše: državni informacijski program, navodila za socio-ekonomski program e-Latvija, državna predstava o e-vladi in e-trgovini, državno pojmovanje internetnega razvoja in doseganje napredka javnega sistema pri preskrbi z IKT in internetom.

Oblikovanje informacijske družbe ni mogoče brez primerne razvoja IKT; za katerega sta med drugimi najbolj odgovorna: oddelek za informatiko na ministrstvu za transport⁸ (infrastruktura IKT), in državni odbor za informacijsko družbo. Slednji je bil ustanovljen aprila 2000 in mu predseduje premier (predsednik vlade) Latvije. Njegove glavne dolžnosti so usklajevanje in sprejemanje projektov informacijske družbe (e-Latvija, e-trgovina, e-vlada); združuje pa predstavnike iz vrst vlade, akademskega in poslovnega sektorja (SIBIS 2003d: 55).

Omeniti velja še državno informacijsko omrežje agencije VITA (dostopno na <http://www.vita.gov.lv>). Je neprofitna državna družba, ki zagotavlja usluge za prenos podatkov po državi. Gre za zaprto omrežje, kar pomeni, da jo uporabljajo le državne in občinske institucije in organizacije (vsa državna ministrstva, policija itd.), ter omejeno število zasebnih podjetij.

Kot odgovor na pobude projekta e-Evropa, je vlada ministrstev, kot pridonos k evropskemu projektu, decembra 2000 sprejela glavne smernice za socio-ekonomski program e-Latvije (SIBIS 2003d). Podobno kot je osnovan evropski projekt so torej tudi oni oblikovali tri glavne smernice, ki naj bi jih izvedli v štirih letih. To so: cenejši, hitrejši in varen internet; vlaganje v ljudi in njihove spretnosti/veščine in spodbujanje uporabe interneta.

⁸ dostopno na <http://www.sam.gov.lv/branches/informatics/character>

4.5 Litva

Prvi politični koraki proti informacijski družbi so bili narejeni leta 1991. Kasneje (1993) je, po navedbah SIBIS-ovega poročila (2003d), vlada odobrila nov program o javnem komuniciranju in informatiki, ki so ga obnovili 1996 in je bil v veljavi vse do leta 2000, ko se je (po državni osamosvojitvi in vzpostavitvi informacijske družbe, ki ji je bila omogočena demokratičnost) zgodil naslednji korak – poudarjati se je začelo pomembnost gradnje informacijske infrastrukture, kot temeljne za informacijsko družbo.

Ukrepe za izvedbo pomembnejših političnih pobud, ki so okrepili litvansko zavezanost e-Evropi, so podprle mnoge organizacije in ogromno število ljudi: npr. memorandum razvoja informacijske družbe (za zagotovitev zadostne politične podpore) so podpisali vodilni petih največjih državnih strank, nato pa se jim je pridružilo še preko 20 organizacij (SIBIS 2003d: 67). Da bi državo vzpodbudili k zagotavljanju pravic za vse državljane do uporabe poceni in hitrega interneta, je 2000 nastala deklaracija o pravicah do interneta.

Država se je torej politično pripravila za pobude e-Evrope, vlada pa je razglasila razvoj informacijske družbe kot glavno prednost in eno glavnih vplivov za državno dobro.

Dolgoročna ekonomsko razvojna strategija Litve, je 2001 napovedala prizadevanja za dvig informacijskih komunikacij na nivo vladajočega sektorja (do leta 2015 naj bi zajemale 25% BDP). V letu 2001 je tržišče IKT v Litvi, po podatkih italijanskega observatorija, v primerjavi z letom poprej naraslo za 11,5% in je bilo največje med baltskimi državami (SIBIS 2003d).

Med pomembnejšimi projekti za uresničitev informacijskih tehnologij (med leti 2001 in 2002) so po navedbah poročila SIBIS-a (2003d) naslednji: uvedba računalnikov v vsakdanjik ljudi, uporabljanje pametnih kartic (elektronsko poslovanje, bančništvo, nakupovanje...), izboljšanje zdravstvenega vodenja, delovanja bank, uporaba za izobraževalno in raziskovalno delo (ekonomija znanja), on-line knjižnice.

Neposredna izvedba pobud e-Evrope se je preko usposabljanja populacije za informacijske tehnologije, opremljanja šol z računalniki, modernizacijo sistema znanosti in izobraževanja, vzpodbujanjem e-poslovanja in vzpostavitvijo e-vlade, začela sredi leta 2000.

Leto kasneje (2001) je vlada prvič v zgodovini namenila sredstva za financiranje razvoja informacijskih tehnologij, neposredno iz državnega proračuna (SIBIS 2003d).

Glavne institucije v procesu razvoja informacijskih tehnologij so: svet družbe znanja (podaja predloge za oblikovanje državne politike v zvezi z znanjem in izvedbo tovrstnih projektov), razvojni komite informacijske družbe (pripravlja zakonite listine za uravnavanje vprašanj informacijskih tehnologij in vodi parlamentarni nadzor uporabe državnih virov in vlaganj v programe), vladna komisija za razvoj informacijskih tehnologij, ki mu predseduje premije (zadolžen za koordinacijo strategij in programov), odbor za razvoj informacijske tehnologije, ki je pod vodstvom republike Litve (ki se osredotoča na probleme štirih področij: sposobnosti populacije, e-vlada, e-poslovanje in podpora kulturni dediščini) (SIBIS 2003d).

4.6 Madžarska

Madžarski parlament je leta 1989 izpostavil problematiko enotnega telekomunikacijskega zakona. V letu 2001 se je zakonska osnova z elektronsko vodenje razširila z odobritvijo zakona o digitalnem podpisu. Ta del zakonodaje pokriva tri področja:

- zagotavlja možnosti uporabe digitalnega podpisovanja,
- opredeljuje pravila za zagotavljanje tovrstnih uslug in
- urejuje javen nadzor nad njimi (SIBIS 2003d: 37).

Že leta 1989 je torej madžarska vlada oblikovala različne programe, kako se spopasti s tehnološkim razvojem na področju informacijskih tehnologij. Sredi 80.let so strokovnjaki po navodilih ministrskega predsednika oblikovali projekt, imenovan »Development Programme of the Information Infrastructure«; ki se je izvajal vse od leta 1986 do 1994. Sledil je »National Information Infrastructure Development Programme« (1995) in »National Information Strategy« (1996). Sočasno je na ministrstvu za izobraževanje potekal projekt »Sulinet« (ponudba interneta v šolah), ki je vključeval osnovne in srednje šole. Da bi uskladili prizadevanja različnih vej vlade, so leta 1997 na pobudo le-te razvili z nov program, pod imenom »Governmental Information Strategy« (SIBIS 2003d).

Decembra 2000 je tudi ministrstvo za ekonomijo izdalo program »Széchenyi«, v katerem so načrtovali pospešitev ekonomskega razvoja države (razvoj podjetij, turizma, stanovanjske modernizacije, regionalne ekonomije; energetske varčevanje in podpora pri zaposlovanju), ki bi ga izvedli preko malih in srednjih državnih podjetij, gospodinjstev, nevladnih organizacij ipd. Eden glavnih ciljev je bil tudi modernizacija infrastrukture IKT in uporabe le-teh (v programu omenjeno kot vzpostavitev e-madžarske).

Madžarska univerza za znanosti je 1997 sestavila načrt »Fast Internet Project«, ki je opisoval tehnološke in družbene pogoje za vzpostavitev internetnih povezav. Ti so bili, kot navaja SIBIS (2003d), vse prej kot idealni, saj so bile povezave razpršene po celotni državi. Za reševanje informacijsko-komunikacijskih problemov je zato bil ustanovljen nov državni urad (prej je za ta vprašanja bilo odgovorno ministrstvo za transport, komunikacije in upravljanje voda).

Pomemben in zanimiv dokument je tudi »načrt državnega razvoja« iz leta 2002, kjer je omenjena odgovornost države do ohranjanja državne blagajne. Le-to naj bi izpolnjevala z razvojem informacijske družbe (z modernizacijo javne uprave in vzpostavitvijo države, ki bo usmerjena k ponujanju e-uslug), ki bo pripomogla k državni blaginji in izboljšala pogoje in kvaliteto življenja.

Vlada, izvoljena 2002, je nadalje razširila urade, odgovorne za IKT in informacijsko družbo, ter ustanovila Ministrstvo za informatiko in komunikacije. Pristojnosti in moč mu je dodelila pri razvijanju enotne in vsestranske vladne strategije, v zvezi z informacijsko družbo; in, za koordinacijo in nadzor aktivnosti, povezanih z IKT (znotraj madžarske in mednarodno). Izraža osnovne pravice državljanov - dostopa do informacij, širjenja le-teh in medsebojnega komuniciranja.

Za izvedbo navedenih nalog mora ministrstvo organizirati in ohranjati posebne odbore in razvijati ustrezne institucije. Glavne naloge, ki jih ima so še:

- prenova zakonodaje povezane z razvojem in izvedbo e-vlade,
- standardizacija elektronskega poslovanja pisarn javne uprave,
- razvoj, uveljavljanje in razširitev varnostnih standardov in sistemov za zagotavljanje varovanja pred nevarnostmi, ki jih prinaša informacijska tehnologija itd. (SIBIS 2003d).

S to odredbo evropska unija ministrstvo zakonsko zavezuje k izvajanju programov e-Evropske (e-vlada, e-poslovanje, tehnični razvoj, vzpostavitev informacijske družbe, vzpodbujanje konkurenčnosti ponudnikov IKT in liberalizacijska politika za le-te).

Pomembnejši cilji so še:

- omogočanje internetnega dostopa za invalidne ljudi,
- vzpostavitev komunikacije med lokalno vlado in državljani,
- nastanek prostorov elektronskega trgovanja,
- javna elektronska preskrbljenost in
- uporaba digitalnih knjižnic.

Državni raziskovalni inštituti in univerzitetni raziskovalni centri so (v gospodinjstvih, šolah, bolnišnicah, lokalnih vladnih pisarnah in drugod) izvedli več raziskav, da bi odkrili mehanizme za širjenje inovacij IKT. Izkazalo se je, da so ljudje zelo različno občutljivi na razvoj IKT (SIBIS 2003d). Odprtost je odvisna od starosti, nivoja izobrazbe, preteklih izkušenj, zaupanja, oddaljenosti od mest in družbenega razreda; nanjo pa v veliki meri vplivajo tudi šolsko in delovno okolje. Tam se otroci in starši ob srečanju z novimi IKT naučijo kako jih uporabljati, nato pa znanje prenesejo na širši krog ljudi (družinske člane, prijatelje itd.).

Po podatkih iz raziskave Pinter⁹ (2002), je država pripravljena na prihod informacijske družbe (še posebej na e-učenje; nekoliko manj pa na e-ekonomijo), problem pa predstavljajo drage internetne povezave in nezadostna pokritost z infrastrukturo (ki še vedno ne omogoča dostopa za vse državljane). Aprila 2000 je bila objavljena politika oziroma oblika strategije za izvedbo priporočil vlade, o razvoju informacijske družbe, v katerem je navedeno, da je potrebno podpirati vstop mladih v digitalno dobo, zagotavljati poceni dostop do interneta, pospeševati pokritost z elektronsko trgovino, omogočiti hiter internetni dostop za raziskovalce in študente, zagovarjati uporabo t.i. pametnih kartic v modernih informacijskih sistemih, razširiti možnosti elektronske participacije za invalide in ljudi s posebnimi potrebami, vzpodbujati on-line zdravstvo in vzpostaviti e-vlado. V letih 2002/2003 se je ob madžarsko-slovenski meji, natančneje v občini Dobrovnik, izvajal še projekt »e-vasi«, ki pa ga bomo podrobneje obravnavali v poglavju 4.10 (Slovenija).

⁹ Celoten vprašalnik je dostopen na <http://www.readinessguide.org>

4.7 Poljska

Ministrska konferenca na temo informacijske družbe in pospeševanja evropske integracije, je bila organizirana v Varšavi, maja 2000 in predstavlja osnovo za nastanek dokumenta eEvropa+ (SIBIS 2003d). Z njim so se države, kandidatke za vstop v evropsko unijo, zavezale k sodelovanju z evropsko komisijo, pri vprašanih informacijskih tehnologij. Ne samo, da so slednje vključili v politične programe, ampak so nastajali tudi novi programi, ki so zadevali zakonodajne in organizacijske spremembe.

Začetki soočanja s vprašanji informacijske družbe segajo v leto 1994. Na prvem kongresu (dostopno na <http://www.kongres.org.pl>) o poljskih informacijskih tehnologijah v mestu Poznań, so (na osnovi pregleda stanja, predlogov in pogleda v prihodnost) nastali prvi programi in strategije za razvoj le-teh. Na drugem kongresu (1999) je bil oblikovan dogovor za uresničitev nastanka informacijske družbe na Poljskem, 23. februarja 1999 pa je parlament razpravljal o zakonu o telekomunikacijah (ki ga je sprejel šele 21. julija 2000). Eden prvih zakonov v zvezi s problematiko informacijskih tehnologij je bil vladni projekt o avtorskih in izvirmih pravicah¹⁰ (odobren 9. junija 2000). Država se je pri sprejemanju zakonodaje soočala tudi z različnimi političnimi pritiski (lobiji). Na tretjem srečanju je bil ustvarjen poljski Forum za informacijsko družbo, katerega namen je bil pomagati oblastem pri realizaciji ciljev; rezultat četrtega pa je sodelovanje vlade s krajevnimi telesi. Institucionalni in družbeni vrh so dosegli 14. julija 2000, s parlamentarnim sprejetjem zakona o ustvarjanju informacijske družbe. Ministrstvo za komunikacije je delalo na projektu »e-Poljska« - strategija za razvoj informacijske družbe v letih 2001 – 2006, ki predstavlja glavni dokument, ki določa prihodnost informacijske družbe na Poljskem. Z njim so želeli pospešiti reforme in modernizirati ekonomijo. Deležen je bil ostrih kritik iz strani Poljskega Foruma, češ da se v nezadostni meri povezuje z nevladnimi in znanstvenimi organizacijami (SIBIS 2003d).

Kot kaže je takrat čakala Poljsko še dolga in težka pot do uresničitve danih ciljev. Velik problem je predstavljalo pomanjkanje finančnih sredstev. To so poskušali rešiti leta 2002, s preoblikovanjem državnega odbora znanstvenega raziskovanja v ministrstvo za znanost in izvedbo informacijskih tehnologij; le čas pa bo pokazal ali je to pripomoglo k povečanju učinkovitosti.

¹⁰ Official Journal of 2000. V SIBIS 2003d

4.8 Romunija

Vlada je leta 1998 odobrila prvo državno strategijo za pospeševanje razvoja informacijske družbe in akcijski program za sektor IKT. Dobro opredeljen in uresničljiv načrt iz leta 2002 z naslovom »strategija romunske vlade za razvoj informacijskih tehnologij«, je tisti, s katerim se je Romunija zavezala k uresnitvi ciljev e-Evrope (SIBIS 2003d: 82). S tem je razvoj informacijske družbe glavna prednost romunske politike, pri katerem sodeluje vlada, akademsko osebje in privatni sektor. Slednji je ključnega pomena za razvoj infrastrukture, ustreznosti in uporabnosti informacijske družbe.

Poseben položaj v državi ima e-administracija, ki si prizadeva k izboljšanju odnosov med državljani in lokalno ali centralno upravo. Mnogo se posveča poklicnemu in nadaljnjemu izobraževanju, ki bi temeljilo na IKT in internetu; zato skuša zagotoviti računalnike in usluge informacijskih tehnologij tudi v vaseh, ter razširiti priključljivost interneta, za potrebe šol in ostalih ljudi na podeželju. Z rastjo trga informacijskih tehnologij se povečuje tudi pobuda posameznikov in podjetij, ki delujejo v sektorju IKT (ponujajo usluge, produkte, treniranje, marketing in oglaševanje). Kljub temu pa so tranzicijske težave (pri prehodu ekonomije) drastično zmanjšale število in s tem učinke njihovih pobud, zato je izvedba zastavljenih ciljev v zaostanku, za nekatere regije pa celo nemogoča.

Ministrstvo za komunikacije in informacijsko tehnologijo je podalo navodila za izvedbo načel projekta e-Europe+, pri katerem morajo sodelovati vsi državljani (SIBIS 2003d). Do sprememb naj bi prišlo na področju uprave (e-vlada) ter (elektronskega) poslovanja, izobraževanju (na daljavo), v kulturnem okolju (navidezni multimedijski centri) in načinu dela (tele-delo)¹¹. Odgovorno je za nadziranje aktivnosti, ki se odvijajo preko javne ali privatne komunikacije.

Marca 2002 je bila ustanovljena skupina za podpiranje informacijskih tehnologij, ki ji je bila dana celo še večja odgovornost kot ministrstvu za komunikacije in informacije. Ima vlogo usklajevanja projektov različnih sektorjev. Zanj skrbita romunski premier (predsednik vlade) in predsednik države, sestavlja pa jo še sedem članov ostalih ministrstev (SIBIS 2003d: 83).

¹¹ dostopno na <http://www.mcti.ro>

Z obravnavanimi strateškimi vprašanji se ukvarjajo številna ministrstva (za finance, javno upravo, zdravje, sodstvo, izobraževanje in raziskovanje, delo in družbeno kohezivnost).

Državna taktika izpostavljena februarja 2002 je:

- omogočiti razvoj informacijske družbe,
- državnih politik za podporo razvoju IKT in
- hitro infrastrukturo znotraj države (SIBIS 2003d).

4.9 Slovaška

Ena od posebnosti Slovaške poleg njenega razvoja k informatizaciji družbe in njenega sodelovanja z e-Evropo je njena zapletenost. Zgodovinsko gledano ni bila naklonjena razširitvi računalnikov in informatizaciji na splošno. Če izhajamo iz tega dejstva, moramo v zakup vzeti naslednje značilnosti: kot del češko-slovaške federativne republike; je med ostalimi področji za Češko ogromno zaostajala tudi pri računalništvu. Za ponazoritev, ko sta se državi ločili (leta 1993), je indeks osebnih računalnikov na 100 prebivalcev na Češkem znašal 27, medtem ko je na Slovaškem komaj dosegal indeks 17. Iz tega sledi zaključek, da je kompletna osnova za razmah računalništva in z njim povezane tehnologije pod bivšim socialističnim režimom bila zelo slabo razvita (SIBIS 2003d: 90).

Kljub vsem težavam, da bi presegli ta tehnološki manko je na nekaterih področjih uspel preboj, razširitev in splošna pokritost populacije z računalniki in računalniško opremo, na izrednem, mednarodno priznanem nivoju. Napredek se na primer pozna pri državnih statistikah, kjer je zahvaljujoč tehnični podpori v 60. letih v Bratislavi (kot raziskovalni in razvojni center bivšega federativnega statističnega urada v Pragi) bil ustanovljen center za računalniške raziskave (SIBIS 2003d).

Nekateri raziskovalni projekti so veliko prinesli k programom računalniške statistične obdelave podatkov, celo v okvirju združenih narodov in ekonomske komisije za Evropo v Ženevi. Še posebej izstopata projekta ISIS (Integrated Statistical Information System) in METIS (Meta information system for Statistics).

V zvezi z razširjanjem uporabe računalnikov in informatizacijo, je bila Slovaška, kot neodvisna država s 1. januarjem 1993 popolnoma na začetku (SIBIS 2003d). V veliki meri gre razloge za to iskati v že omenjeni izpostavljenosti negativnim vplivom zgodovinskega razvoja, v zvezi s vprašanji tehnoloških in komunikacijskih infrastruktur.

Po drugi strani pa je rojstvo nove države pomenilo tudi prosto pot in priložnost za nastanek svežih programov informatizacije. Vzporedno so morali v državnih institucijah in ostalih porah družbe uvajati IKT. Prvih nekaj let neodvisnosti so spremljali številni projekti, konec 90. let pa so praktično vsa ministrstva in ostale organizacije razvile samostojne informacijske sisteme, postavljene na temelje internetnih mrež. Preko njih so ponujali informacije o določenih institucijah, in omogočali dostop in približanje s pomočjo on-line komunikacije. Pojavljati so se začele spletne strani posameznih ministrstev, ostalih vladnih organov, nevladnih institucij in podjetij, ki so bile na voljo tudi v angleškem jeziku. Po svoji obliki so zelo raznovrstne, nimajo enotne oblike in skupne notranje strukture, kar nekoliko zniža njihovo praktično uporabo.

Podobno globalnemu trendu večine evropskih držav, v zvezi z informatizacijo družbe, je vlada 30. junija 1999 izdala sklep, da se ministri za transport, pošto in telekomunikacije sestanejo s predstavniki ostalih ministrstev in organov državne uprave, ter pripravijo strategijo za razvoj informacijske družbe v novem tisočletju. 1. januarja 2000 so se te naloge prenesle na ministrstvo za izobraževanje, ki je nato junija 2001 pripravilo strateški vladni dokument o politiki informatizacije družbe Republike Slovaške. Vlada ga je potrdila 13.6.2001 in podala naslednje zaključke: odobrava politiko informatizacije in se priključuje pobudam e-Evropske, širok pristop k vprašanju informatizacije družbe pa spoznava kot hkrati tudi strateški vladni cilj. Kasneje je bilo sprejetih še več zakonskih aktov (za varstvo osebnih podatkov v informacijskih sistemih, zagotavljanje javnega in zasebnega dostopa do informacij, v zvezi z elektronskim podpisom, o varovanju zaupnih podatkov, državnih statistikah), da bi omogočili potrebno zakonodajno osnovo za postopno implementacijo načel in strategije e-Evropske (SIBIS 2003d). Poleg področja zakonodaje je za nadaljnji razvoj informacijskega področja bil potreben tudi razvoj tehničnih in organizacijskih predpogojev. Oblikovana je bila posebna spletna stran (dostopno na <http://www.eEurope.sk>), kjer najdemo vse pomembne informacije v zvezi s tem vprašanjem, vključno s projekti e-Evropske in ostalimi programi ter raziskavami.

4.10 Slovenija

Naša država ima relativno dobro infrastrukturo IKT, vključno s pokritostjo osebnih računalnikov (ki je skoraj enako kot povprečje EU¹² iz sredine 90. let). Ker se je nivo razvoja v zadnjih letih znižal, pa kljub temu Slovenija zaradi nepreudarnih vlaganj v strukture IKT, že od leta 2000 vedno bolj zaostaja za EU. Vlada RS je zato podala cilje in poudarila pomembnost razvoja informacijske družbe. Januarja, leta 2001 je bilo ustanovljeno ministrstvo za informacijsko družbo; vprašanja informacijske družbe pa so vključena tudi v razvoj državnega razvojnega plana 2001-2006 (SIBIS 2003d).

V preteklosti je vlada RS dodelila večino sredstev za to področje, za javno uporabno in dostopno infrastrukturo IKT; od česar imajo največ koristi državljani. Kljub temu pa še ni zaznati večjega vpliva na pospešitev in razširitev e-poslovanja v ekonomski in javni sferi, ali povečanja zanimanja za dostop do uslug informacijske družbe. Eno najbolj izpostavljenih vprašanj v preteklih letih je bilo preureditev trga telekomunikacij, ki je, kljub mnogim pobudam, relativno počasno.

Oktobra 2002 je vlada sprejela strategijo za izvedbo informacijske družbe, ki jo je pripravilo ministrstvo za to področje in jo povzelo v strateškem dokumentu, imenovanem »RS v informacijski družbi«. Gre za povezavo s projektom eEvrope, ki je bil prevzet s strani držav kandidatki za vstop v EU, v Goteburgu (junija 2001). Namen države je opredeliti ukrepe za doseganje nivoja informacijske družbe EU do leta 2006; in sicer na naslednjih glavnih področjih: povečanje dostopa do infrastrukture IKT, z zagotavljanjem ustreznih regulativnih okvirjev; inovativen pristop in ureditev novih trgovskih priložnosti, s pospeševanjem sodelovanja med raziskovalnimi inštituti in ekonomisti IKT; vzpostavitev ustreznih pogojev za razvoj intelektualnega poslovanja (industrija IKT); uporaba IKT v izobraževalne namene; zagotovitev dostopa do uslug informacijske družbe za vse; ureditev digitalne vsebine in opredelitev njenih vplivov na kulturna in širša družbena področja, za ohranjanje kulturne dediščine in jezika; podrobna in temeljita predstavitev e-uslug, e-poslovanja ipd.; zmanjševanje digitalnega razkoraka, z zagotavljanjem enakosti za vse državljane, tudi za skupine iz marginaliziranih področij ali tistih, s posebnimi potrebami (SIBIS 2003d: 100).

¹² 1995 je bila stopnja pokritosti z osebnimi računalniki naslednja: 10% v Sloveniji in 14% v EU; leta 2001 je odstotek za Slovenijo enak 27,6 (EU 31%) (Sicherl 2001)

Ministrstvo za informacijsko družbo (kot se je takrat imenovalo) samo ni moglo uresničiti celotne strategije RS, zato sta odgovornost in financiranje razporejeni na več ministrstev, ki pokrivajo različna področja (telekomunikacije, izobraževanje, znanost, šport, ekonomijo, industrijo, finance, delo, družino in družbene zadeve, kulturo, notranje zadeve, javne odnose itd.). Z dnem 18.11.2004 sta pričeli veljati noveli Zakona o vladi (Uradni list RS 123/04 z dne 18.11.2004, ZVRS-D) in Zakona o državni upravi (Uradni list RS 123/04 z dne 18.11.2004, ZDU-1C), ki ukinjata Ministrstvo za informacijsko družbo, njegove naloge pa prenašata na Ministrstvo za gospodarstvo, novo ustanovljeno Ministrstvo za visoko šolstvo, znanost in tehnologijo, posamezne naloge "pospeševanja informacijske družbe" pa so, v skladu z novima zakonoma, opravljala druga resorno pristojna ministrstva. Novembra 2004 je torej sprejet »zakon o spremembah in dopolnitvah zakona o državni upravi« (ZDU-1C). S tem smo dobili Ministrstvo za visoko šolstvo, znanost in tehnologijo, ki opravlja naloge na področjih visokega šolstva, znanosti, raziskovanja, tehnologije, meroslovja in pospeševanja informacijske družbe na področjih, ki ne sodijo v delovna področja drugih ministrstev, in usklajevanja dela na področju informacijske družbe.

Med odmevnejšimi programi Slovenije pa omenimo še projekt »e-vas«, ki se je izvajal ob Madžarsko-Slovenski meji. Takratno Ministrstvo za informacijsko družbo (danes Ministrstvo za visoko šolstvo, znanost in tehnologijo¹³) je 30.8.2002 objavilo prvi javni razpis za pilotni projekt e-vas v občini Dobrovnik. Projekt naj bi pokazal, da je mogoče vzpostaviti ugodno okolje za razvoj informacijske družbe tudi na manj razvitih področjih ter premagati digitalno ločnico in na podeželje pripeljati sodobno tehnologijo, predvsem širokopasovne povezave ter večpredstavnostne komunikacije. V decembru 2003 (natančneje 16.12.) je v občini Dobrovnik blizu madžarske meje potekala slovesnost ob otvoritvi prenovljene dvojezične šole, pred tem pa so v prostorih občinske uprave predstavili pilotni projekt Ministrstva za informacijsko družbo »Informatizacija ruralnih zaselkov (e-vas)«. V projektu je sodeloval tudi Microsoft, ki je zagotovil programsko opremo. Pilotni projekt e-vasi je nadgradnja prvih korakov v smeri informatizacije slovenskega podeželja, ki so jih v Dobrovniku z odprtjem informacijsko-komunikacijskega centra na šoli storili že v letu prej¹⁴.

Med izjemno uspešne projekte sodita tudi storitvi e-uprava¹⁵ in e-dohodnina, ki se še uvaja.

¹³ dostopno na <http://www.mvzt.gov.si/>

¹⁴ dostopno na <http://www.agencijanet.si/microsoft-v-projektu-e-vas/>

¹⁵ dostopno na <http://e-uprava.gov.si/e-uprava/>

5. SKRB ZA VARNOST

Varstvo osebnih podatkov in dostop do informacij javnega značaja intenzivneje posega v naša življenja in nas vznemirja šele v zadnjem času (Čebulj 2005).

Danes je internet najhitrejši in najcenejši vir podatkov, ki je nenehno na voljo vse večjemu številu prebivalstva (saj se dostop do interneta ceni in izboljšuje). Postal je močno sredstvo medijev, ustanov, organizacij in posameznikov, ki želijo širšemu krogu ljudi posredovati določeno sporočilo (Vurušič 2006).

Z razvojem internetnih uslug pa smo deležni tako pozitivnih, kot negativnih plati. Hitro lahko iščemo podatke, si jih izmenjujemo in hkrati komuniciramo s prijatelji in znanci; hkrati pa so naši računalniki lahko žrtev virusa, vdorov raznih hekerjev, ali pa naš poštni predal napada kup nezaželene oglasne pošte.

Na prvi pogled ne zglada nič resnega in ne vzbuja skrbi, vendar tovrstni napadi lahko vodijo h kvarjenju našega računalnika, v smislu kvarjenja podatkov, sistemov, onemogočanja delovanja omrežij (virus, ki povzroča ugašanje računalnika ali briše datoteke, ki so na njem); hkrati pa lahko gre tudi za poseganje v zasebnost, krajo informacij (vdor v bazo podatkov, ki niso namenjeni javnosti) ipd.

Ljudje se v življenju vedno soočamo z različnimi tveganji in moramo velikokrat pretehtati dobre in slabe lastnosti posameznega orodja, da se nato lahko odločimo ali ga bomo kljub temu uporabljali. Podobno je tudi pri internetu. Če je uporabnik previden in upošteva vsa navodila, so možnosti, da se mu kaj pripeti, manjše (Vurušič 2006: 5).

Prvi korak k varni uporabi interneta je že samo zavedanje, da nevarnost sploh obstaja. Menim, da so v prednosti ljudje, ki že dalj časa uporabljajo to omrežje, v katero je povezana množica računalnikov po vsem svetu, saj so si imeli možnost pridobiti bogate izkušnje, tudi če se niso obnašali tvegano.

Vsakemu od nas se je že kdaj pri vsakodnevnem delu in brskanju po internetu pojavilo okno, ki ponuja mamljive vsebine (casino, poker, zadetek na loteriji za katero sploh še nismo slišali) in mnogi so kdaj z levim klikom miške sprejeli tovrstne izzive. In potem se ni zgodilo nič. Pripeljalo nas je do naslednjega okna in potem še do petero drugih. Vse skupaj se nam je zdelo butasto, pri tem pa še opazili nismo, da omogočamo nekomu od zunaj spremljanje našega početja, da nam pri tem mogoče pošilja kakšne paketke, ki smo jih seveda pridno naložili na računalnik in so nam šele kasneje, ko smo že tretjič obiskali računalniški servis, povedali, da so to potencialni virusi.

Iz navedenega sledi, da bi bili (H3) *ljudje, ki redno uporabljajo internet, prej pripravljeni prijaviti kršitve varnosti ali zasebnost* (saj bi jih v prvi vrsti najbrž tudi lažje prepoznali in bi posledično tudi zato prijavo bilo lažje izvesti), (H4) *pri čemer bi jim bilo vseeno, ali je prijava anonimna ali ne.*

6. METODOLOGIJA

Raziskave, ki presegajo meje ene družbe v eni časovni točki zgodovine so mednarodne. Le-te nam zagotavljajo zelo uporabne metode za nastanek, preverjanje in nadaljnji razvoj socioloških teorij (Kohn M.L. 1989, V MESPA 2002-2003). Gre za komparativno metodologijo, kjer (povsod) z enakim raziskovalnim instrumentom merimo, kako se dve ali več držav odziva na razno-razne družbeno-kulturne dogodke. Lahko se nam zgodi, da rezultatov ne moremo aplicirati na druge države ali družbe. Pri delu skušamo uporabiti Millsova priporočila induktivne logike, da bi videli kaj je podobnega v populacijah, kjer dobimo podobne rezultate in kaj je različnega pri tistih populacijah, kjer so rezultati različni (Nowak S. 1989, V MESPA 2002-2003). Takšne raziskave so izjemno drage in zahtevne, zato jih ne izvajamo dokler nimamo za to dobrega razloga; t.j. v primerih, ko določenega pojava ne moremo pojasniti s preučevanjem ene države ali družbe. Omogočajo nam namreč sveže, razburljive vpoglede in globlje razumevanje problemov različnih držav; saj se je pri tovrstnih raziskavah, za razumevanje miselnosti druge (tuje) kulture, potrebno vživeti v različne kulturne vidike in hkrati ponovno razmisliti o svoji državi, prav tako iz položaja zunanjega opazovalca.

Sociologi niso zelo homogeni (isto-misleči, složni), imajo različne odnose do posameznih vprašanj in se nenazadnje razlikujejo tudi v njihovih pristopih h komparativnemu raziskovanju.

6.1 Predmet in cilji proučevanja

Za obravnavo svoje diplomske naloge sem si izbrala problematiko interneta, oziroma odnos do njegove (varne) uporabe; saj ga ljudje po mojem mnenju pogosto sprejemajo zaletavo, brez predsodkov in odprtih rok, pri tem pa jim manjka vsaj kanček kritičnosti in zavedanja, da tudi v tem navideznem svetu velja biti previden.

Poskušala sem raziskati odnos različnih evropskih držav do tega vprašanja, pri tem pa upoštevati različne dejavnike, kot so: razvoj infrastrukture, časovna prisotnost pojava in kulturni vplivi.

V nalogi sem najprej raziskovala kateri so osnovni pogoji za vzpostavitev kritičnega odnosa do (varne) uporabe interneta, v nadaljevanju podala še podatke o značilnostih in aktivnostih različnih evropskih držav pri uporabi interneta ter, kako skrbijo za varnost uporabe interneta.

6.2 Uporabljene metode

Pri izdelavi diplomskega dela sem pretežno uporabila analizo sekundarnih podatkov, deskriptivne in primerjalne metode analize. Glavna metoda za sintezo je bila sistematična vsebinska analiza raziskave iz projekta evropske komisije, imenovanega SIBIS (angl. Statistical Indicators Benchmarking the Information Society), in nekaterih pisnih virov povezanih z njim. Poleg tega sem pregledala še vsebino relevantnih knjig, člankov, podatke z interneta ipd., s katerimi sem skušala empirično preveriti svoje hipoteze, jih na osnovi analize¹⁶ baze podatkov¹⁷ ter s pomočjo obstoječih teorij dokazati oziroma zavrniti. Za potrebe naloge sem uporabila vse enote o novo pridruženih članicah EU (NAS) iz baze podatkov – gre torej za pragmatično izbiro enot.

¹⁶ narejene s pomočjo programskega paketa za statistično obdelavo podatkov SPSS

¹⁷ le-te mi je zaupala Fakulteta za družbene vede, kot ena izmed fakultet, ki je pri izvedbi samega projekta tudi sodelovala

6.2.1 Empirična raziskava – SIBIS

Projekt SIBIS se je izvajal v na novo pridruženih članicah evropske unije (NAS), januarja 2003 (intervjuji so potekali med 1. in 31. januarjem). Anketiranje je bilo osebno (PAPI – angl. personal aided personal interviews); koordinirano in izvedeno s strani Češke organizacije NFO AISA iz Prage. Zajemalo je populacijo oseb, starih 15 ali več let. Skupno je bilo, v jeziku posameznih držav, opravljenih 10.379 intervjujev (približno 1000 na državo). Povprečna dolžina anketiranja je variirala med 20 (Romunija) in 40 minutami (Litva).

Da bi zadostili kriterijem primerljivosti podatkov, je za raziskavo bil narejen enoten vprašalnik in izvedena enaka vzorčna metoda (npr. metoda naslednjega rojstnega dne ali Kisheva metoda izbora oseb); izjema je bila Bolgarija, kjer so uporabili kvoto. Baza podatkov obsega približno 160 spremenljivk.

Raziskava pokriva različna področja¹⁸:

- dostopnost, ažurnost, zmožljivost in zanesljivost informacijsko-komunikacijske infrastrukture (IKT)
- znanje in odnosi (mnenja, strahovi in dvomi) povezani z uporabo IKT
- sodelovanje in pripravljenost uporabe uslug različnih IKT uporabnih področij, kot so e-učenje, e-delo, e-trgovina, e-zdravje in e-vlada.

Da bi zagotovili zanesljive in primerljive podatke, so morali prilagoditi še neutežene vzorčne strukture na uradne statistike, utežene vzorčne strukture na populacijo držav NAS, in na Poljskem ter v Sloveniji pretvoriti vzorce gospodinjstev v osebno vzorčenje.

Gre za projekt, sestavljen iz številnih študij posameznih držav. Da bi si lahko predstavljali ozadje raziskave in si s tem pomagali pri pravilnem interpretiranju podatkov, so raziskovalci in vse države, ki so pri projektu sodelovale preučevali zakonita, politična, institucionalna in poslovna ozadja razpršenosti IKT. S to dodatno informacijsko vrednostjo je torej SIBIS-ova baza podatkov primerna za aplikacijo na druge raziskave, npr. za primerjavo z učinkovitostjo IKT ostalih evropskih držav.

¹⁸ za potrebe naloge bomo podrobneje pregledali in v raziskavo vključili internetne kazalce in varno informacijsko infrastrukturo (prvi dve alineji)

6.2.1.1 Internetni kazalci - vpliv dostopnosti interneta na vzpostavitev kritičnega odnosa do uporabe

Leta 2002 (eEurope 2002 Action Plan) se je politika evropske unije osredotočala na razširitev internetne povezanosti po Evropi, kasneje (projekt eEurope 2005), ko so predvidevali, da je ta cilj dosežen vsaj v večjem delu Evrope, pa so želeli vzpodbuditi njegovo ekonomsko produktivnost in boljše, predvsem pa boljše dostopne in podprte usluge za vse prebivalce Evrope, podkrepljene z varno in povsod dostopno, prostrano infrastrukturo.

Po podatkih poročila (eEurope+ Progress) iz leta 2001, je v povprečju 77% gospodinjstev v NAS državah imelo urejeno telefonsko povezavo. Če primerjamo odstotek s takratnimi evropskimi državami¹⁹ (EU 15), je bil le-ta tam večji za 11 odstotnih točk (86%). Žal v mnogih na novo pridruženih državah torej nimajo niti generalne pokritosti s telefonskimi linijami, posodobitev telefonskega omrežja je še daleč, ali pa vsaj še ni končana; na ruralnih področjih imajo še vedno stare analogne sisteme, ki onemogočajo ali vsaj močno znižujejo kvaliteto internetne povezave. Vse to povzroča ogromne in na kratki rok nepremagljive prepreke za razmah interneta.

Morda je prihodnost v internetnih povezavah, ki so neodvisne od podpore telefonske infrastrukture (kabelski internet ipd.), vendar si težko predstavljamo, da bi države, ki že tako zaostajajo v razvoju bile sposobne preskočiti določene nivoje in ponuditi kaj tako »novega in naprednega«. Rešitev bi lahko bila na primer v tujih vlaganjih.

NAS se še vedno soočajo s problemom, kako razviti dovolj poceni in zanesljivo komunikacijsko infrastrukturo in skozi liberalizacijo vzpodbuditi vsaj osnovno uporabo interneta. Ko bo takšna infrastruktura enkrat razvita, pa najbrž ne bo več zavor in preprek, da se internet ne bi razmahnil tudi na ta področja. Ker smo neučakani, ko je govora o napredku in z odprtimi rokami sprejemamo nove stvari, ki nam prinašajo vidne pozitivne spremembe, na tem mestu še ne razmišljamo o možnih posledicah v ozadju, ki ob tem pritičejo; zato sklepam, da se *(HI) ljudje, ki dalj časa uporabljajo internet, bolj zavedajo nevarnosti, ki jih le-ta prinaša.*

¹⁹ Avstrija, Belgija, Nemčija, Danska, Grčija, Španija, Francija, Finska, Italija, Irska, Luksemburg, Nizozemska, Portugalska, Švedska, Velika Britanija

6.2.1.2 Varna informacijska infrastruktura – vpliv občutka varnosti in zanesljivosti na vzpostavitev kritičnega odnosa do uporabe

V zvezi s vprašanji o varnosti omrežja, kriminala na internetu in direktiv o varnosti podatkov, poslanih preko elektronskih komunikacij, je evropska unija skušala uveljaviti obširno strategijo, ki bi zajela celotno območje evropskega prostora. Novi mejnik je bil postavljen na osnovi resolucije 28.januarja 2002²⁰, s katero so do konca leta 2002 predvideli izpolnitev mnogih pobud (za vzpostavitev varnosti, osveščanje ljudi, oglaševanje pozitivnih izkušenj in novih možnosti izmenjave informacij), kar pomeni pomemben korak naproti varni informacijski infrastrukturi v Evropi²¹.

Podobno je bila z načrtom »eEurope+ 2003 Action plan« predstavljena gradnja samozavesti in zaupanja pri e-trgovini, kot enem največjih izzivov znotraj NAS. Države se močno zavedajo, da bodo varstvo omrežij, pridobitev in povečanje zaupanja uporabnikov, nadaljnji razvoj in uporaba »pametnih« plačilnih kartic (uporabljenih pri plačevanju preko spleta), pridobljeni samo s sodelovanjem in vzajemnostjo z razvijanjem infrastrukture.

Aktivnosti tako vključujejo varnostne mehanizme, ki pa jih vodi industrija. Iz tega sledi potreba po sodelovanju javnega in zasebnega, saj so po drugi strani tudi informacijske infrastrukture odvisne od uporabnikov. Za obojestranske koristi bi tako morali vzpodbujati zakonsko uveljavljanje in zagotavljanje varnosti.

Po drugi strani pa poznamo tudi primere, ko je razvoj vodil industrijo. Kot primer lahko navedemo primer spletnega bančništva, kjer je varnost poslovanja ključnega pomena; zato so banke zahtevale razvoj in uvedbo varnostnih mehanizmov, certifikatov in s tem na nek način usmerjale razvoj industrije tudi v to smer.

Sledil je projekt »eEurope 2005«, v katerem so bili osvetljeni trije cilji: uresničitev varnosti na internetu, zastavljene sredi leta 2003; doseganje nivoja »kulture varnosti«, v smislu zasnove in izvedbe varne IKT do konca leta 2005; in nenazadnje, ustanovitev takega okolja komunikacije, ki bo varno tudi za izmenjavo zaupnih vladnih informacij.

²⁰ 28 January Resolution 2002

²¹ eEurope 2005: An information society for all. V SIBIS 2003d

Evropska unija je torej izvedla več projektov in predstavila kar nekaj strategij za vzpostavitev varnega omrežja. Raziskava, ki jo uporabljamo za potrebe svoje naloge le delno pokriva obravnavo »e-Europe 2005« kazalcev, ki predstavljajo tudi najobsežnejšo raziskavo tovrstne problematike v zvezi z varno informacijsko infrastrukturo. e-Europe projekt je namreč zajemal tako izkušnje uporabnikov interneta, kot uporabo glede na dojemanje varnosti IKT; projekt SIBIS-a pa se je le rahlo dotaknil slednjega - skrbi pri uporabi interneta.

Kljub temu menim, da podatki zadostujejo za preverjanje domneve, da so *(H2) ljudje v državah, kjer je internet bolj razširjen, manj zaskrbljeni nad varnostjo, zasebnostjo in zaupnostjo podatkov, ki se prenašajo preko interneta*. Pri tem kot razširjenost obravnavamo dostop do interneta doma (več kot imajo ljudje doma internetnih priključkov, bolj razširjen domnevamo, da je internet).

6.3 Povzetek hipotez

Za boljši pregled ciljev naše raziskave povzeman hipoteze, ki so nastale ob pregledu teoretskih izhodišč iz že narejenih raziskav, in katerih veljavnost bomo preverili v sledečem, empiričnem delu naloge.

H1: Ljudje, ki dalj časa uporabljajo internet, se bolj zavedajo nevarnosti, ki jih le-ta prinaša.

H2: Ljudje v državah, kjer je internet bolj razširjen, so manj zaskrbljeni nad varnostjo, zasebnostjo in zaupnostjo podatkov, ki se prenašajo preko interneta.

H3: Ljudje, ki redno uporabljajo internet, bi bili prej pripravljeni prijaviti kršitve varnosti ali zasebnosti..

H4: Ljudem, ki redno uporabljajo internet, je vseeno ali je prijavita kršitve varnosti ali zasebnosti anonimna ali ne.

V nadaljevanju diplomske naloge sledijo rezultati empiričnega dela raziskave. Z analizo podatkov SIBIS-a, izvedene s pomočjo programskega paketa za statistično obdelavo podatkov SPSS, bom preverila delovne hipoteze, in jih skušala potrditi ali ovreči .

7. REZULTATI

7.1 Zavedanje nevarnosti

Pod pojmom nevarnost v našem primeru razumemo varnostne kršitve prenosa podatkov in kršitve varnosti in zasebnosti, ki jih bomo podrobneje obravnavali še nekoliko kasneje (v poglavju 7.2). Najprej bomo pogledali kakšna je skrb za varnost glede na dolžino obdobja uporabe interneta. Vprašanje v raziskavi se je glasilo: ***Kdaj ste prvič uporabili internet?*** Primerjali smo uporabnike v kategorijah: pred manj kot 6 meseci, pred 6 do 12 meseci, pred 1 do 2 letoma, pred več kot 2 letoma, ne vem.

Naslednje relevantno vprašanje v povezavi s prakso uporabe interneta je bilo: ***V kolikšni meri ste zaskrbljeni glede varnosti podatkov na internetu, npr. glede izgube ali zlorabe vaših podatkov?*** Možni odgovori pa so bili: zelo zaskrbljeni, nekoliko zaskrbljeni, niste zaskrbljeni, ne vem.

Rezultati, v zvezi z zaskrbljenostjo nad varnostjo podatkov, ki se prenašajo preko interneta, so pokazali (glej tabelo 7.1.1), da so ljudje, ki dalj časa uporabljajo internet, v primerjavi s tistimi, ki ga uporabljajo manj kot eno leto dejansko veliko bolj zaskrbljeni; s čimer potrjujem svojo prvo hipotezo (H1). Kljub temu pa anketiranci v obravnavanih državah v splošnem ne kažejo pretiranega zanimanja za to problematiko. Nekoliko so v skrbeh le prebivalci Češke, Estonije, Romunije in Slovenije; zelo zaskrbljeni pa le Latvijci in Poljaki, ki po največji zaskrbljenosti med vsemi zelo izstopajo.

Sledilo je vprašanje: ***V kolikšni meri ste zaskrbljeni glede zasebnosti in zaupnosti na internetu, npr. glede zlorabe vaših podatkov s strani tretje osebe?*** Možni odgovori so bili enaki kot pri zgoraj navedenem vprašanju.

O vprašanju zasebnosti in zaupnosti, glede na časovno uporabo interneta, lahko rečemo podobno, kot pri vprašanju v zvezi z zaskrbljenostjo glede varnosti. Med vsemi državljani po visoki stopnji skrbi izstopajo Latvijci, Poljaki in Romuni; po izraziti ne-zaskrbljenosti pa velja izpostaviti prebivalce Bolgarije in Madžarske. Ostali anketiranci (med njimi tudi Slovenci) se do tega problema ne opredeljujejo v nobeno smer, in so glede tega vprašanja le nekoliko zaskrbljeni (glej tabelo 7.1.2). Če primerjam podatke obeh tabel, ugotovim, da so ljudje, v t.i. novo pridruženih članicah evropske unije, vseeno bolj zaskrbljeni nad slednjim vprašanjem.

Tabela 7.1.1 – Varnost podatkov na internetu – vpliv prve uporabe

država			varnost podatkov na internetu				
			zelo zaskrbljeni	nekoliko zaskrbljeni	niste zaskrbljeni	ne vem	skupaj
BG	prva uporaba interneta	pred manj kot 6 meseci	14.3 % (2)	28.6 % (4)	42.9 % (6)	14.3 % (2)	100 % (14)
		pred 6 do 12 meseci	10.0 (3)	20.0 (6)	56.7 (17)	13.3 (4)	100 (30)
		pred 1 do 2 letoma	2.7 (2)	31.5 (23)	63.0 (46)	2.7 (2)	100 (73)
		pred več kot 2 letoma	4.0 (4)	37.4 (37)	57.6 (57)	1.0 (1)	100 (99)
skupaj			5.0 (11)	32.6 (71)	58.3 (127)	4.1 (9)	100 (218)
CZ	prva uporaba interneta	pred manj kot 6 meseci	17.1 (6)	28.6 (10)	40.0 (14)	14.3 (5)	100 (35)
		pred 6 do 12 meseci	3.4 (2)	36.2 (21)	43.1 (25)	17.2 (10)	100 (58)
		pred 1 do 2 letoma	7.6 (11)	44.4 (64)	40.3 (58)	7.6 (11)	100 (144)
		pred več kot 2 letoma	9.7 (16)	53.3 (88)	31.5 (52)	5.5 (9)	100 (165)
skupaj			8.8 (36)	45.3 (186)	37.0 (152)	9.0 (37)	100 (411)
EE	prva uporaba interneta	pred manj kot 6 meseci	0.0 (0)	40.0 (2)	60.0 (3)	0.0 (0)	100 (5)
		pred 6 do 12 meseci	10.0 (1)	30.0 (3)	50.0 (5)	10.0 (1)	100 (10)
		pred 1 do 2 letoma	5.3 (1)	42.1 (8)	42.1 (8)	10.5 (2)	100 (19)
		pred več kot 2 letoma	9.8 (5)	51.0 (26)	35.3 (18)	3.9 (2)	100 (51)
skupaj			8.2 (7)	45.9 (39)	40.0 (34)	5.9 (5)	100 (85)
HU	prva uporaba interneta	pred manj kot 6 meseci	0.0 (0)	27.8 (5)	66.7 (12)	5.6 (1)	100 (18)
		pred 6 do 12 meseci	16.7 (3)	22.2 (4)	61.1 (11)	0.0 (0)	100 (18)
		pred 1 do 2 letoma	1.5 (1)	21.5 (14)	67.7 (44)	9.2 (6)	100 (65)
		pred več kot 2 letoma	4.9 (6)	28.5 (35)	60.2 (74)	6.5 (8)	100 (123)
skupaj			4.4 (10)	25.8 (58)	63.1 (142)	6.7 (15)	100 (225)
LV	prva uporaba interneta	pred manj kot 6 meseci	20.0 (1)	20.0 (1)	40.0 (2)	20.0 (1)	100 (5)
		pred 6 do 12 meseci	45.5 (5)	27.3 (3)	27.3 (3)	0.0 (0)	100 (11)
		pred 1 do 2 letoma	34.8 (8)	34.8 (8)	26.1 (6)	4.3 (1)	100 (23)
		pred več kot 2 letoma	50.0 (23)	30.4 (14)	19.6 (9)	0.0 (0)	100 (46)
skupaj			42.5 (37)	29.9 (26)	25.3 (22)	2.3 (2)	100 (87)
LT	prva uporaba interneta	pred manj kot 6 meseci	17.6 (3)	23.5 (4)	47.1 (8)	11.8 (2)	100 (17)
		pred 6 do 12 meseci	11.1 (2)	38.9 (7)	33.3 (6)	16.7 (3)	100 (18)
		pred 1 do 2 letoma	8.3 (3)	25.0 (9)	47.2 (17)	19.4 (7)	100 (36)
		pred več kot 2 letoma	12.3 (7)	38.6 (22)	43.9 (25)	5.3 (3)	100 (57)
skupaj			11.7 (15)	32.8 (42)	43.8 (56)	11.7 (15)	100 (128)
PL	prva uporaba interneta	pred manj kot 6 meseci	8.8 (5)	59.6 (34)	21.1 (12)	10.5 (6)	100 (57)
		pred 6 do 12 meseci	26.4 (23)	50.6 (44)	17.2 (15)	5.7 (5)	100 (87)
		pred 1 do 2 letoma	38.3 (90)	35.3 (83)	20.4 (48)	6.0 (14)	100 (235)
		pred več kot 2 letoma	46.1 (239)	38.8 (201)	13.1 (68)	1.9 (10)	100 (518)
skupaj			39.9 (369)	39.6 (366)	16.4 (152)	4.1 (38)	100 (925)
RO	prva uporaba interneta	pred manj kot 6 meseci	31.8 (7)	9.1 (2)	40.9 (9)	18.2 (4)	100 (22)
		pred 6 do 12 meseci	22.4 (13)	41.4 (24)	32.8 (19)	3.4 (2)	100 (58)
		pred 1 do 2 letoma	11.4 (17)	35.6 (53)	51.7 (77)	1.3 (2)	100 (149)
		pred več kot 2 letoma	30.2 (62)	40.0 (82)	29.8 (61)	0.0 (0)	100 (205)
skupaj			22.8 (99)	37.1 (161)	38.2 (166)	1.8 (8)	100 (434)
SK	prva uporaba interneta	pred manj kot 6 meseci	0.0 (0)	41.7 (5)	58.3 (7)	0.0 (0)	100 (12)
		pred 6 do 12 meseci	11.1 (4)	44.4 (16)	44.4 (16)	0.0 (0)	100 (36)
		pred 1 do 2 letoma	12.7 (7)	32.7 (18)	50.9 (28)	3.6 (2)	100 (55)
		pred več kot 2 letoma	18.6 (11)	40.7 (34)	39.0 (23)	1.7 (1)	100 (59)
skupaj			13.5 (22)	39.3 (64)	45.4 (74)	1.8 (3)	100 (163)
SI	prva uporaba interneta	pred manj kot 6 meseci	0.0 (0)	33.3 (1)	66.7 (2)	0.0 (0)	100 (3)
		pred 6 do 12 meseci	14.3 (1)	42.9 (3)	42.9 (3)	0.0 (0)	100 (7)
		pred 1 do 2 letoma	11.8 (2)	47.1 (8)	41.2 (7)	0.0 (0)	100 (17)
		pred več kot 2 letoma	15.9 (10)	49.2 (31)	33.3 (21)	1.6 (1)	100 (63)
skupaj			14.3 (23)	48.4 (44)	36.3 (33)	1.1 (1)	100 (91)

Tabela 7.1.2 – Zasebnost in zaupnost na internetu – vpliv prve uporabe

država			zasebnost in zaupnost na internetu				
			zelo zaskrbljeni	nekoliko zaskrbljeni	niste zaskrbljeni	ne vem	skupaj
BG	prva uporaba interneta	pred manj kot 6 meseci	15.4 % (2)	30.8 % (4)	38.5 % (5)	15.4 % (2)	100% (13)
		pred 6 do 12 meseci	10.0 (3)	26.7 (8)	53.3 (16)	10.0 (3)	100 (30)
		pred 1 do 2 letoma	4.1 (3)	28.8 (21)	64.4 (47)	2.7 (2)	100 (73)
		pred več kot 2 letoma	5.1 (5)	39.4 (39)	54.5 (54)	1.0 (1)	100 (99)
		skupaj	6.0 (13)	33.6 (73)	56.7 (123)	3.7 (8)	100 (217)
CZ	prva uporaba interneta	pred manj kot 6 meseci	19.4 (7)	27.8 (10)	36.1 (13)	16.7 (6)	100 (36)
		pred 6 do 12 meseci	8.8 (5)	35.1 (20)	45.6 (26)	10.5 (6)	100 (57)
		pred 1 do 2 letoma	12.5 (18)	45.8 (66)	37.5 (54)	4.2 (6)	100 (144)
		pred več kot 2 letoma	16.3 (27)	53.0 (88)	27.7 (46)	3.0 (5)	100 (166)
		skupaj	14.1 (58)	45.6 (188)	34.5 (142)	5.8 (24)	100 (412)
EE	prva uporaba interneta	pred manj kot 6 meseci	0.0 (0)	40.0 (2)	60.0 (3)	0.0 (0)	100 (5)
		pred 6 do 12 meseci	10.0 (1)	30.0 (3)	50.0 (5)	10.0 (1)	100 (10)
		pred 1 do 2 letoma	10.5 (2)	36.8 (7)	42.1 (8)	10.5 (2)	100 (19)
		pred več kot 2 letoma	12.0 (6)	52.0 (26)	34.0 (17)	2.0 (1)	100 (50)
		skupaj	10.7 (9)	45.2 (38)	39.3 (33)	4.8 (4)	100 (84)
HU	prva uporaba interneta	pred manj kot 6 meseci	5.6 (1)	27.8 (5)	61.1 (11)	5.6 (1)	100 (18)
		pred 6 do 12 meseci	33.3 (6)	11.1 (2)	55.6 (10)	0.0 (0)	100 (18)
		pred 1 do 2 letoma	7.6 (5)	21.2 (14)	62.1 (41)	9.1 (6)	100 (66)
		pred več kot 2 letoma	8.9 (11)	30.6 (38)	56.5 (70)	4.0 (5)	100 (124)
		skupaj	10.1 (23)	26.0 (59)	58.6 (133)	5.3 (12)	100 (227)
LV	prva uporaba interneta	pred manj kot 6 meseci	40.0 (2)	40.0 (2)	20.0 (1)	0.0 (0)	100 (5)
		pred 6 do 12 meseci	60.0 (6)	20.0 (2)	20.0 (2)	0.0 (0)	100 (10)
		pred 1 do 2 letoma	41.7 (10)	33.3 (8)	20.8 (5)	4.2 (1)	100 (24)
		pred več kot 2 letoma	56.5 (26)	23.9 (11)	17.4 (8)	2.2 (1)	100 (46)
		skupaj	50.6 (44)	27.6 (24)	19.5 (17)	2.3 (2)	100 (87)
LT	prva uporaba interneta	pred manj kot 6 meseci	17.6 (3)	23.5 (4)	41.2 (7)	17.6 (3)	100 (17)
		pred 6 do 12 meseci	10.5 (2)	42.1 (8)	31.6 (6)	15.8 (3)	100 (19)
		pred 1 do 2 letoma	11.1 (4)	25.0 (9)	44.4 (16)	19.4 (7)	100 (36)
		pred več kot 2 letoma	17.9 (10)	41.1 (23)	33.9 (19)	7.1 (4)	100 (56)
		skupaj	14.8 (19)	34.4 (44)	37.5 (48)	13.3 (17)	100 (128)
PL	prva uporaba interneta	pred manj kot 6 meseci	24.1 (14)	55.2 (32)	20.7 (12)	0.0 (0)	100 (58)
		pred 6 do 12 meseci	48.3 (42)	34.5 (30)	11.5 (10)	5.7 (5)	100 (87)
		pred 1 do 2 letoma	35.3 (83)	51.1 (120)	9.4 (22)	4.3 (10)	100 (235)
		pred več kot 2 letoma	47.2 (245)	42.4 (220)	8.1 (42)	2.3 (12)	100 (519)
		skupaj	42.7 (396)	44.9 (417)	9.5 (88)	2.9 (27)	100 (928)
RO	prva uporaba interneta	pred manj kot 6 meseci	42.9 (9)	19.0 (4)	19.0 (4)	19.0 (4)	100 (21)
		pred 6 do 12 meseci	30.5 (18)	40.7 (24)	28.8 (17)	0.0 (0)	100 (59)
		pred 1 do 2 letoma	18.9 (28)	38.5 (57)	42.6 (63)	0.0 (0)	100 (148)
		pred več kot 2 letoma	43.6 (89)	35.3 (72)	21.1 (43)	0.0 (0)	100 (204)
		skupaj	33.3 (144)	36.3 (157)	29.4 (127)	0.9 (4)	100 (432)
SK	prva uporaba interneta	pred manj kot 6 meseci	7.7 (1)	61.5 (8)	30.8 (4)	0.0 (0)	100 (13)
		pred 6 do 12 meseci	16.7 (6)	50.0 (18)	30.6 (11)	2.8 (1)	100 (36)
		pred 1 do 2 letoma	18.2 (10)	36.4 (20)	41.8 (23)	3.6 (2)	100 (55)
		pred več kot 2 letoma	27.1 (16)	42.4 (25)	27.1 (16)	3.4 (2)	100 (59)
		skupaj	20.1 (33)	43.9 (72)	32.9 (54)	3.0 (5)	100 (164)
SI	prva uporaba interneta	pred manj kot 6 meseci	0.0 (0)	33.3 (1)	66.7 (2)	0.0 (0)	100 (3)
		pred 6 do 12 meseci	14.3 (1)	42.9 (3)	42.9 (3)	0.0 (0)	100 (7)
		pred 1 do 2 letoma	22.2 (4)	44.4 (8)	33.3 (6)	0.0 (0)	100 (18)
		pred več kot 2 letoma	18.8 (12)	45.3 (29)	34.4 (22)	1.6 (1)	100 (64)
		skupaj	19.1 (18)	44.7 (42)	35.1 (33)	1.1 (1)	100 (94)

7.2 Zaskrbljenost nad varnostjo, zasebnostjo in zaupnostjo

V povezavi s prvo hipotezo sem podrobneje pregledala zaskrbljenost nad varnostjo, zasebnostjo in zaupnostjo; tokrat v odvisnosti od tega, ali imajo ljudje internetne priključke doma.

Novo vprašanje iz ankete, na katerega sem se torej naslanjala, se glasi: *Ali imate doma dostop do interneta?* Anketiranci so imeli na voljo sicer tri odgovore (da, ne, ne vem), vendar smo pri analizi uporabili samo »da« in »ne«, saj odgovor »ne vem« ni uporabna kategorija.

Tabela 7.2.1 – Varnost podatkov na internetu - vpliv dostopa doma

država	varnost podatkov na internetu						skupaj
	zelo zaskrbljeni	nekoliko zaskrbljeni	niste zaskrbljeni	ne vem			
BG	dostop do interneta da	7.1 % (5)	38.6 % (27)	50.0 % (35)	4.3 % (3)	100 % (70)	
	doma ne	4.1 (6)	29.7 (44)	62.2 (92)	4.1 (6)	100 (148)	
	skupaj	5.0 (11)	32.6 (71)	58.3 (127)	4.1 (9)	100 (218)	
CZ	dostop do interneta da	10.1 (19)	49.5 (93)	32.4 (61)	8.0 (15)	100 (188)	
	doma ne	7.6 (17)	42.2 (94)	40.8 (91)	9.4 (21)	100 (223)	
	skupaj	8.8 (36)	45.5 (187)	37.0 (152)	8.8 (36)	100 (411)	
EE	dostop do interneta da	10.5 (4)	52.6 (20)	34.2 (13)	2.6 (1)	100 (38)	
	doma ne	6.3 (3)	41.7 (20)	43.8 (21)	8.3 (4)	100 (48)	
	skupaj	8.1 (7)	46.5 (40)	39.5 (34)	5.8 (5)	100 (86)	
HU	dostop do interneta da	6.3 (6)	35.8 (34)	56.8 (54)	1.1 (1)	100 (95)	
	doma ne	3.8 (5)	18.3 (24)	67.2 (88)	10.7 (14)	100 (131)	
	skupaj	4.9 (11)	25.7 (58)	62.8 (142)	6.6 (15)	100 (226)	
LV	dostop do interneta da	53.3 (8)	33.3 (5)	13.3 (2)	0.0 (0)	100 (15)	
	doma ne	41.1 (30)	28.8 (21)	26.0 (19)	4.1 (3)	100 (73)	
	skupaj	43.2 (38)	29.5 (26)	23.9 (21)	3.4 (3)	100 (88)	
LT	dostop do interneta da	17.6 (6)	44.1 (15)	35.3 (12)	2.9 (1)	100 (34)	
	doma ne	9.8 (9)	28.3 (26)	47.8 (44)	14.1 (13)	100 (92)	
	skupaj	11.9 (15)	32.5 (41)	44.4 (56)	11.1 (14)	100 (126)	
PL	dostop do interneta da	45.8 (193)	38.5 (162)	14.0 (59)	1.7 (7)	100 (421)	
	doma ne	35.0 (177)	40.1 (203)	18.6 (94)	6.3 (32)	100 (506)	
	skupaj	39.9 (370)	39.4 (365)	16.5 (153)	4.2 (39)	100 (927)	
RO	dostop do interneta da	35.8 (29)	39.5 (32)	24.7 (20)	0.0 (0)	100 (81)	
	doma ne	20.0 (71)	36.3 (129)	41.1 (146)	2.5 (9)	100 (355)	
	skupaj	22.9 (100)	36.9 (161)	38.1 (166)	2.1 (9)	100 (436)	
SK	dostop do interneta da	18.6 (8)	41.9 (18)	39.5 (17)	0.0 (0)	100 (43)	
	doma ne	11.6 (14)	37.2 (45)	47.9 (58)	3.3 (4)	100 (121)	
	skupaj	13.4 (22)	38.4 (63)	45.7 (75)	2.4 (4)	100 (164)	
SI	dostop do interneta da	14.3 (8)	51.8 (29)	32.1 (18)	1.8 (1)	100 (56)	
	doma ne	15.8 (6)	42.1 (16)	36.8 (14)	5.3 (2)	100 (38)	
	skupaj	14.9 (14)	47.9 (45)	34.0 (32)	3.2 (3)	100 (94)	

Iz podatkov tabele 7.2.1 je razvidno podobno stanje, kot pri preverjanju prve hipoteze (H1). Bolgarijo, Madžarsko, Romunijo in Slovaško sploh ne skrbi prodiranje izkoriščevalnih orodij (napake, notranje grožnje ipd.), ki ogrožajo varnost podatkov na internetu. Nekaj skrbi kažejo anketiranci Češke, Estonije, Litve in Slovenije; ponovno pa izstopajo prebivalci Poljske. Izjemno zanimivo je, da so nad varnostjo podatkov na internetu, v večjem številu nekoliko zaskrbljeni tisti Poljaki, ki doma sploh ne dostopajo do svetovne mreže. Podobne rezultate dobim, ko obravnavam še drugi del problematike, t.j. zasebnost in zaupnost na internetu – le da se tokrat Romuni in Slovaki opredeljujejo kot nekoliko zaskrbljeni (glej tabelo 7.2.2).

Tabela 7.2.2 – Zasebnost in zaupnost na internetu – vpliv dostopa doma

država			zasebnost in zaupnost na internetu				
			zelo zaskrbljeni	nekoliko zaskrbljeni	niste zaskrbljeni	ne vem	skupaj
BG	dostop do interneta doma	da	5.7 % (4)	37.1 % (26)	54.3 % (38)	2.9 % (2)	100 % (70)
		ne	6.1 (9)	32.4 (48)	57.4 (85)	4.1 (6)	100 (148)
	skupaj		6.0 (13)	33.9 (74)	56.4 (123)	3.7 (8)	100 (218)
CZ	dostop do interneta doma	da	17.6 (33)	47.3 (89)	29.8 (56)	5.3 (10)	100 (188)
		ne	11.2 (25)	44.4 (99)	38.1 (85)	6.3 (14)	100 (223)
	skupaj		14.1 (58)	45.7 (188)	34.3 (141)	5.8 (24)	100 (411)
EE	dostop do interneta doma	da	13.2 (5)	50.0 (19)	34.2 (13)	2.6 (1)	100 (38)
		ne	10.4 (5)	39.6 (19)	41.7 (20)	8.3 (4)	100 (48)
	skupaj		11.6 (10)	44.2 (38)	38.4 (33)	5.8 (5)	100 (86)
HU	dostop do interneta doma	da	8.4 (8)	35.8 (34)	54.7 (52)	1.1 (1)	100 (95)
		ne	11.6 (15)	18.6 (24)	62.0 (80)	7.8 (10)	100 (131)
	skupaj		10.3 (23)	25.9 (58)	58.9 (132)	4.9 (11)	100 (226)
LV	dostop do interneta doma	da	56.3 (9)	31.3 (5)	12.5 (2)	0.0 (0)	100 (15)
		ne	48.6 (35)	26.4 (19)	20.8 (15)	4.2 (3)	100 (73)
	skupaj		50.0 (44)	27.3 (24)	19.3 (17)	3.4 (3)	100 (88)
LT	dostop do interneta doma	da	22.2 (8)	44.4 (16)	30.6 (11)	2.8 (1)	100 (34)
		ne	12.9 (12)	30.1 (28)	39.8 (37)	17.2 (16)	100 (92)
	skupaj		15.5 (20)	34.1 (44)	37.2 (48)	13.2 (17)	100 (126)
PL	dostop do interneta doma	da	53.4 (225)	39.0 (164)	7.4 (31)	0.2 (1)	100 (421)
		ne	33.8 (171)	49.6 (251)	11.5 (58)	5.1 (26)	100 (506)
	skupaj		42.7 (396)	44.8 (415)	9.6 (89)	2.9 (27)	100 (927)
RO	dostop do interneta doma	da	47.5 (38)	36.3 (29)	16.3 (13)	0.0 (0)	100 (81)
		ne	29.9 (106)	36.3 (129)	32.7 (116)	1.1 (4)	100 (355)
	skupaj		33.1 (144)	36.3 (158)	29.7 (129)	0.9 (4)	100 (436)
SK	dostop do interneta doma	da	23.3 (10)	48.8 (21)	27.9 (12)	0.0 (0)	100 (43)
		ne	18.2 (22)	42.1 (51)	34.7 (42)	5.0 (6)	100 (121)
	skupaj		19.5 (32)	43.9 (72)	32.9 (54)	3.7 (6)	100 (164)
SI	dostop do interneta doma	da	17.9 (10)	46.4 (26)	33.9 (19)	1.8 (1)	100 (56)
		ne	18.9 (7)	40.5 (15)	35.1 (13)	5.4 (2)	100 (38)
	skupaj		18.3 (17)	44.1 (41)	34.4 (32)	3.2 (3)	100 (94)

Zaradi teh dejstev zavračam mojo drugo hipotezo (H2). Očitno je, da skrb za varnost podatkov (oziroma zaznavanje ogroženosti in mnenje o upravičeni zaskrbljenosti nad varnostjo), ki se prenašajo preko interneta ni odvisna samo od razširjenosti interneta; oziroma števila priključkov v gospodinjstvih. Razloge lahko med drugim najdemo v uspešnosti izvajanja programov in projektov, ki bodo pripomogli k uresničevanju in vzpostavitvi informacijske družbe.

Poljska se je sicer pri svojem razvoju soočala z nemalo nevšečnostmi, saj sta jo na poti razvoja ovirala tako politični svet, kot pomanjkanje finančnih sredstev; vendar se je ob vsem tem okrepila visoka stopnja narodne zavesti. Vse omenjene države, ki se problematike varnosti lotevajo nekoliko bolj postransko, so se tudi problemov IKT lotevale relativno pozno (od 1998 naprej) in v zvezi z njimi še niso nabrале zadostnega števila izkušenj; to pa odpira prostor mnogim vprašanjem in skepticizmu o novih tehnologijah.

Slovenija je zaradi nepreudarnih vlaganj v strukture IKT, že od leta 2000 vedno bolj zaostaja za nivojem EU. Eno najbolj izpostavljenih in perečih vprašanj v preteklih letih pa je bilo preureditev trga telekomunikacij, ki je, kljub mnogim pobudam, relativno počasno.

Na Češkem se je liberalizacija telekomunikacijskega sektorja zgodila pozno, prav tako pa je država izvajanje programov in dejavnosti prepuščala množicam. S tem so se tudi ljudje bili pripravljani seznaniti s posledicami informacijsko-komunikacijskih tehnologij in sprejeti dejstvo, da ima tudi ta medalja dve plati.

Bolgarija je ena vodilnih držav in še vedno ohranja visok nivo izobrazbe specializiranih ljudi v IKT, vendar veliko kvalificiranih ljudi odhaja na delo v tujino. Kljub temu gre za državo, ki ima veliko število kvalificiranih znanstvenikov in tehnikov v poslovnem sektorju (izučeni elektroniki in mehanični inženirji), kar posledično pomeni, da kvantiteta ljudi podpira razvoj IKT. Od tod izvira določena samozavest in ne-zaskrbljenost nad nevarnostmi, ki nam jih lahko prinese internet.

Podobno ima tudi Madžarska visoko razvit sistem IKT, saj je že leta 1989 vlada oblikovala različne programe, kako se spopasti s tehnološkim razvojem na področju informacijskih tehnologij; s tem pa je poskrbela za osveščanje ljudi, za državljane, ki jih ni strah novih izzivov novih tehnologij, saj imajo na tem področju že kar lepo tradicijo.

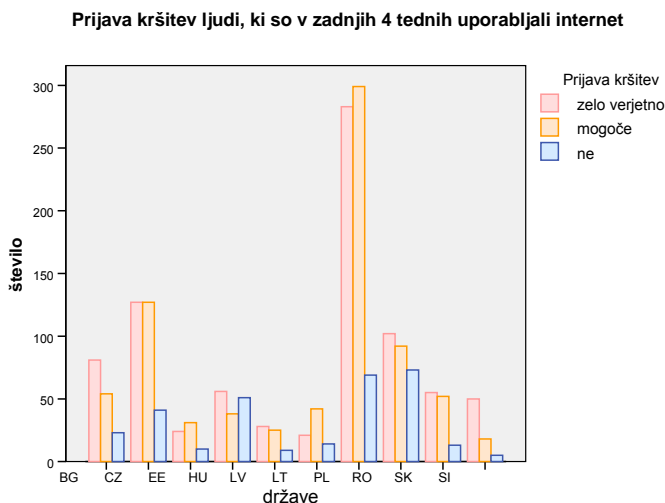
7.3 Prijava kršitev

Za preverjanje tretje (H3) in četrte hipoteze (H4), sem zajela uporabnike, ki so v zadnjem mesecu dostopali do interneta. V anketnem vprašalniku je vprašanje pri poglavju o računalnikih in internetu navedeno na sledeč način: *Ali ste v zadnjih 4 tednih uporabljali računalnik (pc, mac, ali katerikoli drugi) v službene ali zasebne namene?* Ponujeni so bili trije odgovori: »da«, »ne« in »ne vem«, za potrebe analize pa sem slednjega ponovno lahko izključila.

Odgovore sem povezala s sklopom o varnosti na internetu, in sicer s vprašanjem: *Ali bi prijavi kršitve vaše varnosti, zasebnosti in zaupnosti na internetu, npr. v ta namen ustanovljeni vladni agenciji?* Možne kategorije odgovorov so bile »zelo verjetno bi«, »mogoče«, »ne« in »ne vem« (slednjo sem izključila).

Za ponazoritev podatkov zraven tabel 7.3.1 in 7.3.2 služita tudi grafa (7.3.1 in 7.3.2).

Graf 7.3.1 – Prijava kršitev ljudi, ki so v zadnjih 4 tednih uporabljali internet



Graf 7.3.2 – Anonimna prijava kršitev

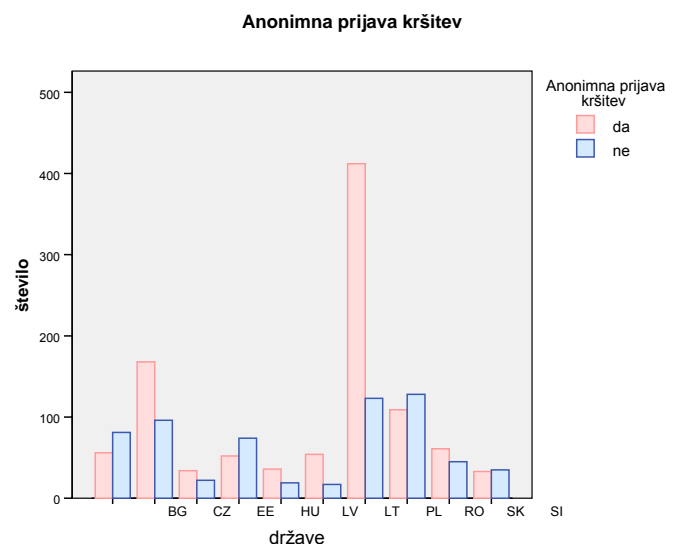


Tabela 7.3.1 – Prijava kršitev

država	prijava kršitev								
	zelo verjetno bi	mogoče	ne	ne vem	skupaj				
BG	uporaba interneta v da	47.4 % (81)	31.6 % (54)	13.5 % (23)	7.6 % (13)	100%	(171)		
	zadnjem mesecu ne	37.8 (17)	37.8 (17)	15.6 (7)	8.9 (4)	100	(45)		
	skupaj	45.4 (98)	32.9 (71)	13.9 (30)	7.9 (17)	100	(216)		
CZ	uporaba interneta v da	36.9 (127)	36.9 (127)	11.9 (41)	14.2 (49)	100	(344)		
	zadnjem mesecu ne	33.3 (22)	27.3 (18)	16.7 (11)	22.7 (15)	100	(66)		
	skupaj	36.5 (150)	35.3 (145)	12.7 (52)	15.6 (64)	100	(410)		
EE	uporaba interneta v da	32.0 (24)	41.3 (31)	13.3 (10)	13.3 (10)	100	(75)		
	zadnjem mesecu ne	18.2 (2)	36.4 (4)	9.1 (1)	36.4 (4)	100	(11)		
	skupaj	30.2 (26)	40.7 (35)	12.8 (11)	16.3 (14)	100	(86)		
HU	uporaba interneta v da	31.6 (56)	21.5 (38)	28.8 (51)	18.1 (32)	100	(177)		
	zadnjem mesecu ne	29.2 (14)	12.5 (6)	41.7 (20)	16.7 (8)	100	(48)		
	skupaj	31.0 (70)	19.5 (44)	31.9 (71)	17.7 (40)	100	(225)		
LV	uporaba interneta v da	42.4 (28)	37.9 (25)	13.6 (9)	6.1 (4)	100	(66)		
	zadnjem mesecu ne	40.9 (9)	31.8 (7)	18.2 (4)	9.1 (2)	100	(22)		
	skupaj	42.0 (37)	36.4 (32)	14.8 (13)	6.8 (6)	100	(88)		
LT	uporaba interneta v da	19.4 (21)	38.9 (42)	13.0 (14)	28.7 (31)	100	(108)		
	zadnjem mesecu ne	22.2 (4)	16.7 (3)	11.1 (2)	50.0 (9)	100	(18)		
	skupaj	19.8 (25)	35.7 (45)	12.7 (16)	31.7 (40)	100	(126)		
PL	uporaba interneta v da	36.9 (283)	39.0 (299)	9.0 (69)	15.0 (115)	100	(766)		
	zadnjem mesecu ne	23.1 (37)	35.6 (57)	20.6 (33)	20.6 (33)	100	(160)		
	skupaj	34.6 (320)	38.4 (356)	11.0 (102)	16.0 (148)	100	(926)		
RO	uporaba interneta v da	34.1 (102)	30.8 (92)	24.4 (73)	10.7 (32)	100	(299)		
	zadnjem mesecu ne	32.6 (44)	35.6 (48)	20.7 (28)	11.1 (15)	100	(135)		
	skupaj	33.6 (146)	32.3 (140)	23.3 (101)	10.8 (47)	100	(434)		
SK	uporaba interneta v da	42.6 (55)	40.3 (52)	10.1 (13)	7.0 (9)	100	(129)		
	zadnjem mesecu ne	29.4 (10)	47.1 (16)	8.8 (3)	14.7 (5)	100	(34)		
	skupaj	39.9 (65)	41.7 (68)	9.8 (16)	8.6 (14)	100	(163)		
SI	uporaba interneta v da	64.9 (50)	23.4 (18)	6.5 (5)	5.2 (4)	100	(77)		
	zadnjem mesecu ne	50.0 (8)	25.0 (4)	12.5 (2)	12.5 (2)	100	(16)		
	skupaj	62.4 (58)	23.7 (22)	7.5 (7)	6.5 (6)	100	(93)		

Večina ljudi, ki redno uporabljajo internet (oziroma so ga uporabljali v zadnjem mesecu), bi kršitev zelo verjetno prijavila (ljudje v Bolgariji, Češki, Madžarski, Latviji, Romuniji Slovaški in Sloveniji), ostali (v Estoniji, Litvi in Poljski²²) so nekoliko bolj zadržani in se opredeljujejo, da bi to mogoče storili. S podatki iz tabele 7.3.1 in 7.3.2 tako potrjujem tretjo delovno hipotezo (H3), da so ljudje, ki redno uporabljajo internet (vsaj enkrat mesečno), prej pripravljeni prijaviti kršitve varnosti ali zasebnosti.

²² le-ta ima skoraj enako visoko frekvenco tudi v kategoriji zelo verjetne prijave

Tabela 7.3.1 – Anonimna prijava kršitev

država	anonimna prijava kršitev						skupaj
	da	ne		ne vem			
BG	uporaba interneta v	da	35.2 % (56)	50.9 % (81)	13.8 % (22)	100 % (159)	
	zadnjem mesecu	ne	47.5 (19)	45.0 (18)	7.5 (3)	100 (40)	
	skupaj		37.7 (75)	49.7 (99)	12.6 (25)	100 (199)	
CZ	uporaba interneta v	da	56.8 (168)	32.4 (96)	10.8 (32)	100 (296)	
	zadnjem mesecu	ne	56.9 (29)	27.5 (14)	15.7 (8)	100 (51)	
	skupaj		56.9 (198)	31.6 (110)	11.5 (40)	100 (348)	
EE	uporaba interneta v	da	52.3 (34)	33.8 (22)	13.8 (9)	100 (65)	
	zadnjem mesecu	ne	50.0 (4)	25.0 (2)	25.0 (2)	100 (8)	
	skupaj		52.1 (38)	32.9 (24)	15.1 (11)	100 (73)	
HU	uporaba interneta v	da	35.9 (52)	51.0 (74)	13.1 (19)	100 (145)	
	zadnjem mesecu	ne	41.0 (16)	46.2 (18)	12.8 (5)	100 (39)	
	skupaj		36.8 (68)	50.3 (92)	13.0 (24)	100 (184)	
LV	uporaba interneta v	da	58.1 (36)	30.6 (19)	11.3 (7)	100 (62)	
	zadnjem mesecu	ne	50.0 (10)	35.0 (7)	15.0 (3)	100 (20)	
	skupaj		56.1 (46)	31.7 (26)	12.2 (10)	100 (82)	
LT	uporaba interneta v	da	69.2 (54)	21.8 (17)	9.0 (7)	100 (78)	
	zadnjem mesecu	ne	66.7 (6)	22.2 (2)	11.1 (1)	100 (9)	
	skupaj		69.0 (60)	21.8 (19)	9.2 (8)	100 (87)	
PL	uporaba interneta v	da	63.3 (412)	18.9 (123)	17.8 (116)	100 (651)	
	zadnjem mesecu	ne	46.9 (60)	21.9 (28)	31.3 (40)	100 (128)	
	skupaj		60.6 (472)	19.4 (151)	20.0 (156)	100 (779)	
RO	uporaba interneta v	da	40.7 (109)	47.8 (128)	11.6 (31)	100 (268)	
	zadnjem mesecu	ne	42.0 (50)	43.7 (52)	14.3 (17)	100 (119)	
	skupaj		41.1 (159)	46.5 (180)	12.4 (48)	100 (387)	
SK	uporaba interneta v	da	50.8 (61)	37.5 (45)	11.7 (14)	100 (120)	
	zadnjem mesecu	ne	55.2 (16)	31.0 (9)	13.8 (4)	100 (29)	
	skupaj		51.7 (77)	36.2 (54)	12.1 (18)	100 (149)	
SI	uporaba interneta v	da	45.2 (33)	47.9 (35)	6.8 (5)	100 (73)	
	zadnjem mesecu	ne	50.0 (7)	35.7 (5)	14.3 (2)	100 (14)	
	skupaj		46.0 (40)	46.0 (40)	8.0 (7)	100 (87)	

Prijave kršitev varnosti, zasebnosti in zaupnosti na internetu, bi v ta namen ustanovljeni vladni agenciji, veliko rajši anonimno posredovala Poljska, najmanj pa se s tem obremenjuje Bolgarija. Malo več kot polovica držav bi prijavo raje podala anonimno, zaradi česar ne morem sprejeti četrte hipoteze (H4), kjer sem domnevala, da je ljudem ob prijavi kršitev vseeno, ali je njihova prijava anonimna ali ne. Izkazalo se je, da je v ljudeh še vedno prisoten strah pred neraziskanim, neizkušenim in nepreverjenim; zato bi se v svojih aktivnostih raje posluževale varne obleke, v kateri se jim ne bi bilo potrebno izpostavljati.

8. ZAKLJUČEK

Splošno znano dejstvo je, da širjenje interneta in uporaba novih tehnologij v Sloveniji še vedno naraščata. Z njima se večajo tudi tveganja, nevarnosti in zlorabe teh tehnologij, zlasti za otroke in mladostnike, ki v večini primerov naivno nasedajo mamljivosti tega fenomena. Za varno izkoriščanje možnosti, ki jih ponuja le-ta v kombinaciji z novimi tehnologijami, sta namreč potrebna znanje in zavedanje, ki ščitita uporabnike pred potencialno škodljivimi vsebinami.

V nalogi sem raziskovala kakšen odnos imajo različne evropske države (novo pridružene članice Evropske unije) do vprašanja varne uporabe interneta. Ugotavljala sem kako na ta odnos vpliva politika posameznih držav, kakšne so značilnosti in aktivnosti le-teh, vpliv dostopnosti interneta na vzpostavitev kritičnega odnosa do uporabe interneta, nivo razvoja varne informacijske infrastrukture ipd.

Z rezultati v zvezi z zaskrbljenostjo nad varnostjo podatkov, ki se prenašajo preko in interneta in o vprašanju zasebnosti in zaupnosti, npr. glede zlorabe podatkov uporabnikov s strani tretje osebe; sem potrdila svojo prvo domnevo, da se ljudje, ki dalj časa uporabljajo internet, bolj zavedajo nevarnosti, ki jih le-ta prinaša (H1). Pod pojmom nevarnost sem v mojem primeru obravnavala varnostne kršitve prenosa podatkov in kršitve varnosti in zasebnosti. Nekoliko večjo zaskrbljenost kažejo le anketiranci Latvije in Poljske (slednja med vsemi izrazito izstopa); v splošnem pa ljudje v obravnavanih državah ne kažejo pretiranega zanimanja za to problematiko.

Sledilo je preverjanje zaskrbljenosti nad varnostjo, zasebnostjo in zaupnostjo - tokrat v odvisnosti od tega, ali imajo ljudje internetne priključke doma. Predvidevala sem namreč, da so ljudje v državah, kjer je internet bolj razširjen, manj zaskrbljeni. Ponovno so izstopali le Poljaki; izjemno zanimiv pa je podatek, da je med njimi nekoliko zaskrbljenih več tistih ljudi, ki doma sploh ne dostopajo do svetovne mreže. Kljub temu, da so rezultati torej podobni kot pri prvi domnevi, pa sem zaradi omenjenega podatka to hipotezo (H2) morala ovreči. Očitno skrb za varnost podatkov, ki se prenašajo preko interneta ni odvisna samo od razširjenosti interneta. Razloge lahko med drugim najdemo tudi v uspešnosti izvajanja programov in projektov, ki bodo pripomogli k uresničevanju in vzpostavitvi informacijske družbe.

Ker je varna raba interneta ena izmed prednostnih nalog programov Evropske Komisije, namerava Komisija v prihodnje še naprej vlagati znatna sredstva v projekte povezane s tovrstno tematiko. V povezavi s tem naj omenim Akcijski načrt o Varnejšem internetu (1999-2004), ki ga je leta 1999 sprejela Evropska Komisija, in je zagotovil nadaljnjo financiranje številnih projektov. Med njimi tudi projekt »SAFE SI«, ki ga je pripravila Fakulteta za družbene vede (FDV) Univerze v Ljubljani v sodelovanju z Arnesom (akademsko in raziskovalno mrežo Slovenije) in v okviru katerega na različne načine osvešča javnost o varni uporabi interneta.

V nadaljevanju preučevanja problematike odnosa do varne uporabe interneta sem predvidevala še, da bi bili ljudje, ki redno uporabljajo internet, prej pripravljeni prijaviti kršitve varnosti ali zasebnosti (H3), pri čemer bi jim bilo vseeno, ali je prijava anonimna ali ne (H4). Za preverjanje teh dveh hipotez, sem kot redne uporabnike zajela ljudi, ki so v zadnjih štirih tednih dostopali do interneta in ugotovila, da bi večina ljudi kršitev resnično zelo verjetno prijavila; s čimer sem potrdila tretjo hipotezo. Bolj zanimivo pa je bilo ob pregledu četrte hipoteze, ki sem jo morala ovreči. Menila sem namreč, da bodo ljudje indiferentne do vprašanja anonimne prijave, vendar se je po podrobnejši analizi izkazalo, da bi malo več kot polovica prebivalcev vseh držav prijavo raje podala anonimno, kot javno. Veliko preferenco anonimnosti daje Poljska, najmanj pa se s tem obremenjuje Bolgarija. Gledano v celoti, se je izkazalo, da je v ljudeh še vedno prisoten strah pred neraziskanim, neizkušenim, nepreverjenim; zato bi se v svojih aktivnostih raje posluževale varne obleke, v kateri se jim ne bi bilo potrebno izpostavljati.

Slovenija pri nobenem vprašanju posebej ne izstopa. Kljub mladosti in neizkušenosti v razvoju in uporabi te visoke tehnologije smo pogumni in stopamo naprej z jasnimi cilji, k razvoju infrastrukture in podpori uporabe interneta. Dostop do interneta je v prvem četrtletju 2006 imelo, po podatkih statističnega urada RS in raziskave o uporabi interneta RIS 2006, nekaj več kot 350.000 gospodinjstev, kar predstavlja 54% prebivalstva (glede na leto 2005 se je delež povečal za 6%). Če navedem še nekaj podatkov, je večji delež dostopa med gospodinjstvi, ki imajo otroke (75%), kot pa med tistimi, ki otrok nimajo (47%). Dnevni uporabniki interneta v populaciji 10 do 74 let je 37% - v starostni skupini od 16 do 34 let je 81% uporabnikov interneta, med starimi od 35 do 54 let pa 50%. Med ljudmi z višjo izobrazbo je bilo kar 90% uporabnikov interneta, med tistimi z nižjo pa 39%.

Globalno gospodarstvo, ekonomija, družba in nove komunikacijske poti se koncentrirajo okoli interneta (Herman 2005). Danes si težko predstavljamo organizacijo ali podjetje, ki v svoji panogi napreduje brez tržnega raziskovanja, rast informacijsko-komunikacijskih tehnologij na tržne raziskave še kako vpliva. Skozi razvoj anketiranja se je najprej izvajalo osebno anketiranje, sledilo je telefonsko, za tem je prišlo na vrsto računalniško podprto, danes, trenutno zadnja stopnja, pa so spletne ankete. Razlike med slednjima dvema so velike, največjo omejitev pri izvajanju spletnega anketiranja pa predstavlja premajhen delež uporabnikov interneta. Po podatkih »RIS 2006« in statističnega urada RS, internet v Sloveniji mesečno uporablja 880.000 prebivalcev. Število uporabnikov se sicer še vedno povečuje, vendar pa se rast upočasnjuje.

Najpogostejši metodi raziskav na internetu sta metodi spletnega anketiranja in anketiranja z vprašalniki, ki jih raziskovalci pošiljajo po elektronski pošti. Prvo je najpogostejša oblika raziskav na internetu. Sodi med računalniško podprto samo-anketiranje, pri čemer anketiranci s pomočjo osebnega računalnika in interneta sami izpolnjujejo vprašalnik (brez pomoči anketarja). Hitra rast interneta torej tudi pri poslovanju in tržnem raziskovanju odpira številne možnosti; vendar z njimi prinaša tudi tehnična in etična vprašanja. Svetovno združenje tržnih raziskovalcev Esomar je tako izdalo etična načela za izvajanje raziskav na internetu (Esomar 2003). Med njimi je nenazadnje zapisano tudi, da je treba zaščititi anonimnost respondentov, zapisana mora biti izjava o varovanju podatkov, raziskovalci pa morajo poskrbeti za varnost podatkov. Kljub temu pa se stopnja nezaupljivosti do novih tehnologij v smislu internetnih orodij zagotovo zrcali tudi na to področje. Nepredstavljivo je, da bi se ljudje, ki imajo odpor do vsakdanje uporabe interneta, in tega orodja ne vključujejo niti v reševanje problemov za potrebe vsakdanjika, odločali za spletno anketiranje. Menim, da je to korak, ki sledi šele po tem, ko bo prehojena in dobro utrjena pot splošnega zaupanja v to orodje.

Si upamo pogledati za desetletje naprej? Pew Internet je objavil rezultate raziskave med strokovnjaki o spletni prihodnosti oziroma, o tem, kaj se bo z internetom dogajalo do leta 2020. Internet naj bi tvorila milijarda naprav, povezanih v omrežje z nizkimi stroški. Veliko presenečenje za raziskovalce je predstavljala skoraj polovica (42%) črnohledih anketirancev, v zvezi s vprašanjem, ali bomo ljudje sposobni upravljati in nadzorovati tehnologijo v prihodnosti. Navidezna resničnost bo po njihovih besedah na eni strani povečala delavčevo produktivnost, hkrati pa bo proizvedla nove probleme z zasvojenostjo.

Menijo, da se bo pojavila kultura ljudi, znotraj katere bodo ljudje zavračali tehnologijo ali omrežja; nekateri bodo samo kljubovali informacijskim obremenitvam, drugi pa bodo proti tehnološkim spremembam protestirali tudi z nasilnimi dejanji. Ljudje bodo o sebi izdajali vedno več informacij, kar bo vodilo k izgubi določenega dela zasebnosti, po drugi strani pa bo prinašalo tudi nekatere koristi. Angleški jezik bo postal jezik globalnih komunikacij, ostali jeziki pa se bodo ohranili, ali celo pridobili na pomembnosti.

Mnenja o tem, ali bo svet zaradi informacijske tehnologije in transparentnosti organizacij ter posameznikov boljši, ostajajo deljena. Dejstvo je, da potrošniki počasi izgublamo strah pred novimi informacijsko-komunikacijskimi tehnologijami in možnostmi, ki jih prinašajo, če so le-te dobre, koristne in prihranijo čas ter denar (Gosar 2005). Pomanjkanje zaupanja je mogoče reševati in brez težav odpraviti s primernim obveščanjem, vlaganjem v zmanjševanje tveganj, ki lahko nastanejo pri uporabi in opravljanju storitev preko interneta. Ogromno lahko pri tem naredi tudi država in razna ostala strokovna združenja pri Gospodarski zbornici. Dejstvo pa je, da je problem je kompleksen in nanj v mnogih situacijah gledamo preveč poenostavljeno in enoplastno.

Veljalo bi uvajati sveže, nove projekte, ki bi predvsem otroke in mladostnike opozarjali na možne nevarnosti pri uporabi interneta. Tudi starše bi bilo potrebno osveščati o tovrstni problematiki in jih vzpodbujati k učenju njihovih otrok, pravičnega obnašanja v svetovnem spletu. Če bomo že otrokom uspeli privzgojiti kritičnost do podatkov, ki so mu dostopni preko interneta, se nam za prihodnost ni bati. Po jutru se dan pozna.

Včasih, vsaj v začetnih fazah, ko se uporabnik še seznanja z orodji in možnostmi, ki jih ta sodobna informacijsko-komunikacijska tehnologija ponuja je nujen tudi nadzor (sploh starejših nad otroci). Starši si lahko pomagajo z nastavitvijo na računalnikih – omejena uporaba samega računalnika, omejevanje ogleda neprimernih vsebin, namestitvev različnih filtrov, ki preprečujejo prikaz vsebinsko neprimernih stvari. Obstajajo tudi programski paketi za omejevanje uporabe različnih internetnih storitev, za časovno omejevanje uporabe računalnika in nadzorovanje njegove uporabe (npr. NetNanny, dostopno na <http://www.netnanny.com>, CYBERsitter, dostopno na <http://www.solidoak.com>, CyberPatrol, dostopno na <http://www.cyberpatrol.com> ipd.). Na tem mestu velja omeniti še dobro znana slovenska projekta SAFE-SI in Spletno Oko, kjer najdemo veliko nasvetov za varno uporabo računalnika tako za starše kot otroke (dostopno na <http://www.safe.si>).

LITERATURA

- Samostojne publikacije, diplomska in magistrska dela

Castells, Manuel (2001): *The Internet Galaxy*. New York: Oxford University Press Inc.

Čebulj, Janez, Juri Žurej in Tomaž Vesel (2005): *Varstvo osebnih podatkov in informacije javnega značaja*. Ljubljana: Nebra.

Feather, John (1999): *The Information Society: a study of continuity and change*. London: Library Association.

Gosar, Vito (2005): *Zaupanje in Elektronsko poslovanje*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

Head, Milena, Khaled Hassanein and Edward Cho (2003): *Establishing eTrust through Humanized Website Design*. V 16th Bled eCommerce Conference: *eTransformation*. Bled, Slovenija.

Herman, Roman (2005): *Internet kot medij osvobajanja in podrejanja*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

Kovačič, Matej (2006): *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.

Kovačič, Matej (2003): *Zasebnost na internetu*. Ljubljana: Inštitut za sodobne družbene in politične študije.

MESPA (Master's Degree in European Social Policy Analysis) (2002-2003): *Comparative Research Methodology*. University of Ljubljana: Faculty of Social Sciences.

Renko, Erik (2005): *Uporabnost spletnega anketiranja v trženjskem raziskovanju*. Magistrsko delo. Ljubljana: Ekonomska fakulteta.

Vehovar, Vasja, Zenel Batagelj, Marjan Jarkovič, Tomaž Kalin, Davor Kozmus, Anton Kramberger, Rok Kraševac, Katja Lozar Manfreda, Tanja Oblak, Matija Remec, Andrej Škerlep in Franc Trček (1998): *Internet v Sloveniji: projekt RIS '96-'98*. Ljubljana: Fakulteta za družbene vede.

Vehovar, Vasja in Boris Kragelj (2003): *Uporaba interneta: RIS 2002*. Ljubljana: Fakulteta za družbene vede.

Vurušič Robert, Petra (2006): *Internetni kašipot*. Ljubljana: Tehniška založba Slovenije.

- Članki in poročila v revijah oziroma zbornikih

eEurope (2005): An information society for all. V SIBIS (2003): *Annex to WP4 – D4.3.1, 2003, Overview of the National Contexts – NAS 10 Countries*, 15–16.

Kohn, M.L. (1989). V MESPA (2002–2003): *Comparative Research Methodology*. University of Ljubljana: Faculty of Social Sciences.

Nowak, S. (1989). V MESPA (2002–2003): *Comparative Research Methodology*. University of Ljubljana: Faculty of Social Sciences.

Official Journal of 2000. V SIBIS (2003d): Overview of the National Contexts – NAS 10 Countries. *Annex to WP4 – D4.3.1, 2003*.

Progress Report, 2002. V SIBIS (2003d): Overview of the National Contexts – NAS 10 Countries. *Annex to WP4 – D4.3.1, 2003*.

SIBIS (2003a): An evaluation of the EU, the EU Accession Countries, Switzerland and the United States. *Matching up to the Information Society*, August 2003.

SIBIS (2003b): eEurope Benchmarking: Key Figures for NAS 10 Countries. *WP4 – D4.3.1*, July 2003.

SIBIS (2003c): Measuring the Information Society in the EU, the EU Accession Countries, Switzerland and the US. *Sibis pocket book 2002/03; SIBIS project and European Communities*.

SIBIS (2003d): Overview of the National Contexts – NAS 10 Countries. *Annex to WP4 – D4.3.1, 2003*.

Sukič, Boštjan (2007): Otroci v zankah spleta. *DOBRO JUtRO* 119(6), 42.

- *Internetni viri*

Agencija NET (2003): *Microsoft v projektu e-vas*. Dostopno na <http://www.agencijanet.si/microsoft-v-projektu-e-vas> (1. september 2007)

Agencija NET (2002–2007): *Novice z različnih področij, povezanih z informacijskimi tehnologijami*. Dostopno na <http://www.agencijanet.si> (1. september 2007)

CyberPatrol (2003–2007): *Internet safety software protecting an online generation*. Dostopno na <http://www.cyberpatrol.com> (5. avgust 2007)

ESOMAR (2006–2007): *The World Association of Research Professionals*. Dostopno na <http://www.esomar.org> (23. junij 2007)

Geer, Dan, Rebecca Bace, Peter Gutmann, Perry Metzger, John S. Quarterman, Charles Pfleeger and Bruce Schneier (2007): *Cyber Insecurity: The Cost of Monopoly*. Dostopno na http://securityforest.com/wiki/index.php/Cyber_Insecurity:_The_Cost_of_Monopoly (2. september 2007)

Košena, Dejan (2000): *Zgodovina interneta*. Maribor: Pedagoška fakulteta. Dostopno na http://www.pfmb.uni-mb.si/didgradiva/nastopi/didrac2/00/2/zgodovina_interneta.htm (22. oktober 2006)

Ministrstvo za javno upravo (2007): *Državni portal RS*. Dostopno na <http://e-uprava.gov.si/e-uprava> (13. avgust 2007)

Net Nanny (2001–2007): *Protection for Every Member of Your Family*. Dostopno na <http://www.netnanny.com> (18. julij 2007)

Pew Internet (2000–2007): *Pew Internet & American Life Project*. Dostopno na <http://www.pewinternet.org> (22. julij 2007)

SafeSi (2005–2007): *Varna raba interneta*. Dostopno na: <http://www.safe.si> (28. junij 2007)

Sicherl, Pavle (2001): *Comments on Two Crosscutting Issues: Methods for Comparative Analysis and Strategy for the European Research Area*. Dostopno na http://www.sicenter.si/pub/bru_sich.pdf (24. avgust 2007)

SolidOakSoftware (2007): *Are Your Kids Really Safe on the Internet? CYBERSitter*. Dostopno na <http://www.solidoak.com> (8. julij 2007)

Statistični letopis 2007. Ljubljana: Statistični urad Republike Slovenije. Dostopno na <http://www.stat.si> (15. avgust 2007)

PRILOGE

A - Kratice obravnavanih oziroma omenjenih držav Evropske unije in njihova imena v celoti:

kratice držav Evropske unije:	celotno ime države
A	Avstrija
B	Belgija
BG	Bolgarija
CZ	Češka
D	Nemčija
DK	Danska
E	Španija
EE	Estonija
GR	Grčija
F	Francija
FIN	Finska
HU	Madžarska
IE	Irska
IT	Italija
L	Luksemburg
LT	Litva
LV	Latvija
NL	Nizozemska
P	Portugalska
PL	Poljska
RO	Romunija
S	Švedska
SI	Slovenija
SK	Slovaška
UK	Velika Britanija

Legenda:

□ - NAS (10)

□ - EU (15)

B1 - Vprašalnik v slovenskem jeziku – del, ki smo ga vključili v analizo:

ŠT. VPRAŠANJA	POGOJ	VPRAŠANJE	ODGOVOR	PRESKOK
X-A1	VSI	SEDAJ PA BI VAS ŽELEL/A VPRAŠATI NEKAJ VPRAŠANJ O RAČUNALNIKI IN INTERNETU.		A1
A1	VSI	ALI STE V ZADNJIH 4 TEDNIH UPORABLJALI RAČUNALNIK (PC, MAC ALI KATERIKOLI DRUGI) V SLUŽBENE ALI ZASEBNE NAMENE?	1 - DA 2 - NE 3 - NE VEM	A5A
A5A	VSI	ALI STE ŽE SLIŠALI ZA INTERNET? POJASNI: INTERNET JE SVETOVNA MREŽA RAČUNALNIKOV, KI VAM OMOGOČA DOSTOP DO INFORMACIJ PREKO RAČUNALNIKA.	1 - DA 2 - NE 3 - NE VEM	A5B Y-E1 A5B
A5B	ČE JE A5A=1,3	ALI IMATE DOMA DOSTOP DO INTERNETA?	1 - DA 2 - NE 3 - NE VEM	A11A A6
A6	ČE JE A5B=2,3	ALI STE KDAJ IMELI DOSTOP DO INTERNETA DOMA?	1 - DA 2 - NE 3 - NE VEM	A7
A11A	ČE JE A5B=1	ALI VESTE KAJ UPORABLJATE DOMA ZA POVEZAVO Z INTERNETOM?	1 - DA 2 - NE 3 - NE VEM	A11B A7 A11B

ŠT. VPRAŠANJA	POGOJ	VPRAŠANJE	ODGOVOR	PRESKOK
A11B	ČE JE A11A=1,3	PREBRAL/A VAM BOM NEKAJ METOD ZA POVEZAVO Z INTERNETOM. KATERO OD TEH UPORABLJATE DOMA? KARTICA A11B. MOŽNIH JE VEČ ODGOVOROV.	1 - MODEM 2 - DSL (ADSL) 3 - ISDN 4 - DRUGE METODE (MOBILNI TELEFON, NAJETA LINIJA, INTERNET PREKO SATELITA) 5 - NE VEM	A7
A7	VSI	ALI STE V ZADNJIH 4 TEDNIH VSAJ ENKRAT UPORABLJALI INTERNET DOMA, V ŠOLI, V SLUŽBI ALI KJERKOLI DRUGJE?	1 - DA 2 - NE 3 - NE VEM	A9 A8
A8	ČE JE A7=2,3	ALI STE UPORABLJALI INTERNET VSAJ ENKRAT V ZADNJIH 12 MESECIH?	1 - DA 2 - NE 3 - NE VEM	A10 A3
A9	ČE JE A7=1	ČE POMISLITE NA TIPIČNI TEDEN, KOLIKO ČASA POVPREČNO UPORABLJATE INTERNET... KARTICA A9! *ODGOVOR NIČ OZNAČITE TUDI, KO OSEBA INTERNETA NA DOLOČENEM KRAJU NE UPORABLJA, ALI PA SE DOLOČEN KRAJ NANJO NE NANANŠA (NPR. OSEBA, KI NI ZAPOSLENA, INTERNETA NE UPORABLJA V SLUŽBI).		A10
A	DOMA?		1 - NIČ* 2 - MANJ KOT 1 URO 3 - 1 DO 5 UR 4 - 6 DO 10 UR 5 - 11 DO 20 UR 6 - VEČ KOT 20 UR 7 - NE VEM	
B	V SLUŽBI?		1 - NIČ* 2 - MANJ KOT 1 URO 3 - 1 DO 5 UR 4 - 6 DO 10 UR 5 - 11 DO 20 UR 6 - VEČ KOT 20 UR 7 - NE VEM	
C	V ŠOLI, UNIVERZI ALI DRUGI IZOBRAŽEVALNI USTANOVI?		1 - NIČ* 2 - MANJ KOT 1 URO 3 - 1 DO 5 UR 4 - 6 DO 10 UR 5 - 11 DO 20 UR 6 - VEČ KOT 20 UR 7 - NE VEM	
D	NA JAVNEM MESTU, KJER JE UPORABA INTERNETA BREZPLAČNA?		1 - NIČ* 2 - MANJ KOT 1 URO 3 - 1 DO 5 UR 4 - 6 DO 10 UR 5 - 11 DO 20 UR 6 - VEČ KOT 20 UR 7 - NE VEM	
E	V INTERNET CAFÉ-JU ALI DRUGJE KJER JE UPORABO INTERNETA POTREBNO PLAČATI?		1 - NIČ* 2 - MANJ KOT 1 URO 3 - 1 DO 5 UR 4 - 6 DO 10 UR 5 - 11 DO 20 UR 6 - VEČ KOT 20 UR 7 - NE VEM	
F	NA KATEREMKOLI DRUGEM MESTU, KI GA ŠE NISMO OMENILI?		1 - NIČ* 2 - MANJ KOT 1 URO 3 - 1 DO 5 UR 4 - 6 DO 10 UR 5 - 11 DO 20 UR 6 - VEČ KOT 20 UR 7 - NE VEM	

A10	ČE JE A7=1 ALI A8=1	KDAJ STE PRVIČ UPORABILI INTERNET? KARTICA A10!	1 - PRED MANJ KOT 6 MESECI	2 - PRED 6 DO 12 MESECI	A3
			3 - PRED 1 DO 2 LETOMA	4 - PRED VEČ KOT 2 LETOMA	

A3	ČE JE A1=1 ALI ČE JE A5A=1,3	ALI STE V ZADNJIH 4 TEDNIH POSLALI ALI PREJELI KAKRŠNOKOLI OSEBNO ALI SLUŽBENO SPOROČILO PO ELEKTRONSKI POŠTI (E-MAIL)?	1 - DA		A4A
			2 - NE		A18
			3 - NE VEM		
A4A	ČE JE A3=1	S KOLIKO PRIJATELJI IN SORODNIKI REDNO KOMUNICIRATE PREKO ELEKTRONSKE POŠTE (E-MAILA)? KARTICA A4A!	1 - S SKORAJ VSEMI 3 - S Približno polovico 5 - SAMO Z NEKATERIMI OZIROMA Z NOBENIM	2 - S Približno tremi četrtinami 4 - S Približno četrtino 6 - NE VEM	A4B
A4B	ČE JE A3=1	IN KOLIKO VAŠIH PRIJATELJEV IN SORODNIKOV IMA SVOJ E-MAIL NASLOV? KARTICA A4B!	1 - SKORAJ VSI 3 - Približno polovica 5 - SAMO NEKATERI OZIROMA NIHČE OD NJIH	2 - Približno tri četrtine 4 - Približno četrtina 6 - NE VEM	A18
A18	ČE JE A5A=1,3	SEDAJ VAM BOM PREBRAL/A NEKAJ TRDITEV O INTERNETU. ZA VSAKO OD TRDITEV MI PROSIM, POVEJTE, ALI SE S TRDITVIJO POPOLNOMA STRINJATE, NEKOLIKO STRINJATE ALI NE STRINJATE. KARTICA A18!			Y-B1
A		ZA INTERNET SO POTREBNA POGLOBLJENA RAČUNALNIŠKA ZNANJA.	1 - POPOLNOMA SE STRINJAM SE STRINJAM 4 - NE VEM	2 - NEKOLIKO 3 - NE STRINJAM SE	
B		DOSTOPA DO INTERNETA SE NE DA DOBITI NA DOVOLJ ENOSTAVEN NAČIN.	1 - POPOLNOMA SE STRINJAM SE STRINJAM 4 - NE VEM	2 - NEKOLIKO 3 - NE STRINJAM SE	
C		UPORABA INTERNETA VZAME PREVEČ ČASA.	1 - POPOLNOMA SE STRINJAM SE STRINJAM 4 - NE VEM	2 - NEKOLIKO 3 - NE STRINJAM SE	
D		UPORABA INTERNETA JE PREDRAGA.	1 - POPOLNOMA SE STRINJAM SE STRINJAM 4 - NE VEM	2 - NEKOLIKO 3 - NE STRINJAM SE	
E		NA INTERNETU PRIMANJKUJE UPORABNIH ALI ZANIMIVIH INFORMACIJ.	1 - POPOLNOMA SE STRINJAM SE STRINJAM 4 - NE VEM	2 - NEKOLIKO 3 - NE STRINJAM SE	
F		INTERNET NI ZAME.	1 - POPOLNOMA SE STRINJAM SE STRINJAM 4 - NE VEM	2 - NEKOLIKO 3 - NE STRINJAM SE	
Y-B1	VSI			A8=2,3 → Y-E1 A7 ALI A8=1 → B1	

ŠT. VPRAŠANJA	POGOJ	VPRAŠANJE	ODGOVOR	PRESKOK
X-J1	ČE JE A7 ALI A8=1	SEDAJ BOMO GOVORILI O VARNOSTI NA INTERNETU.		J1A
J1A	ČE JE A7 ALI A8=1	V KOLIKŠNI MERI STE ZASKRBLJENI GLEDE VARNOSTI PODATKOV NA INTERNETU, NPR. GLEDE IZGUBE ALI ZLORABE VAŠIH PODATKOV? ALI STE...? KARTICA J1A!	1 - ZELO ZASKRBLJENI 2 - NEKOLIKO ZASKRBLJENI 3 - NISTE ZASKRBLJENI 4 - NE VEM	J1B
J1B	ČE JE A7 ALI A8=1	V KOLIKŠNI MERI STE ZASKRBLJENI GLEDE ZASEBNOSTI IN ZAUPNOSTI NA INTERNETU, NPR. GLEDE ZLORABE VAŠIH PODATKOV S STRANI TRETJE OSEBE? ALI STE...? KARTICA J1A!	1 - ZELO ZASKRBLJENI 2 - NEKOLIKO ZASKRBLJENI 3 - NISTE ZASKRBLJENI 4 - NE VEM	Y-J1
Y-J1				J1A ALI J1B=1,2 → J2 J1A IN J1B=3→ J3
J2	ČE JE J1A ALI J1B=1,2	KAKO POGOSTO-ZARADI TEH SKRBI NE KUPUJETE IZDELKOV ALI STORITEV NA INTERNETU? KARTICA J2!	1 - POGOSTO 2 - VČASIH 3 - NIKOLI 4 - NE VEM 5 - ŠE NIKOLI NISEM KUPOVAL/A NA INTERNETU	J3
J3	ČE JE A7 ALI A8=1	ALI BI PRIJAVILI KRŠITVE VAŠE VARNOSTI, ZASEBNOSTI IN ZAUPNOSTI NA INTERNETU NPR. V TA NAMEN USTANOVLJENI JAVNI AGENCIJI? KARTICA J3!	1 - ZELO VERJETNO BI 2 - MOGOČE 3 - NE	J4
			4 - NE VEM	J5
J4	ČE JE J3=1,2, 3	ALI BI TO LAŽJE STORILI, ČE BI TO LAHKO NAREDILI ANONIMNO?	1 - DA 2 - NE 3 - NE VEM	J5
J5	ČE JE A7 ALI A8=1	KAKO POGOSTO SE ZAVEDATE VARNOSTNIH ELEMENTOV SPLETNIH STRANI, KO KUPUJETE PREKO INTERNETA? KARTICA J2!	1 - POGOSTO 2 - VČASIH 3 - NIKOLI 4 - NE VEM	J6
			5 - ŠE NIKOLI NISEM KUPOVAL/A NA INTERNETU	X-K1
J6	ČE JE A7 ALI A8=1	IN KAKO POGOSTO UPOŠTEVATE VARNOSTNE ELEMENTE SPLETNIH STRANI, KO SE ODLOČATE ZA NAKUP NA INTERNETU? KARTICA J2!	1 - POGOSTO - VČASIH 3 - NIKOLI - NE VEM	2 4 X-K1
X-K1	ČE JE A7 ALI A8=1	SEDAJ PA BI VAS ŽELEL/A VPRAŠATI NEKAJ VPRAŠANJ O KONTAKTIRANJU VLADNIH URADOV PREKO INTERNETA.		K1

B2 - Vprašalnik v angleškem jeziku – del, ki smo ga vključili v analizo:

Module A: Basic ICT equipment access and use		
A19a ALL	Do you have access to a fax machine in your household?	(1) yes → A19b (2) no → A19b (3) DK → A19b
A19b ALL	Do you have access to a telephone in your household?	(1) yes → A19c (2) no → A19c (3) DK → A19c
A19c ALL	Do you have a mobile phone for your own personal use? <i>PROMPT: Includes office phone which can be used for own personal use</i>	(1) yes → A20 (2) no → A20 (3) DK → A20
A20 ALL	How many of your friends and relatives have a mobile phone for their personal use? <i>[INTERVIEWER: Read out answer categories]</i>	(1) all or almost all → Y-A1 (2) about three quarters → Y-A1 (3) about half → Y-A1 (4) about one quarter → Y-A1 (5) only few or no-one → Y-A1 (6) DK → Y-A1
Y-A1 BRANCHING		IF A19c=1 → A27 IF A19c=2,3 → X-A1
A27 IF A19c=1	Have you, in the last four weeks, used SMS* messages for communicating with other people? [<i>* TRANSLATOR: Check if another term is more common in your country</i>]	(1) yes → A30 (2) no → A30 (3) DK → A30
A30 IF A19c=1 but see (d) and (e)	Now, think about what your everyday life would be like if you didn't have a mobile phone. Please tell me how much you agree that if you didn't have a mobile phone (ITEM). Would you say that you ... <i>[INTERVIEWER: Read out answer categories for the first 2 items]</i> (a) you would often not be able to contact your friends and family, or be reached by them (b) you would be less exposed to dangerous electromagnetic radiation (c) you would be more helpless in case of emergencies <i>[IF in4=1]</i> (d) you would not receive some of the information you need for your job <i>[IF in4=1]</i> (e) you would have less exchange with some of your business contacts (f) you would have less fun	FOR EACH: (1) agree completely (2) agree somewhat (3) do not agree (4) DK / not applicable → X-A1
Transition X-A1 ALL	Now we would like to ask you a few questions about computers and the Internet	
A1 ALL	Have you used a PC, Mac or any other computer, for work or for private purposes - in the last four weeks?	(1) yes → A5a (2) no → A5a (3) DK → A5a
A5a ALL	Have you ever heard of the Internet? <i>PROMPT: The Internet is a worldwide computer network that allows you to access information through a computer</i>	(1) yes → A5b (2) no → Y-E1 (3) DK → A5b
A5b IF A5a=1,3	Do you have access to the Internet in your home?	(1) yes → A11a (2) no → A6 (3) DK → A6
A6 IF A5b=2,3	Did you once have Internet access in your home?	(1) yes → A7 (2) no → A7 (3) DK → A7

A11a IF A5b=1	Do you know what technical method you use at home to connect to the Internet?	(1) yes → A11b (2) no → A7 (3) NA → A11b
A11b IF A11a=1,3	I will read to you a number of methods to access the Internet. Which of these do you use at home? [INTERVIEWER: Read out and code those that apply]	MULTIPLE ANSWERS (1) Dial-up with modem -(2) DSL (e.g. ADSL) (3) ISDN -(4) Other not mentioned (e.g. mobile, leased line, Internet via satellite) (5) DK → A7
A7 IF A5a=1,3	Have you used the Internet at least once in the last four weeks, at home, at school or work or at any other place?	(1) yes → A9 (2) no → A8 (3) DK → A8
A8 IF A7=2,3	Have you used it in the last 12 months at least once?	(1) yes → A10 (2) no → A3 (3) DK → A3
A9 IF A7=1	How much <u>time</u> do you spend in a typical week on using the Internet ... [item] [INTERVIEWER: Read out answer categories for the first 2 items] (a) at home? (b) at the workplace? (c) at school, university or another educational institution? (d) at a public place where Internet access is free? (e) at an Internet café or other place where you have to pay for access? (f) at another place not mentioned yet	FOR EACH (1) none (includes no usage there at all / not applicable) (2) less than 1 hour (3) between 1 and 5 hours (4) between 6 and 10 hours (5) between 11 and 20 hours (6) more than 20 hours (7) DK → A10
A10 IF A7=1 or A8=1	When did you use the Internet for the first time? [INTERVIEWER: Read out answer categories]	(1) < 6 months ago (2) 6 - 12 months ago (3) 1 year - 2 years ago (4) 2 years + ago (5) DK → A3
A3 IF A1=1 and A5a=1,3	Have you sent or received any e-mail messages, for work or for private purposes, during the last four weeks?	(1) yes → A4a (2) no → A18 (3) DK → A18
A4a IF A3=1	With how many of your friends and relatives do you communicate regularly via email? [INTERVIEWER: Read out answer categories]	(1) all or almost all → A4b (2) about three quarters → A4b (3) about half → A4b (4) about one quarter → A4b (5) only few or no-one → A4b (6) DK → A4b
A4b IF A3=1	And how many of your friends and relatives have their own email address? [INTERVIEWER: Read out answer categories]	(1) all or almost all (2) about three quarters (3) about half (4) about one quarter (5) only few or no-one (6) DK → A18

<p>A18 A5a=1,3</p>	<p>Now I will read to you a list of statements about the Internet. Please tell me for each statement whether you agree completely, agree somewhat or do not agree. The Internet ... [item]. Do you ... (a) requires advanced computer skills, (b) is not easy enough to get access to, (c) is too time consuming, (d) is too expensive to use, (e) lacks useful or interesting information (f) is not something for me</p>	<p>FOR EACH (1) agree completely (2) agree somewhat (3) or do you not agree (4) DK ➔ Y-B1</p>
------------------------	--	--

Module J: Security		
Transition X-J1 <i>IF A7=1 or A8 = 1</i>	Now the topic is Internet security.	→ J1a
J1a <i>IF A7=1 or A8 = 1</i>	How concerned are you about data security on the Internet, i.e. the loss or manipulation of your data? Are you ... <i>[INTERVIEWER: Read out answer categories]</i>	(1) very concerned (2) somewhat concerned (3) not concerned (4) DK → J1b
J1b <i>IF A7=1 or A8 = 1</i>	How concerned are you about privacy and confidentiality on the Internet, i.e. personal information about you being misused by third parties? Are you ... <i>[INTERVIEWER: Read out answer categories]</i>	(1) very concerned (2) somewhat concerned (3) not concerned (4) DK → Y-J1
Y-J1		<i>IF J1a=1,2 or J1b=1,2 → J2</i> <i>IF J1a=3 and J1b=3 → J3</i>
J2 <i>IF J1(a)=1,2 or J1(b)=1,2</i>	Are these concerns stopping you from using the Internet to buy goods or services online: often, sometimes, or never?	(1) often → J3 (2) sometimes → J3 (3) never → J3 (4) DK → J3 (5) Never tried to buy on-line (DO NOT READ) → J3
J3 <i>IF A7=1 or A8 = 1</i>	Would you report violations of your on-line security, privacy and confidentiality to a third independent party, for example a public agency created for this task? <i>[INTERVIEWER: Read out answer categories]</i>	(1) yes, very likely → J4 (2) maybe → J4 (3) no → J4 (4) DK → J5
J4 <i>IF J3=1,2,3</i>	Would it be easier for you to do so if you could do it anonymously?	(1) yes → J5 (2) no → J5 (3) DK → J5
J5 <i>IF A7=1 or A8 = 1</i>	How often are you aware of security features of websites when you use the Internet to buy online: often, sometimes or never?	(1) often → J6 (2) sometimes → J6 (3) never → J6 (4) DK → J6 (5) Never tried to buy on-line (DO NOT READ) → X-K1
J6 <i>IF (A7=1 or A8 =1) & J5 ~5</i>	And how often do you take security features of websites into account when deciding about whether to buy online: often, sometimes or never?	(1) often → X-K1 (2) sometimes → X-K1 (3) never → X-K1 (4) DK → X-K1

Otroci v zankah spleta

Tveganja z uporabo interneta pri otrocih



Se kdaj vprašate kaj počne vaš otrok pred računalnikom? Katere spletne strani obiskuje, katere igre igra, s kom se pogovarja v spletnih klepetalnicah in predvsem koliko časa »ždi« pred računalnikom. Že danes lahko s pomočjo dobre (hitre) internetne povezave in ustreznih programov pridobite velike količine podatkov, kamor štejemo predvsem glasbo, filme in druga avtorsko zaščitena dela. Velika večina datotek, ki se izmenjujejo po omrežju, ni legalnega izvora, zato velja opozorilo tudi staršem. Vsak računalnik ima namreč svoje ime, ki se mu reče IP številka in jo je mogoče slediti.

Aktivnosti na internetu

Zadnja raziskava Eurobarometra o aktivnostih mladih na internetu, ki je bila opravljena tudi v Sloveniji, je poskušala

ugotoviti, ali so evropski otroci na internetu preveč samozavestni, ali jim starši lahko zaupajo in kje je meja med varnim in nevarnim. Nove tehnologije uporabljajo otroci podobno po vsej Evropi, med najpopularnejše spletne aktivnosti spadajo: spletno igranje iger, brskanje ter komuniciranje. Večina internet uporabljaja večkrat dnevno, njegovo uporabo starši nekoliko bolj nadzirajo, uporaba mobilnika pa je bolj svobodna in manj nadzorovana. Otroci se potencialnih spletnih tveganj zavedajo, kar nekaj pa jih tudi ve, kako preprečiti tveganja.

Ugotovitve za Slovenijo

Vsi otroci imajo vsaj nekaj izkušenj z uporabo interneta. Menijo, da je koristen ter uporaben in so ga že uporabili za šolske potrebe. Pogostost uporabe


in izkušnost se večata z leti. Mlajša skupina otrok, stara od 9 do 10 let, internet uporablja občasno, kadar pa ga, ga uporablja od pol ure do največ ene ure. Starejša skupina anketiranih otrok, starih od 12 do 14 let, internet uporablja bolj redno, nekateri tudi več ur dnevno. Vsi so odgovorili, da internet uporabljajo za šolske potrebe, med mlajšimi so priljubljene spletne igre, v skupini starejših otrok pa nekateri opravljajo tudi bolj zahtevne operacije, kot so prenos različnih datotek. Odprte klepetalnice predstavljajo največje tveganje za otroke.

Večino deklic so starši posvarili, naj ne razkrivajo svojih fotografij in osebnih podatkov. Deklice se potencialne ogroženosti bolj zavedajo, dečke pa bolj skrbijo virusi, ki bi utegnili okužiti njihov računalnik. Ozaveščenost se večja s starostjo. Dečki, stari od 12 do 14 let, niso preveč v skrbeh zaradi pedofilije, saj menijo, da so deklice bolj ogrožene. Mlajše deklice vedo, da ni dobro komunicirati z neznanci, vendar jih kar nekaj nima jasne predstave o tem, zakaj to ni dobro. Uporaba npr. MSN Messengerja se jim zdi neškodljiva, saj same izbirajo, komu bodo dovolile komunikacijo. Vsi otroci se zavedajo, da internet ni popolnoma kredibilen, strani, ki se redno osvežujejo in so lepega videza, naj bi bile po mnenju otrok bolj kredibilne. Kot primer kredibilne strani se pogosto omenja Wikipedia. Med dečki in dek-

licami obstaja razlika glede škodljivih in šokantnih vsebin. Deklice so v primeru, da naletijo na pornografijo, šokirane in skušajo stran čimprej zapreti, nekaj dečkov pa si te strani tudi ogleda. Deklice so nad nasiljem šokirane in se jim zdi moteče, medtem ko nekaj dečkov priznava, da so že sami iskali spletne strani s tovrstno vsebino. Starejši dečki ne odobravajo vsega, ne odobravajo nasilja nad mlajšimi, brutalnega mučenja, ubijanja, spolnega nasilja, nekaj pa jih ne odobrava homoseksualnih spolnih odnosov.

Kaj storiti?

Kaj torej storiti, da bi vašega otroka zaščitili pred uporabo škodljivih vsebin? Vsekakor je aktivnosti otrok med delom z računalnikom potrebno spremljati, kar pa seveda ne pomeni »viseti« zraven ali gledati čez ramo. Marsikdaj zadostuje že bežen pregled računalnika in pozornost pri kupovanju iger, programov itd. Žal se marsikateri starši veliko slabše znajdejo za računalnikom kot njihovi otroci, zato le-ti zlahka prikrijejo sledove svojih aktivnosti. Koristne informacije o varnih načinih rabe svetovnega spleta lahko starši dobite na spletni strani slovenske točke o varni uporabi SAFE-SI (<http://www.safe.si>). V okviru projekta SAFE-SI bodo jeseni potekala posebna izobraževanja za starše.

 Boštjan Sukič