Univerza v Mariboru

Fakulteta za varnostne vede

DOKTORSKA DISERTACIJA

Družbena sprejemljivost biometrične tehnologije v boju proti terorizmu

September, 2011 Robert BRUMNIK

Univerza v Mariboru
Fakulteta za varnostne vede

DOKTORSKA DISERTACIJA

Družbena sprejemljivost biometrične tehnologije v boju proti terorizmu

September, 2011

Kandidat: Robert BRUMNIK
Mentor: red. prof. dr. Iztok Podbregar
Somentor: red. prof. dr. Eva Jereb

Noben tiran ne more matirati svobode.

Machiavelli

ZAHVALA

Zahvaljujem se mentorju red. prof. dr. Iztoku Podbregarju za vso strokovno pomoč, spodbudo in koristne nasvete pri izdelavi disertacije.

Zahvaljujem se somentorici red. prof. dr. Evi Jereb za vso strokovno pomoč in koristne nasvete pri izdelavi disertacije.

Zahvala gre tudi vsem profesorjem Fakultete za varnostne vede, ki so mi kakorkoli pomagali v vseh letih, ko sem se kot raziskovalec uvajal v akademske in raziskovalne sfere.

Zahvala vsem, ki so kakorkoli prispevali k nastajanju tega dela.

Kazalo tabel

Kazalo slik

POVZETEK

Začetek naše študije predstavlja opredelitev in definiranje terorizma, ki danes predstavlja velik izziv tudi v informacijski sferi. Informacijski vidik opredelitve terorizma (kibernetski terorizem[1]) predstavlja za globalni varnostni sektor vedno večjo grožnjo. Zaradi terorističnih napadov 11.09.2001 v ZDA (Združene države Amerike), je boj proti terorizmu dobil nove razsežnosti. Za povečanje učinkovitosti odkrivanja terorizma je potrebno povečati nadzor ter sprejeti dodatne varnostne ukrepe.

Nadalje v študiji prikazujemo biometrične metode in zgodovinski pregled raziskovalnega področja. Biometrija se nanaša na identifikacijo osebe, na osnovi fizikalnih in vedenjskih značilnosti (prstni odtisi, geometrija roke, glas, šarenica itd.). Ker je sodobna IKT zaradi svoje uporabnosti ter razširjenosti postala cilj tudi v funkciji terorističnega delovanja, v študiji obravnavamo tudi kibernetično kriminaliteto in terorizem ter posebnosti viktimizacij kibernetične kriminalitete. V ospredju je največkrat protikulturni ali politični boj in boj za družbene vrednote postmodernega kapitalizma.

Osrednji del disertacije predstavlja raziskava in statistična analiza raziskovalnih parametrov, ki vplivajo na sprejemljivost biometričnega sistema. Z raziskavo smo se osredotočili na meritve v slovenskem prostoru ter na okviren pregled relevantnih nacionalnih in mednarodnih standardov ter zakonodaje, ki služi za določitev politike biometričnih ukrepov, varnostnih mehanizmov in uspešno ter kakovostno izvedbo identifikacije. V raziskavi smo s statističnim modeliranjem na osnovi korelacije in ANOVE, t-testa ter faktorske in regresijske analize določili sprejemljivost in učinkovitost biometričnega identifikacijskega sistema. S povzetkom dobljenih ocen parametrov sprejemljivosti in učinkovitosti biometričnega sistema smo

[1] V literaturi se pojavlja mnogo različnih izrazov: kiberterorizem (Denning, 2000), informacijski terorizem (Belič, 2001; Svete, 2005), IP terorizem (Bedi, 2005), računalniški terorizem (Galley, 1996), kibernetski terorizem (Coleman, 2003). V disertaciji bomo uporabili ime kibernetski terorizem.

testirali predpostavljene hipoteze. V raziskavi obravnavan biometrični sistem je glede na parametre in pogoje raziskave učinkovitejši od klasične metode identifikacije (kartice) in tudi zagotavlja družbeno sprejemljivost v primerih, ko gre za najhujša kriminalna in teroristična dejanja, kot v primerih vsakdanje uporabe. Ugotavljamo, da je »sprejemljivost« (statistično) pomemben dejavnik pri obravnavi in delovanju vseh biometričnih sistemov s stališča zasebnosti.

V izogib sodobnim pojavnim oblikam terorizma je potrebno zagotoviti sofisticiran koncept identifikacije deviantnega obnašanja, ki zahteva prožnost in hitrost izvajanja. Naloga identifikacijskih sistemov je prilagoditi procese identifikacije primerno današnji informacijski dobi, ki s seboj prinaša informacijsko tehnologijo, kar omogoča sodoben in inovativen način identifikacije v globalnem prostoru. Potreba informatizacije pa rezultira v visokih vložkih ter investicijah, ki imajo neposreden ekonomski vpliv na gospodarstvo največkrat tehnološko razvitejših držav.

Študijo zaključimo z razvojem odločitvenega modela sprejemljivosti biometrije ter podanimi izhodišči in smernicami za nadaljnje raziskave.

Ključne besede:

terorizem, kibernetski terorizem, biometrija, zasebnost, informacijsko-komunikacijska tehnologija

UDK: 004.93:57.087.1+343.3/.7(043.3)

Social acceptance of biometric technology to combat terrorism

SUMMARY

The beginning of our study represents the identification and definition of terrorism, which today represents a major challenge in the information sphere. This aspect of the definition of terrorism (cyber terrorism[2]) represents the global challenge of threat in security sector. The terrorist attacks of 9.11.2001 in the U.S. was fighting against terrorism got a new dimension. To increase the efficiency of detecting terrorists, it was necessary to increase control and take additional precautions.

The study continued in the direction of biometric methods areas and of historical overview. Biometrics refers to the identification of the person on the basis of physical and behavioural characteristics (fingerprints, hand geometry, voice, iris, etc.). Modern ICT is both because of its usefulness and become target of widespread terrorist activity. The survey is also designed to display cyber crime, terrorism and cyber-crime victimization specificities. In the foreground are the most counter-culture or political struggle and the struggle for social values of postmodern capitalism.

The central part of the dissertation presents a statistical analysis of survey and research parameters that affect the acceptability of biometric system in use. Acceptance is an important factor in the consideration and operation of biometric systems from the standpoint of privacy. For the study, we focused on measurements in Slovenian territory, and the indicative overview of relevant national and international standards and legislation that serves to determine the policies of biometric measures, security mechanisms and effective, and quality execution of identification. The study was the statistical modeling based on correlation and ANOVA, t-test, and factor and

[2] In literature there are many different terms: cyberterrorism (Denning, 2000), information terrorism (Belič, 2001; Svete, 2005), IP terrorism (Bedi, 2005), computer terrorism (Galley, 1996), cyber terrorism (Coleman, 2003). In this study we use the name of cyber terrorism.

regression analysis to determine the acceptability and effectiveness of a biometric identification system. The summary of parameter estimates obtained acceptability of biometric system we provide hypotheses test. The study considered a biometric system, given the parameters and conditions of research more effective than traditional methods of identification (cards) and also provides social acceptability in cases involving the most serious of criminal and terrorist acts, as in cases of ordinary use. We note that the »acceptance« (statistically) significant factor in the consideration and operation of biometric systems in terms of privacy.

In order to avoid the modern phenomena of terrorism, it is necessary to provide a sophisticated concept of identification of deviant behavior that requires flexibility and high performance. Requirement of identification systems is to adapt the process of identifying appropriate to today's information age, which brings information technology and provides a modern and innovative way of identifying in the global environment. Needed computerization results in high inputs and investment that have a direct economic impact on the economy of the most technologically advanced countries.

The study we concluded with a decision model development and acceptance of biometrics announcement baseline and guidance by a further research.

Keywords:

terrorism, cyber terrorism, biometry, privacy, information-communication technology

UDC: 004.93:57.087.1+343.3/.7(043.3)

I TEORETIČNI DEL

1 UVOD

Uvodoma bomo opravili pregled relevantnih področij, ki so rdeča nit naše raziskave. Vodilo pregleda literature, raziskav in raziskovalnih modelov ter pristopov, je terorizem, ki ga bomo še posebej podrobno obravnavali v eni izmed svojih najsodobnejših pojavnih oblik, t.j. kibernetski terorizem. Pomembno področje naše raziskave, pa so tudi elektronska orožja-tehnologije, ki nam služijo, da se s sodobnimi pojavnimi oblikami terorizma spopadamo. Še posebej bo izpostavljena biometrija, kot del identifikacijske tehnologije s katero lahko identificiramo storilce kaznivega (terorističnega) dejanja. Vsak biometrični sistem vključuje tri osnovne postopke: registracija, priprava odčitanega vzorca in preverba ujemanja odčitanega vzorca s shranjenim digitaliziranim vzorcem v bazi podatkov. Prekoračitev razumne meje uporabe takšne tehnologije pa nas lahko hitro vodi v kratenje pravic do zasebnosti in tako človekovih pravic, zato bo tudi zasebnost področje našega študija, kateremu bomo v empiričnem delu raziskave namenili posebno pozornost. Informacijsko komunikacijska tehnologija (IKT) čedalje pogosteje postaja predmet zlorabe. V doktorskem delu bomo interdisciplinarno obravnavali terorizem in biometrijo skozi prizmo:

- upoštevanja človekovih pravic do zasebnosti,
- modernih oblik IKT orodij v funkciji terorizma,
- uporabe identifikacijskih metod v bojevanju proti terorizmu in
- podajanja ocene sprejemljivosti biometrije, ko gre za bojevanje proti terorizmu.

1.1 *Različne teorije, raziskovalni pristopi, pogledi in modeli obravnave terorizma*

V obdobju po hladni vojni je terorizem postal eno izmed najpomembnejših varnostno-političnih tem tudi v državah, ki sicer niso bile neposredno ogrožene. Skozi preteklost si strokovnjaki pri splošni obravnavi in definiranju terorizma kot pojava in njegove percepcije, največkrat niso bili enotni

(Gamage, 2010). Terorizem je verjetno star kot človeštvo (Barnaby, 2000; Lederberg, 1999; Sutton, 2003). Ne glede na to, da pojem zgodovinsko izvira iz časov francoske revolucije v l. 1793 in 1794 (Fossati, 2005), pa večina definicij največkrat izpostavlja uporabo sile ali nasilja, z namenom ustrahovati prebivalstvo. Etimološko gledano, je terorizem koncept, ki izhaja iz samostalnika »teror« in pomeni skrajni strah ali strah v najrazličnejših možnih oblikah (Rapoport, 2001). V tem kontekstu, je bil izraz »terorizem« na pravnem področju prvič uporabljen l. 1930 v Bruslju na mednarodni konferenci, ki je bila namenjena poenotenju kazenskega prava. Izraz »terorizem« je bil opredeljen kot namerna in sistematična uporaba nasilja za dosego določenih ciljev (Levasseur, 1977). Leta 1934, ko sta bila umorjena jugoslovanski kralj Karađorđević in francoski zunanji minister Barthou, so časopisi vsak dan opominjali na kugo tistega časa: mednarodni terorizem (Estevez, Pavolka in Nižňansky, 2006). Schmidt in Youngmen (2005) sta naštela kar 109 različnih definicij terorizma, ki sta jih pridobila v raziskavah vodilnih akademikov tega področja. Iz definicij in opredelitev terorizma so statistično največkrat zastopani naslednji (izolirani) ponavljajoči se elementi:

- nasilje, sila (se je pojavil v 83,5 % definicij),
- politično (65 %),
- strah, groza (51 %),
- grožnje (47 %),
- psihološki učinek in pričakovane reakcije (41,5 %),
- razhajanje med cilji in žrtvami (37,5 %),
- namerno, načrtovano, sistematično, organizirano delovanje (32 %) in
- način boja, strategije, taktike (30,5 %).

Sledijo izsiljevanje, želja po publiciteti, zastraševanje, nedolžnost žrtev ter kriminalni oz. zločinski značaj.

1.1.1 Teoretični pristopi k razumevanju terorizma

Kadar govorimo o terorizmu najprej pomislimo na izvedeno fizično nasilje in marsikdo je mnenja, da je informacijski terorizem predvsem pojavna oblika, katere namen je sejati strah s teroristično grožnjo, saj naj bi bilo nemogoče z

informacijskimi tehnologijami fizično ogrožati prebivalstvo. Kibernetski terorizem[3] je ena izmed najsodobnejših pojavnih oblik terorizma, ki ga nekateri avtorji vključujejo v okvir informacijskega bojevanja (Shahar, 1997), drugi pa menijo, da je informacijsko bojevanje popolno teroristično orožje (Janczewski, 2005; Colarik, 2006; Schiller, 2010). Izraz kibernetski terorizem, se nanaša na zbliževanje kibernetskega prostora in terorizma. V 80. letih prejšnjega stoletja ga je prvi uporabil Collin, raziskovalni sodelavec Inštituta za varnost in obveščevalno dejavnost v Kaliforniji (Denning, 1999). O kibernetskem terorizmu govorimo, ko so zaradi terorističnih napadov na kritično informacijsko infrastrukturo fizično ogrožena življenja in premoženje prebivalstva ter moteno normalno delovanje družbe (Blane, 2003; Cordesman, 2002; Quigley, 2008). Kibernetski terorizem pomeni protipravno namerno uporabo ali grožnjo uporabe nasilja, motenj ali interference kibernetskih sistemov, z verjetnostjo, da takšna uporaba povzroči smrt, poškodbo osebe ali oseb, dejansko škodo fizične lastnine, civilne nemire ali pomembno gospodarsko škodo (Information Warfare Site [IWS], 2011). Denning (2001) kibernetski terorizem definira kot politično motivirano hekersko aktivnost, z namenom, povzročiti resno škodo, smrt ali hudo gospodarsko škodo. Krasavin (2004) trdi, da vsaka namerna uporaba informacijske tehnologije terorističnih skupin in njihovih pripadnikov z namenom, da škoduje predstavlja kibernetski terorizem. Kibernetski terorizem je mogoče opredeliti z uporabo računalnika politično motivirane mednarodne ali sub-nacionalne skupine kot orožje ali kot cilj, za ogrožanje ali povzročitev nasilja in strahu, da bi vplivali na občinstvo, ali povzročili, da neka vlada spremeni svojo politiko (Hutter, 2002). Ta definicija, združuje več mnenj o kibernetskemu terorizmu in zajema tri načine delovanja: fizični, elektronski in informacijski, za napade na računalnike (Congressional Research Service [CRS], 2005). Mehka verzija definicije informacijskega terorizma izpostavlja predvsem IKT, ki jih teroristi uporabljajo za izvajanje pritiska in propagando, namenjeno javnosti in mobiliziranje ter rekrutiranje novih podpornikov (Müller, Wille in Björn,

[3] Kibernetski terorizem; Standardizirane definicije računalniške kriminalitete v funkciji terorizma, veljavne na svetovnem nivoju še ni (Blane, 2003).

2004). Od oblike delovanja in želje uničevanja, so namreč posledice zlonamerne uporabe IKT lahko zelo različne. Po Hoffmanu (1999) ima ta nova oblika trorizma tudi večjo ubojnost. Lahko bi rekli, da gre v primeru kibernetskega terorizma za delovanje, pri katerem sicer neposredno ne pride do poškodovanja lastnine ali ljudi. Samo oškodovanje pri tej obliki kriminala, se največkrat res ne pokaže neposredno, vendar so posredni učinki delovanja lahko katastrofalni tudi za ljudi (Nass in Brave, 2005). Kljub temu pa je kibernetski terorizem po mnenju nekaterih strokovnjakov zapleteno definirati (Murrill, 2011). Ob tem se seveda zastavljajo mnoga vprašanja: »Ali pri računalniškem (kibernetskem) kriminalu ne gre zgolj za varnostno temo, ki jo pogojuje vsesplošna medijska vojna proti terorizmu?« in »Ali ni kibernetski terorizem, delovanje nenevarnih računalniških zanesenjakov željnih medijskega dokazovanja, ki pri svojem delovanju nimajo globjih zlonamernih ciljev in je to bolj ali manj fikcija? (Pollitt, 1997)«. V primeru, da kdo ostane brez elektronske pošte, ker je napadalec onesposobil poštni (e-Mail) strežnik, to seveda ni neko hudo nasilje, ki bi ga lahko označili s terorizmom (Malcolm, 2004; Malik, 2011; Kumar-Singh, 2009; Grabosky in Stohl, 2010). Ne moremo namreč vsako kaznivo dejanje označiti kot terorizem (Adelman, 2010). Tudi vsako politično motivirano nasilje ni terorizem (Maynes, 1986). Za razliko od tradicionalnih komunikacijskih medijev, je internet kot najzmogljivejše komunikacijsko sredstvo vse pomembnejši, tudi za komuniciranje in načrtovanje operacij prostorsko in organizacijsko dislociranih terorističnih organizacij (Weimann, 2005; Bidgoli, 2004; Axelrod, 2009; Vacca, 2007). Le-te danes niso hierarhično in centralizirano organizirane, ampak povzemajo sodobne mrežne oblike (celice) (Rapoport, 2001; Miholič, 2004). Ne glede na različna izhodišča in odprta vprašanja pa ostaja nesporno dejstvo, da so IKT sredstvo in hkrati cilj terorističnega delovanja v 21. stoletju (Coker, 2008; Ryder, 2011). Glede ustrahovanja pa je seveda jasno, da brez medijev in danes pomembnih interaktivnih IKT, o terorizmu ni mogoče govoriti. Medijsko posredovanje in prikaz terorističnih dejanj, omogoča zaznavo občutka strahu in ogroženosti, ki je mnogo večja od tiste, ki jo kažejo podatki o številu žrtev ali poškodovanih v napadih (Glüpker, 2009).

1.1.2 Pregled raziskav na področju terorizma

Število raziskav (Schuster et al., 2001; Lerner, Gonzalez, Small in Fischhoff, 2003) o dojemanju in psiholoških posledicah terorističnih napadov se je povečalo v zadnjih letih zaradi pojava številnih dogodkov, kot so teroristični napadi 11. septembra 2001 in bombni napadi l. 2004 in 2005 v Madridu in Londonu. 19,2% anketirancev, ki so bili vključeni v raziskavo, glede dojemanja osebne bolečine v terorističnem napadu, so po enem letu še vedno čutili zelo močno prisotno psihološko bolečino (Fischhoff, Gonzalez, Lerner in Small, 2005). Raziskava Londončanov, glede reakcije na bombne napade julija 2005 je pokazala, da so doživeli manj psihičnega stresa, kot anketiranci v ZDA, po napadih septembra 2001 (Rubin, Brewin, Greenberg, Simpson in Wessely, 2005). Raziskave glede dojemanja groženj terorizma potrjujejo, da so identificirani dejavniki, ki lahko privedejo do negativnih učinkov na psihično dobro počutje, gospodarstvo ali medskupinske odnose in tudi predstavljajo posredne negativne učinke na poslovanje (Slovic, 2002; Lemyre, Clement in Gibson, 2004).

1.2 *Različne teorije in modeli obravnavanja zasebnosti*

V današnji družbi, so etična vprašanja pomembna za informacijske in identifikacijske tehnologije in soočanje z etičnimi vprašanji v procesu sprejemljivosti je neizogibno. Ker družba v osnovi pomeni skupnost ni mogoče živeti brez ureditve in pravil, ki opredeljujejo kaj se v tej skupnosti lahko stori in kaj se ne sme storiti (Boyle, 2002). Na splošno velja, da nam etika pomaga, da mirno živimo v družbi.

Uporaba računalniške, IKT in identifikacijske tehnologije, ki se uporablja na vseh področjih poslovnega sektorja, industrije in izobraževanja ter širše javnosti, pa je priložnost za neetične uporabe ali zlorabe te tehnologije. Primeri neetične in tudi nezakonite uporabe te tehnologije so različni prekrški glede zasebnosti, npr. nepooblaščen dostop, ustvarjanje virusov in črvov,

kršitev varnosti, piratstvo programske opreme zloraba osebnih podatkov[4] in nepooblaščeni nadzor (Kazenski zakonik Republike Slovenije [KZ-1], 2008), ki jih izvajajo različne organizirane ali neorganizirane skupine in posamezniki. Podjetja v zadnjem času investirajo velik znesek proračuna, za računalniško varnost in preventivne ukrepe na tem področju (varnostna orodja in politike). Med raziskavami in teorijami, ki so povezane z modeli odločanja se avtorji (Henry in Pierce, 1994; Loch in Conger, 1996; Goles, White, Beebe, Dorantes in Hewitt, 2006; Haines in Leonard, 2007) ukvarjajo z vprašanjem sprejemljivosti IKT tehnologije glede na zasebnost, kot temeljno človekovo pravico. Ker gre pri neetičnem vedenju posameznikov za človeški problem, je treba opozoriti, da se z uporabo računalnika dogajajo tudi zlorabe (Henry in Pierce, 1994). Etična odločitev je proces, ki lahko vpliva na okolje posameznika (na primer družbeno okolje, sistem prepričanja, osebno okolje, osebne vrednote, strokovno okolje, pravno okolje in poslovno okolje). Študije o etiki odločanja v okviru IKT se na splošno odvijajo v dveh smereh (Haines in Leonard, 2007). Prvič, raziskave se osredotočajo na pregled demografskih in osebnostnih stilov posameznikov in drugič se osredotočajo na proces etičnega odločanja, da bi našli prepričanja, stališča in dejavnike, ki vodijo do neetičnega ravnanja. V zadnjem času, je zasebnost informacij ena izmed najbolj pomembnih delov na varnostnem področju in je postala pomembno etično vprašanje računalniške etike. Zato, da bi razumeli, zakaj je zasebnost pomembna za etična vprašanja, obstaja kar nekaj empiričnih raziskav in študij o zasebnosti. Haines in Leonard (2007) navajata, da je treba etične vedenjske namere in zasebnost raziskovati v zvezi s spremembami v IKT. Raziskave predstavljajo in obravnavajo tudi zasebnost v povezavi z različnimi teorijami in modeli. Prav tako obravnavajo moralni razvoj, ki obsega dele moralne naslednje intenzivnosti: splošni moralni imperativ, moralne razloge in proces etičnega odločanja.

[4] KZ-1 (2008) ne obravnava tatvine ali kraje identitete (ang. identity theft), ampak to dejanje obravnava kot zlorabo osebnih podatkov (154/2. člen) (Ministrstvo za notranje zadeve [MNZ], 2008). V nalogi bomo v nadeljevnju uporabili termin »zloraba osebnih podatkov«.

1.3 *Začetki modernega bojevanja proti terorizmu v Evropi*

Začetke moderne dobe evropskega boja proti terorizmu lahko najdemo že v sedemdesetih letih z ustanovitvijo mednarodne skupine (Terrorisme, Radicalisme, Extrémisme et Violence Internationale - TREVI) za boj proti terorizmu, radikalizmu in ekstremizmu l. 1975 in s podpisom Evropske konvencije o zatiranju terorizma (European Convention on the Suppression of Terrorism) iz l. 1977 (Casale, 2008). TREVI skupina je bila ustanovljena s strani evropskih policijskih uradnikov z namenom izmenjave informacij in medsebojne pomoči na področju terorizma in z njim povezanih mednarodnih zločinov. To je bil sprva forum za izmenjavo informacij o organiziranemu kriminalu in terorizmu. Skupina je bila sestavljena iz ministrov za pravosodje in notranjih zadev ter visokih uradnikov za nacionalno varnost. Dejavnosti TREVI skupine je naknadno uradno odobrila skupina evropskih ministrov za pravosodje in notranje zadeve. Z delovanjem TREVI, je združena Evropa dosegla dogovore v kooperativnem boju proti terorizmu, kot so policijska delovna skupina za področje terorizma in boja proti terorističnim skupinam. Delovala je do l. 1992, ko jo nadomestijo z določbami Maastrichtskega tretjega stebra, ki vključuje področje priseljevanja in azila, policije, carine in pravnega sodelovanje (Casale, 2008). Leta 1993 so se evropske institucije, ki se ukvarjajo s pravnimi, carinskimi, vprašanji ter vprašanji priseljevanja, združile s pogodbo (poglavje 4) o Evropski Uniji (EU) (Treaty on European Union [TEU], 1992). Poglavje štiri, omenjene pogodbe, zadeva vse izravnalne ukrepe, ki bi jih bilo treba sprejeti, ko je bila sprejeta odprava nadzora na mejah med državami članicami EU (Benyon, 1997). S podpisom Maastrichtske pogodbe je bil ustanovljen tudi Evropski policijski urad (Europol). Leta 1997 je bila za boj proti terorizmu ustanovljena pripravljalna skupina, z namenom oblikovanja vloge Europola na področju boja proti terorizmu. Europol je tako začel delovati l. 1998 (Rauchs in Koenig, 2001). Kljub povečanju mednarodnega policijskega sodelovanja, najprej skupina TREVI in kasneje še druge podobne organizacije, katerih cilj je krepitev dvostranskega sodelovanja, je l. 2001 prišlo do napadov v New Yorku in Washingtonu. Evropsko sodelovanje na področju boja proti mednarodnemu terorizmu je še vedno precej omejeno. Za države članice EU in članice evropske gospodarske

skupnosti (EGS), je to občutljivo področje, saj nacionalno varnost štejejo kot del svoje suverenosti (Wilkinson, 2005).

Težave pri mednarodnemu sodelovanju v boju proti terorizmu nastanejo že pri opredelitvi terorizma v mednarodnem pravu in posledično, v evropskem pravu, kot regionalnemu instrumentu za boj proti terorizmu. To predstavlja velik problem z natančno pravno opredelitvijo terorizma kot pojava in kaznivega dejanja. Drugič, se pojavi vprašanje, »V kako veliki meri je treba razširiti opredelitev kaznivega dejanja terorizma?«. Z drugimi besedami, to slednje je vprašanje identifikacije vedenja, ki ga je treba zajeti v pravno opredelitev terorizma tako, da se lahko storilca opredeli, kot terorista (Shaw, 2003; Cassese, 2001). Težava pri ugotavljanju skupne opredelitve terorizma se kaže tudi v zgodovini evropskega boja proti terorizmu. EU zakonodaja in dokumentacija v preteklosti za terorizem sploh ne poda (pravne) opredelitve kaznivega dejanja. Po terorističnih napadih v združenih državah Amerike (ZDA) l. 2001, je potreba po skupni opredelitvi postala ključnega pomena in okvirni sklep o boju proti terorizmu podpisan dne 13. junija 2002 premosti to vrzel, ki uvaja celovito in usklajeno opredelitev terorizma v zakonodaji EU (Council of the European Union, 2002a). Kasneje l. 2004 iz tega nastane evropska deklaracija za boj proti terorizmu (Council of the European Union, 2004). Ta odločitev dokončno ugotavlja minimalna merila, ki opisujejo sestavne elemente kaznivega dejanja terorizma (Den Boer, 2003). Odločba opredeljuje terorizem, ga razlikuje po skupinah od navadnega kaznivega dejanja in se osredotoča na namen, ki ga zasleduje kaznivo dejanje. Izvirnost opredelitev izhaja iz dejstva, da končni politični cilj predstavlja osnovna merila za razlikovanje terorističnega kaznivega dejanja od drugih kaznivih dejanj (Tillema, 2010; Colarik, 2006). Dejstvo je, da na nacionalni ravni skupna mednarodna zakonodaja opredeli inkriminacijo terorizma (in drugih kaznivih dejanj), ne glede na svoj cilj in se osredotoča na (prepovedane) teroristične dejavnosti (Saul, 2003). Šestinštirideseti člen prvega okvirnega sklepa po nacionalni zakonodaji določa kot teroristična »kazniva dejanja«, vsa dejanja, ki zaradi svojega značaja ali vsebine hudo škodujejo državi ali mednarodni organizaciji, kadar so storjena z namenom, da bi:

1. resno zastraševala prebivalstvo,
2. nezakonito izsiljevala vlado ali mednarodno organizacijo, da izvede ali opusti kakršnokoli dejanje in
3. resno rušila ali uničevala temeljne politične, ustavne, gospodarske ali socialne strukture države ali mednarodne organizacije.

Poleg teh osnovnih točk terorističnih kaznivih dejanj, sklep Sveta Europe opredeljuje tudi tri druge kategorije kaznivih dejanj (Troosters, 2004):

- drugi člen opredeljuje kazniva dejanja v povezavi s teroristično skupino, poudarja nujnost kaznovanja vsakogar, ki sodeluje s teroristično skupino (s podporo, finančnimi sredstvi ali prispevki k dejavnosti skupine),
- tretji člen opisuje kazniva dejanja, povezana s terorističnimi dejavnostmi in sicer deluje kot predpriprava za teroristična dejanja, kot so izsiljevanja in ponarejanja listin in
- četrti člen poziva države članice, naj sprejmejo ukrepe, tudi proti nadaljnjim dejavnostim, kot so spodbujanje, pomoč, podpora in poskus terorističnega delovanja.

Pravno-sistemsko so ta teroristična dejanja zajeta tudi v veljavnem Kazenskem zakoniku Republike Slovenije (Uradni list RS, št. 55/2008 in 66/2008). V členih 108., 109., 110. in 111. so kogentno regulirana kazniva dejanja, ki v slovenskem pravnem redu pomenijo kazniva dejanja terorizma (Tičar, 2010).

Evropski nalog za prijetje (European Arrest Warrant - EAW) je zelo pomemben del zakonodaje EU na področju boja proti terorizmu po napadih v New Yorku in Washingt- onu l. 2001 in tudi najbolj inovativno zakonodajno orodje na tem področju. Že l. 1999, se je na vrhu Evropskega sveta v Tampereju, izdelal okvir za sporazum (Španija in Veliki Britanija) za spodbujanje med evropskimi voditelji držav, po katerih je zakon o izročitvi treba posodobiti med državami članicami, kar zadeva osebe, ki so bile pravnomočno obsojene in ga nadomestiti s preprostejšim zakonom glede predaje teh oseb (Council of the European Union, 1999). Politični dogovor je bil dosežen v l. 2001, okvirni sklep pa je bil dokončno sprejet l. 2002 (Council of the European Union,

2002b). Začel je veljati l. 2004 in je nadomestil prejšnje postopke izročitve med državami. Zadnja članica, ki je sprejela EAW je bila Italija l. 2005. Cilj evropskega naloga za prijetje je izboljšati pravosodno sodelovanje v EU in ustvariti poenostavljen sistem predaje obsojenih in osumljenih oseb z namenom pregona ali izvršitve kazenskih sankcij ter odstraniti stare zamudne dvostranske postopke izročitve. EAW temelji na zaupanju vseh držav članic v pravnem sistemu vsake druge države članice in o vzajemnem priznavanju odločitev nacionalnih sodišč. Zato je Evropski svet navedel, da je EAW temelj EU pravosodnega sodelovanja, v zvezi z realizacijo učinkovitejše območje svobode, varnosti in pravice v Evropske unije. Na praktični in operativni ravni, so zelo pomembne posledice uvedbe evropskega naloga za prijetje. Dejansko lahko nacionalni pravosodni organ izda zahtevo za prijetje in izročitev (in sicer, evropski nalog za prijetje), ki velja v vsej EU, za osebe, obtožene hudih kaznivih dejanj (kaznuje s kaznijo v višini najmanj 10 let zapora) ali za osebo, obsojeno na najmanj 4 mesece zapora. Zahtevane osebe je v tem primeru treba takoj prijeti in predati na zahtevo države članice (Blekxtoon, 2004).

Ob vseh dobrih plateh skupne zakonodaje, pa so bile kritike skupnih EAW še posebej močne. Dejstvo je, da je z uvedbo evropskega naloga za prijetje, postala izročitev osumljenca in morda izrek smrtne kazni v ZDA lažja, čemur pa vse evropske države nasprotujejo. Delna rešitev tega spornega vprašanja, je bil okvirni sklep Sveta (Preambula 13): »Osebe se ne sme odstraniti, izgnati ali izročiti državi, kjer obstaja resna nevarnost, da bo nekdo podvržen smrtni kazni, mučenju ali nečloveškemu ali ponižujočemu ravnanju ali kaznovanju«. Kljub temu ostaja nekaj nejasnosti, saj se zdi ta določba bolj kot načelna izjava, ne pa obveznost držav članic. Še pomembneje je, da se je s sprejetjem EAW in spremembami zakonodaje, pojavilo veliko ustavnih vprašanj, nekaterih držav članic (European Union Committee, 2006). Na primer, nemško ustavno sodišče razglasi za neveljavne, nekatere nemške določbe zakona, ki izvajajo določbe okvirnega sklepa o EAW (odločba iz l. 2005), ker je obstajala domneva, da je ta določba proti temeljnim človeškim pravicam. Zdi se, da bi izboljšanje učinkovitosti pravosodnega sodelovanja, zlasti s pomočjo poenostavljenih in hitrejših postopkov predaje, lahko

zmanjšalo osnovne pravice do obrambe in pravice do poštenega sojenja v državah članicah, ki jih njihove ustavne listine (poleg tega, da temeljna načela priznajo v mednarodnem pravu), zagotavljajo (Centre for European Policy Study [CEPS], 2006). To pa lahko vodi do konflikta med ustavnim sodiščem in evropskimi institucijami ter neželenih ustavnih posledic, zaradi pravosodnega sodelovanja med državami članicami (Satzger in Pohl, 2006; Euractiv, 2005). Večkrat je celo praksa, da države iz bilateralnih pogodb izključujejo menjavo storilcev političnih kaznivih dejanj (Černič-Letnar, 2011).

Ob vsej tej pravni aktivnosti držav članic, je potrebno raziskati še posledice uporabe biometrične tehnologije v boju proti terorizmu. Biometrija je najbolj inovativno tehnološko orodje med metodami boja proti terorizmu, vendar so njena učinkovitost v boju proti terorizmu in prav tako tudi posledice določb glede njene uporabe, lahko sporne za državljanske svoboščine. Analiza biometričnih podatkov, povezanih članic EU je temeljni okvir za boj proti terorizmu. Opredelitev biometrične tehnologije v boju proti terorizmu najdemo v poročilu o vplivu biometrije na zasebnost, ki ga je pripravil raziskovalni center pri Evropski komisiji (Join Research Center [JRC], 2005). Biometrija je fizična ali biološka lastnost ali atribut (glas, oči, ali prstnih odtisov) posameznikov, ki jo je mogoče izmeriti. Biometrična identifikacija in tehnologije preverjanja identitete, ki jih je izbrala Evropska komisija kot biometrične identifikatorje, so: prepoznavanje na osnovi obraza, prstnega odtisa, šarenice in deoksiribonukleinska kislina - DNK. Skratka, biometrični podatek, je opredeljen kot element za samodejno prepoznavanje osebe, na osnovi razlike fizične ali biološke lastnosti (Woodward, Horn, Gatune in Thomas, 2003a). Po napadih 11. septembra 2001 je EU začela razvijati elemente usklajene strategije za izboljšanje varnosti osebnih dokumentov z uporabo biometričnih identifikatorjev. Evropski svet je v Laeknu (2001) in Sevilli (2002) odločil, da se v vizumski informacijski sistem (VIS) vključujejo tudi biometrični podatki z namenom, izboljšanja upravljanja skupne vizumske politike in prispevati k izboljševanju notranje varnosti in boja proti terorizmu. Evropska komisija je predstavila predloge za uvedbo biometričnih vizumov in

dovoljenj za prebivanje za državljane tretjih držav (European Commission, 2003). Leta 2005 je Evropski svet predstavil osnutek sklepov predstavnikov vlad držav članic o skupnih minimalnih varnostnih standardih identifikacijskih kartic za države članice (Council of the European Union, 2005). To daje zagon za razvoj skupnih varnostnih standardov in varnih postopkov izdaje nacionalne osebne izkaznice.

Kritike biometričnih podatkov skrbi, da lahko takšen sistem, ki temelji na ideji velike centralizirane podatkovne baze, privede do erozije osebnih svoboščin. Skrbi jih, da bo nujna uporaba biometričnih podatkov enkrat dodobra uveljavljena in razširjena, glede na količino podatkov, ki bodo zbrani, da se bo sistem uporabljal v vsakdanjem življenju. To je očitno ključno vprašanje v zvezi z ravnotežjem med svobodo in varnostjo. Skrbi z varstvom teh osnovnih pravic, so prisotne tudi v institucijah EU. Poročevalec evropskega parlamenta o biometričnih vizumih Sorensen, je dejal, da so predlogi o uporabi biometričnih podatkov in sistematičnega in centraliziranega shranjevanja občutljivih osebnih podatkov, preveč skrajni glede na pojav problema terorizma (Euractiv, 2004). Hkrati je ugotovil, da iz vidika varstva podatkov, lahko takšno centralno shranjevanje biometričnih podatkov ogroža varstvo državljanskih pravic, zlasti pravico do zasebnosti. Vpliv biometrične tehnologije temelji na modelu zaupanja med državljani in državo, kar je tudi poudarjeno v poročilu sodišča evropskih skupnosti. Ob vladnih težnjah k varnosti se zdi, da izpodbijajo temeljni koncept zaupanja. Obstaja tveganje, da je poudarek na spremembah zaradi varnosti za navadne državljane skoraj enak, kot za osumljence kaznivih dejanj in je meja pravice do zasebnosti in anonimnosti umaknjena (JRC, 2005). V kolikor bi državljani kratkoročno, do določene mere lahko žrtvovali svoje osebne svoboščine za bolj varen svet, bi dolgoročno to žrtvovanje lahko postalo nepriljubljeno in bi vodilo v spodkopavanje zaupanja v vlado. Mnoge tudi skrbi, da če biometrični podatki postanejo skupni način priznanja identitete, bodo biometrični podatki, posledično vezani na vse druge osebne podatke. Kot rezultat, se lahko te podatke in občutljive informacije nenamerno uporabi za vse vrste drugih namenov in bodo zagotovo nagnjeni k zlorabam. Prav tako se z uvedbo

biometričnih potnih listov in osebnih izkaznic, kot tudi nove EU zdravstvene izkaznice, vozniških dovoljenj ob uporabi biometrične tehnologije, zagotovo gibljemo v smeri nadzora družbe (Bunyan, 2005).

Torej, je izražena še posebej močna zahteva po učinkovitih tehnologijah zasebnosti in varstva podatkov. S tega vidika poročilo komisije navaja, da je potreben okrepljen pravni okvir za varstvo zasebnosti in podatkov, ob uvajanju biometrije za preprečevanje terorizma, ki bi lahko postala orodje v službi za nadzor posameznika. Evropski parlament je z direktivo o varstvu podatkov (95/46/EC) l. 1995 dal v uporabo splošne določbe o zaščiti osebnih podatkov o posameznikih. Vendar pa je prišlo do spoznanja, da je tehnologija presegla zahteve glede zasebnosti obstoječe zakonodaje. Da bi našli rešitev, je bil l. 2005 ustanovljen v okviru šestega okvirnega programa EU za raziskave, evropski projekt za preučitev etičnih posledic povečane uporabe biometrične tehnologije. Cilj projekta, imenovan BITE (Biometric Identification Technology Ethics), je uvedba socialnih, pravnih in etičnih norm za razpravo glede uporabe biometrije, ki vključuje vse vpletene strani (Euractiv, 2005).

Glede na vse je sedaj mogoče sestaviti nekaj zaključnih pripomb iz analize EU okvira za boj proti terorizmu, zlasti glede jedra te analize, ki se nanaša na uporabo biometrične tehnologije kot njene glavne značilnosti, v zvezi z vprašanjem problematike in perspektive EU za boj proti terorizmu in politike na institucionalni in pravni ravni.

Zaradi dolge zgodovine in kolektivne izkušnje v boju proti terorizmu v Evropi, se je lahko Evropska pravna in institucionalna struktura na področju pravosodja in notranjih zadev hitro prilagodila na povečano varnostno tveganje. Še vedno pa se soočajo z vprašanjem glede dogodkov ob in po 11. septembru 2001. Čeprav so se države članice morale soočiti z novo grožnjo v obliki mednarodnih mrež terorističnih skupin, je treba priznati, da je bilo s strani evropskih držav opravljenih veliko prizadevanj in pomembnih korakov naprej. Prav tako so združeni narodi sprejeli resolucije za skupen boj proti

terorizmu (United Natons Office of Drug Criminal [UNODC], 2011). V terorističnih napadih v Madridu (2004) in Londonu (2005), kot tudi s terorizmom povezanih dejavnosti v nekaterih evropskih državah, so se okrepile javne in politične skrbi za varnost. Države Evropske unije so se odzvale s preoblikovanjem institucionalnih struktur na področju pravosodja in notranjih zadev (krepitev vloge Europola in o ustanovitvi Eurojusta) in sicer z uvedbo nove zakonodaje proti terorizmu, kot je evropski nalog za prijetje in financiranju terorizma. Ukrepi neodvisnega medvladnega organa za finančno ukrepanje (Financial Action Task Force - FATF), razvijajo in spodbujajo politiko za zaščito svetovnega finančnega sistema proti pranju denarja in financiranju terorizma. Priporočila, ki jih izda FATF so opredelitve do kazenskega pravosodja in regulativni ukrepi, ki jih je potrebno izvajati za reševanje tega problema. Ta priporočila vključujejo tudi mednarodno sodelovanje in preventivne ukrepe, ki jih morajo sprejeti finančne in druge institucije, kot so igralnice, prodajalci nepremičnin, odvetniki in računovodje. Priporočila FATF so priznana kot standard globalnega boja proti pranju denarja (Anti Money Loundering - AML) in boja proti financiranju terorizma (Combating the Financing Terrorism - CFT) in (Financial Action Task Force [FATF], 2009).

Širok pristop EU, ki ga sestavljajo štiri glavne prednostne naloge (preprečevanje, zaščita, preganjanje in odzivanje) je hvalevreden, ker učinkovito implementira protiteroristične politike vendar je potrebno veliko več kot pregon in zunanja obramba. Čeprav se priznava krepitev učinkovitega sodelovanja med državami za boj proti terorizmu, je prav tako potrebno upoštevati, da mora EU okrepiti svoja prizadevanja še za odpravo vrzeli in pomanjkljivosti, ki izhajajo iz institucionalnih in pravnih okvirov protiteroristične politike EU glede uporabe identifikacijske tehnologije. Posebni kazenski in zato protiteroristični ukrepi so v pristojnosti držav članic. Glavna vloga EU, je zato usklajevanje. Ampak, da bi bila uspešna pri tej nalogi, EU v prvi vrsti potrebuje celovit in skladen institucionalni okvir za boj proti terorizmu. Namesto tega je sedanja evropska institucionalna arhitektura boja proti terorizmu sestavljena iz preveč akterjev, s podvajanjem in

prekrivanjem nalog. Takšen način pa kaže na spremembo odnosa do posameznih (varnostnih, obrambnih in zunanjih) politik neke države. Znano je, da je treba delovati na več področjih, uskladiti ukrepe različnih družb in akterjev kriminalne prevencije, v nasprotnem primeru se pokaže, da levica ne ve kaj dela desnica. Zavedanje o tem bi moralo biti prisotno pri vseh snovalcih kriminalitetne politike (Meško, 2000).

Beseda biometrija (ang. biometry) izhaja iz grških besed bios (življenje) in metrikos (meriti) (Prabhakar, Pankanti in Jain, 2003). Slovenski medicinski slovar (2009) biometrijo opredeli kot vedo, ki uporablja merjenje in statistično analizo na vseh področjih biologije in kot sinonim uporablja izraz »biometrika«. Temelji na uporabi telesnih značilnosti, kot načinu identifikacije in nadzorovanja oseb (Fitzpatrick, 2002). Gre za proces zbiranja, procesiranja in shranjevanja podatkov o posameznikovih fizičnih in bioloških (vedenjskih) lastnostih z namenom osebne identifikacije (Kovačič, 2006). Raziskovanje teh človeških lastnosti pa je pot k medsebojnemu ločevanju oseb (Trapečar in Robek, 2003). Prvi prstni odtisi so bili najdeni med izkopaninami starodavnih mest Jericho in Paphos iz 7000 l. pr. n. št. (Maier in Karageorghis, 1984). Za časa vladavine Hamurabija Babilonu v 19. st. pr. n. št., so prstne odtise uporabljali za pečate pogodb. Antični Egipt in Kitajska sta odigrala pomembno vlogo v razvoju biometrije (Ashbaugh, 1991). Izvor biometričnih podatkov lahko zasledimo že v 12. stoletju na Kitajskem. Angleški raziskovalec Barrow je v 18. stoletju zapisal, da so kitajski trgovci z odtisi stopal na papirju razlikovali otroke (Galton, 2003). Zanimivo je, da to prakso še danes uporabljajo v nekaterih delih sveta. Faulds (1880) objavi članek, ki razpravlja o prstnih odtisih na osnovi uporabe tankega filma črnila. Obravnava tudi možnost uporabe prstnih odtisov za identifikacijo kriminalcev. Prvo uporabo prstnih odtisov kot uradni način identifikacije potrdi argentinski policijski uradnik Vucetich l. 1893 (Kaye, 1995). Uporaba temelji na vzorcih, ki jih je opisal Galton. Ameriški zvezni preiskovalni urad (Federal Bureau of Investigation - FBI) l. 1924 uvede oddelek za identifikacijo, ki začne delo na osnovi zapisov in baze prstnih odtisov. Kasneje, v 19. stoletju, je antropolog Bertillon poskušal najti način za identifikacijo zločincev. Razvil je sistem

imenovan »Bertillonage«, ki uporablja fizikalne značilnosti (telesne dimenzije), kot sredstvo za identifikacijo zločincev. Ta sistem je lahko napačno identificiral zločinca, saj je lahko več oseb imelo enake lastnosti, ki jih je Bertillon uporabljal za identifikacijo. Pomanjkljivosti Bertillonovega sistema so v začetku 20. stoletja spodbudile Henrya, da razvije bolj zanesljive metode za odkrivanje kaznivih dejanj (Komarinski, 2005). Henry je temeljil na desetprstni klasifikaciji odtisov, kot najbolj natančnemu načinu identifikacije (Kaye, 1995). Policija v Scotland Yardu ga je sprejela kot glavni način identifikacije v kazenskih zadevah. FBI ga med drugimi, uporablja še danes. Battley l. 1930 razvije prvi enoprstni sistem prstnih odtisov (Maver, 2004). Ideja identifikacijskega sistema na osnovi prepoznave šarenice, postane aktualna l. 1985. Zvezna država Illinois l. 1991 sprejme zakon, da podatke vseh oseb s kriminalno preteklostjo avtomatično zbira in vzdržuje država in, da so na voljo sodiščem (ki imajo pooblastila za pridobitev informacij za aretacijo in obsodbe) v skladu s statutom. Zvezna država Illinois l.1992 začne z elektronskim zajemom prstnih odtisov (U.S. Congress, 1991). Razvoj algoritma za prepoznavo šarenice je bil patentiran l. 1994 in leto kasneje postane dostopen kot prvi komercialni identifikacijski sistem. Ob napadu na Irak l. 2003, je bila ameriška vojska opremljena z najbolj napredno tehnologijo, za ugotavljanje (potencialnih) teroristov na osnovi fizičnih lastnosti (Gorman, 2011).

Problematika, s katero se ukvarja tako rekoč večina raziskovalcev tega področja, zadeva predvsem odsotnost nedvoumne in jasne definicije zasebnosti. Ta nedorečenost je delno tudi posledica tega, da sta pojem in obseg pravice do zasebnosti podvržena nenehnim vplivom družbenih in varnostnih sprememb. V Bruslju so sprejeli nekaj novih ukrepov za izboljšanje dostopnosti do evropskih podatkovnih baz, tako da bi članice EU in Europol imeli dostop do vizumskega informacijskega sistema (VIS) ter do baze prstnih odtisov prosilcev za azil in nezakonitih priseljencev (European Dactyloscopy - EURODAC). S tem naj bi državljani EU dobili pomemben branik pred največjo grožnjo 21. stoletja, terorizmom. Hustinx (2006) meni, da se pri oblikovanju omenjenih podatkovnih baz žal ni dovolj upoštevala zaščita osebnih podatkov.

Interoperativnost teh podatkovnih zbirk povečuje nevarnost za državljane, saj omogoča nov dostop do osebnih podatkov. Zato je po njegovem nujno, da se zadeva pozorneje preuči. EU je na ukaz ZDA vse državljane obvezala k lastništvu biometričnih potnih listov, če želijo potovati v ZDA. Evropa si je za jemanje prstnih odtisov in odčitavanje črtnih kod očesnih šarenic od ZDA skušala izprositi še nekaj časa. EU oziroma njena uprava se je odločila, da malce upočasni projekt implementacije biometrije. Rezultati v zvezi z napredovanjem Lizbonske strategije, po kateri naj bi EU do l. 2010 implementirala biometrijo na vstopnih točkah v države, tako še ne dosegajo začrtanih ciljev.

1.4 *Znanstveno raziskovalno področje in opredelitev pojmov*

Spremembe na znanstvenoraziskovalnem področju IKT in terorizma so opazne v mnogih vejah znanosti, nanje kažejo strokovne knjige, pomembne konference, k določeni temi usmerjene strokovne revije in nastanek novih raziskovalnih združenj. Podobno se dogaja tudi s proučevanjem zasebnosti na področju biometrije (kriptologija, šifrirni algoritmi itd.). Biometriji je namenjenih kar nekaj mednarodnih konferenc (npr.: International Conference on Biometrics, The Biometric Consortium Conference). Prav tako se na področju terorizma odvijajo svetovne konference (npr.: Institut for Counter Terrorism Conference, Australian Counter Terrorism Conference itd.). Število znanstvenih člankov omenjenih tematik je v zadnjem času zelo naraslo, kar kaže na vse pomembnejšo vlogo tega področja v raziskovalni dejavnosti. Biometrične tehnologije so v velikem razmahu in se čedalje bolj širijo tudi na nova področja uporabe, kot so finančni posli, boj proti kriminaliteti in terorizmu, elektronsko bančništvo, dostop do podatkov, pravosodje, obmejni vstopi, varnostni sistemi, letališča, zapori itd. Kjer sta potrebni največja varnost in zanesljivost, se uporabljajo t. i. večmodalni[5] sistemi za preverjanje identifikacije in istovetnosti (JRC, 2005). Pregled relevantnih znanstvenih baz

[5] Večslojni (ang. multilayered) aplikacijski sistemi; združujejo več tehnologij nadzora in tako še bistveno povečajo zanesljivost sistema (Community Research and Development Information Service [CORDIS], 2003).

kaže, da ugotavljanje sprejemljivosti biometričnih identifikacijskih sistemov neposredno pri anketirancih, katere ločimo na poznavalce in nepoznavalce biometrične tehnologije, ni dobro raziskano. Prednjačijo študije za ugotavljanje sprejemljivosti biometrije na osnovi raziskave vzorca splošne populacije, ki lahko poda izkrivljeno sliko o njeni sprejemljivosti. Preden se posameznik ali družba odloči za implementacijo in uporabo določene biometrične identifikacije, je vsekakor nujno raziskati in analizirati prednosti in slabosti različnih biometričnih tehnik (tabela 1), da bi lahko zagotovili namenskost in učinkovitost biometričnega sistema (Kapczyński, 2006).

Tabela 1: Stopnja združljivosti biometrije s posamezno zahtevo: (N)izka, (S)rednja, (V)isoka (Jain, Bolle in Pankanti, 1999)

	splošnost	posebnost	trajnost	dosegljivost	zmogljivost	sprejemljivost
	Vsak človek ima biometrične podatke, ki jih je moč uporabiti v namen identifikacije	Za vsakega človeka so to unikatne značilnosti in se ne ponavljajo	Značilnosti se s časom ne spremenijo veliko	Možno jih je hitro zajeti in med seboj primerjati	Kolikšna je verjetnost pravilne identifikacije	Ljudje bomo morali biometrijo sprejeti kot nekaj običajnega in nenevarnega
DNK	V	V	V	N	V	N
obraz	V	N	S	V	N	V
prstni odtisi	S	V	V	S	V	S
šarenica	V	V	V	S	V	N
glas	S	N	N	S	N	V
podpis	N	N	N	V	N	V

Že iz uvodnega dela lahko ugotovimo, da raziskovalno delo vsebuje raznolika znanstvena področja za katera je zelo pomemben interdisciplinarni pristop, zato v nadaljevanju predstavimo osnovna področja.

1.4.1 Informacijsko - komunikacijske ter identifikacijske tehnologije

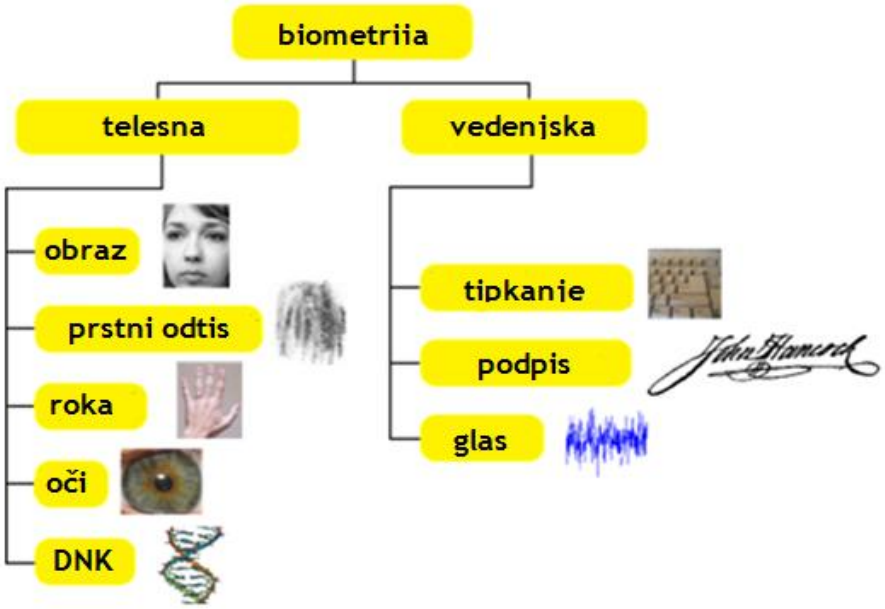
Računalništvo je tehniška znanstvena veda o delovanju in uporabi računalnikov ter vključuje strojno in programsko opremo (Denning, 2005). V praksi je računalništvo večkrat povezano z drugimi vedami, kot so analize algoritmov, programski jeziki, programska in strojna oprema itd. Informatika je veda o podatkih in informaciji, ki vključuje razlago, analizo, hranjenje in dostop do njih. Služi kot znanstvena podlaga analizi komunikacij in podatkovnih zbirk (Jereb in Šmitek, 2006). Elektronika (hardware) proučuje zgradbo in delovanje računalnikov in drugih digitalnih naprav. Informacijski sistemi v okviru računalništva nudijo podporo delovanju organizacije in vključujejo delovanje, nameščanje in vzdrževanje računalnikov, programja in podatkov. Kriptografija vključuje varovanje informacij in obravnava izvedbo varnosti informacijskih sistemov.

Biometrične metode so avtomatizirane metode prepoznave ljudi, temelječe na njihovih fizioloških ali/in vedenjskih značilnostih (Woodward, Orlans in Higgins, 2003b). Beseda »avtomatizirane« je nujna za definicijo, ker bi brez nje opisovali tudi celo množico zelo običajnih, toda bistveno manj zanesljivih identifikacijskih tehnik kot je npr. fotografija ali črnilni prstni odtis na identifikacijski znački itd. Biometrične metode so avtomatizirane do stopnje, kot je avtomatiziran proces zajema vzorca, vzorčenja, primerjave zajetega vzorca s poprej pridobljenim vzorcem in algoritemske primerjave, ki omogoči rezultat (Jain, Ross in Prabhakar, 2004). Različne fizične ali vedenjske karakteristike rangiramo glede na osnovne lastnosti, ki naj bi jih imela dobra biometrična lastnost:

- univerzalnost je značilnost določene osebe (se nujno razlikuje od vseh ostalih, je edinstvena),
- stalnost (karakteristika se s časom ne spreminja),
- zbirnost (karakteristika se zbira na uporabniku prijazen način).

Najbolj pogosto so telesne (fizične) karakteristike (biometrični vzorci) zajeti preko optičnega senzorja. V večini primerov so optični biometrični sistemi enostavni, saj vsebujejo izvor svetlobe, napravo za pozicioniranje biometrije

in kamero. Optični filtri absorbirajo svetlobo določenih valovnih dolžin in prepuščajo potrebno, da prehaja na vzorec. V primeru, ko gre za odčitavanje prstnih odtisov in mrežnice, je optika veliko bolj zahtevna, sistem šablon in algoritmov primerjave pa veliko bolj kompleksen. Sama tehnika temelji na zajemu biometričnih lastnosti, ki poteka preko čitalnika na osnovi primerjave značilnosti osebka, ki naj bi bil identificiran (Prabhakar et al., 2003). Biometrični sistemi (slika 1) so v bistvu primerjalniki vzorcev in se zelo razlikujejo glede na princip delovanja (ne glede na tip karakteristike, ki jo pregledujemo) (Biometric Evaluation Methodology Working Group [BEM WG], 2002). Prepoznava osebe temelji na primerjanju binarne kode neke fiziološke lastnosti, s tisto kodo, ki je v napravi že shranjena (Mraović, 2003). Najprej je potrebno zajeti žive podatke z osebe.



Slika 1: Osnovna delitev biometrije (BEM WG, 2002)

S pomočjo kompleksnih algoritmov sistem zajete podatke pretvori v binarno kodo, ki jo nato primerja s tisto v svojem spominu.

1.4.2 Zasebnost in njena pravna formulacija v boju proti terorizmu

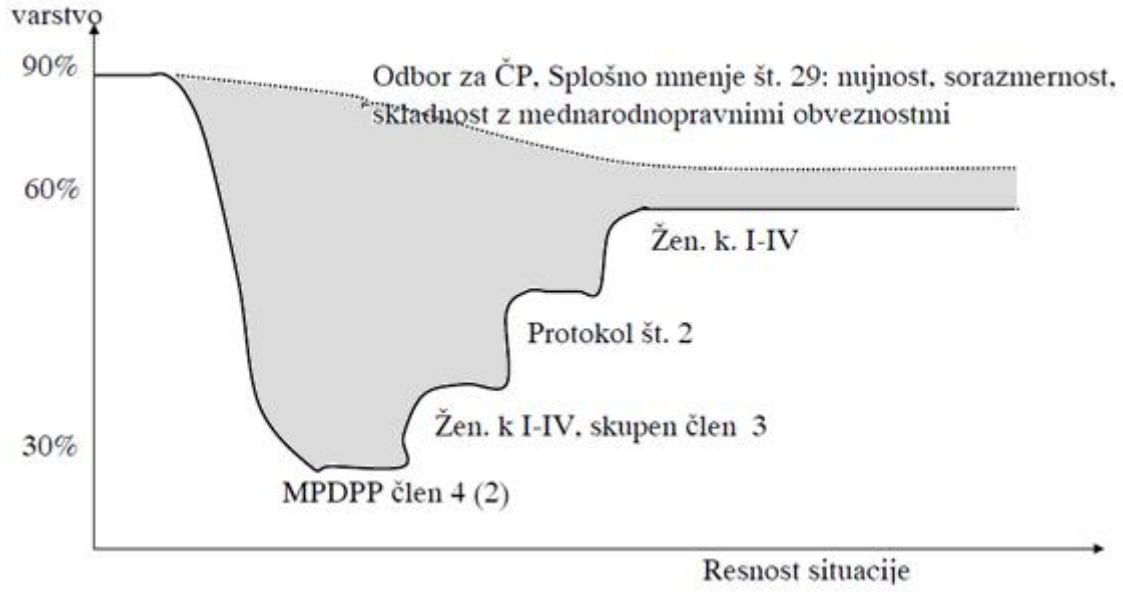
Vsak posameznik ne glede na narodnost, raso, barvo, veroizpoved, etnično pripadnost ima pravico do zasebnosti (ZVOP, 2007). Zasebnost, nadzorne

tehnologije ter soodvisnost obeh raziskujejo številni raziskovalci in strokovnjaki (Casella, 2003; Lyon, 2001; Sanders, 2005 idr.). Zaradi soodvisnosti je nujno interdisciplinarno in hkratno obravnavanje obeh vprašanj. Gre namreč za problematiko, ki ima družbene, pravne, filozofske razsežnosti in se močno dotika pravic posameznikov oziroma uporabnikov identifikacijske tehnologije. Poleg tega imamo opraviti s tehnologijo, ki se izjemno hitro razvija. Vsi ti razlogi narekujejo, poglobljeno interdisciplinarno raziskovanje tega področja, ki je še kako relevantno in aktualno.

Prstni odtis, očesna šarenica, mrežnica, obraz ipd. so biometrični podatki in kot taki nedvomno tudi osebni podatki, saj gre za značilnosti, ki so edinstvene in stalne za vsakega posameznika in na podlagi katerih je oseba določena oziroma vsaj določljiva. Zato se vsakršno zbiranje, shranjevanje, pošiljanje ali uničevanje teh podatkov šteje za obdelavo osebnih podatkov in posledično zanje veljajo določbe zakona, ki ureja varstvo osebnih podatkov (ZVOP, 2007). Kar nekajkrat je prišlo do sporov in precedenčnih sodb ameriških sodišč, ki so morala ugotavljati, kaj je in kaj ni poseg v zasebnost (Dvoršak, 2003).

Situacija glede človekovih pravic in svoboščin pa postane drugačna, ko gre za vprašanje vojne zoper terorizem. Najprej je že terorizem sam po sebi neposreden napad na pravice in svoboščine državljanov, demokracijo in načela pravne države. Po drugi strani pa se negativni učinki (mučenje, nečloveško in ponižujoče ravnanje s terorističnimi osumljenci, brez dostopa do neodvisnega in nepristranskega sodišča, telesni skenerji na letališčih itd.) protiterorističnih ukrepov, odražajo na državljanskih svoboščinah in njihovih temeljnih pravicah. Varstvo temeljnih človekovih pravic, v vojni zoper terorizem postane sekundarna tema in dostikrat zaidemo v sivo območje (Slika 2) med mednarodnim civilnim in vojaškim pravom (Černič-Letnar, 2011). Takšen primer je razveljavitev obveznosti po 4. členu mednarodnega pakta o državljanskih in političnih pravicah (MPDPP). Ta dovoljuje v primeru izjemne splošne nevarnosti, ki ogroža obstanek države (in je to objavljeno z uradnim aktom), da smejo države pogodbenice tega pakta ukreniti kaj, kar razveljavlja

njihove obveznosti iz tega pakta, vendar strogo v obsegu, ki ga tako stanje zahteva; pogoj pa je, da taki ukrepi niso neskladni z drugimi obveznostmi, ki jim jih nalaga mednarodno pravo in da nimajo za posledico diskriminacijo, ki bi temeljila na rasi, barvi, spolu, jeziku, veri ali socialnem poreklu. Vprašanje vojnih žrtev urejajo tudi ženevske konvencije, ki so mednarodni dogovor o varstvu vojnih žrtev.



Slika 2: Siva cona varstva človekovih pravic v vojni proti terorizmu (Černič-Letnar, 2011)

Prav tako različne države zakonodajo v takšnih primerih različno interpretirajo in že podatek najdaljšega dovoljenega pridržanja (npr. v Sloveniji 48 ur, v Angliji 48 dni), kadar gre za utemeljen sum terorizma pove, kako različno je terorizem obravnavan v različnih državah. Strukturo človekovih pravic, ki se jih najpogosteje omejuje v boju zoper terorizem, lahko ponazorimo s piramidalno obliko (slika 3). Iz slike je razvidno, da se od vseh elementarnih človekovih pravic, nekako najlažje odpovemo »pravici do zasebnosti«. Težje se odpovemo »svobodi izražanja« in najtežje dejavniku »prepovedi mučenja«.

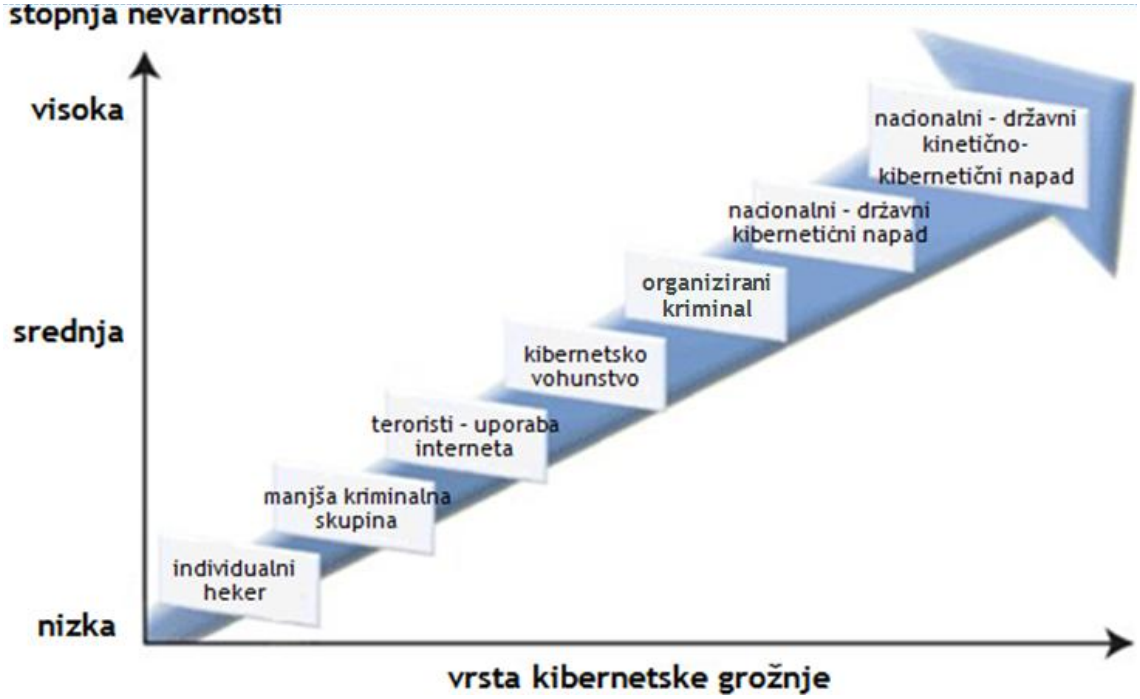
Slika 3: Piramidalna oblika človekovih pravic (Černič-Letnar, 2011)

Boj zoper terorizem in varstvo človekovih pravic nista medsebojno izključujoča cilja, temveč se dopolnjujeta. Protiteroristični ukrepi morajo zato temeljiti na spoštovanju človekovih pravic. V vojnem času se morajo ljudje držati pravil, celo v odnosu do sovražnika.

1.4.3 Kibernetski kriminal in kibernetski terorizem

Terorizem je namenska uporaba ali grožnja uporabe sile proti civilistom in civilnim ciljem z namenom, da se dosežejo kakšni politični cilji (Prezelj, 2006). Ta definicija vsebuje dva elementa: namen oziroma cilj ter kako cilj doseči, to se pravi strategijo. Namen teroristične aktivnosti ima torej vedno politično ozadje, če ne, gre za običajno obliko kriminalitete ali duševno neravnovesje akterja (Fossati, 2005). Prav tako ne more biti verski ali ideološki. Teroristične skupine (npr. Euzkadi Ta Askatasuna - ETA ali Kurdistan Workers' Party - PKK) večkrat izvedejo tudi kako kriminalno dejanje, ki s političnimi cilji ni neposredno povezano, pri tem gre večinoma za nabavo sredstev za financiranje dejavnosti. Izraz »političen« je dovolj širok in ne vključuje motivov političnih ciljev. Tarče terorističnih napadov so civilisti ali civilni objekti, ne pa državni organi kot sta policija in vojska.

Kibernetski kriminal in kibernetski terorizem nista popolni sopomenki. Napad v kibernetskem prostoru mora imeti teroristično (politično) komponento, da ga lahko označimo za kibernetski terorizem, čeprav je za izvedbo napada lahko uporabljeno povsem isto kibernetsko orodje. To predstavlja soodvisnost kibernetskega kriminala in terorizma (Bucci, 2009). Verjetnost kibernetskega terorizma se vsak dan povečuje, kot se povečuje število internetnih priključkov in drugih računalniških sistemov, ki jih za svoje napade uporabljajo teroristi na različne načine in stopnje nevarnosti (slika 4).



Slika 4: Spekter kibernetskih groženj (prirejeno po Bucci, 2009)

Kibernetski terorizem je mogoče opredeliti kot orožje ali kot cilj politično motivirane mednarodne ali sub-nacionalne skupine, da z uporabo računalnika, za ogroža ali povzroči nasilje in strah, da bi vplivali na občinstvo, ali povzroči, da neka vlada spremeniti svojo politiko. Ta definicija, združuje več mnenj o kibernetskemu terorizmu in zajema tri načine delovanja: fizični (kinetični), elektronski in informacijski, za napade na računalnike (CRS, 2005).

Identificiramo lahko naslednje dejavnike klasičnega mednarodnega terorizma (Miholič, 2004):

a. Človeški dejavnik, kjer sta opazna predvsem dva trenda in sicer nabor aktivistov iz vrst mladih, ki praktično slepo sledijo ideji terorizma in omogočajo tajno delovanje skupine, ter rekrutacija na osnovi osebnih in sorodstvenih poznanstev, kar omogoča preverjanje posameznikove preteklosti in vzgibov za članstvo v teroristični organizaciji.
b. Finančni dejavnik, je pomemben za mednarodne teroristične združbe, ki uporabljajo različne metode, ki so odvisne od velikosti organizacije, velikosti območja delovanja in metod delovanja. Najpogostejši načini financiranja so: državna podpora, zakonito poslovanje, donacije posameznikov in financiranje preko dobrodelnih dejavnosti ter kriminalna dejavnost (droga, orožje itd.).
c. Materialni dejavnik, zaseda osrednje mesto v organizaciji tradicionalnih in sodobnih terorističnih skupin in zajema konvencionalno orožje, predvsem lahko pehotno orožje in eksplozivna sredstva, ki jih teroristične skupine pridobivajo preko nelegalnih in legalnih poti oziroma celo same vzpostavijo proizvodnjo določenih vrst orožja.
d. Komunikacijski dejavnik je postal zelo efektiven s prelomnico v načinu komuniciranja med terorističnimi skupinami in javnostjo ob uveljavitvi medmrežja, saj se je s tem zelo poenostavilo objavljanje velikega števila informacij; prav tako je dostop do medmrežja praktično globalen in nevarnost odkritja s strani državnih varnostnih organov je veliko manjše.
e. Ideološki dejavnik se v praksi razlikuje od skupine do skupine, vendar je mogoče poiskati nekatere skupne smernice, ki razvrščajo teroristične skupine v tri poglavitne motivacijske skupine in sicer racionalno, psihološko, versko in kulturno.

2 TERORIZEM IN NJEGOVE SODOBNE POJAVNE OBLIKE

Vse hitrejša širitev brezžičnih komunikacijskih sistemov zelo povečuje možnosti zlorab. V tem primeru namreč tradicionalni obrambni pristop (securing the perimer) ni učinkovit, saj nimamo fizičnega nadzora nad uporabniki in napravami. Vedno večja je tudi prepletenost in dostopnost na računalniku temelječih sistemih, ki postajajo kritični oz. ključnega pomena za ekonomijo, logistiko, razširjanje dobrin in storitev (CRS, 2008). Globalnost IKT povečuje število uporabnikov v domačem in mednarodnem prostoru ter tako omogoča teroristom intenzivnejše delovanje v vseh vrstah terorizma.

2.1 *Vrste terorizma*

Obstaja več vrst terorizma in med nekaterimi so meje nejasne ali celo zabrisane. To pomeni, da lahko neka teroristična skupina izvaja več različnih vrst terorizma. Na splošno lahko rečemo, da lahko teroristična dejanja potekajo na dveh ravneh: državni in nedržavni. Terorizem lahko v tem smislu razdelimo širše na dve obliki: državni (vladni) terorizem in nedržavni (nevladni) terorizem. Kot pove že besedna zveza »državni terorizem«, je glavni protagonist terorističnih dejanj v tem primeru, država oziroma nosilci državne oblasti, ki nad prebivalstvom izvajajo množične kršitve človekovih pravic in temeljnih svoboščin s ciljem, ohraniti se na oblasti. Kršitve pravic se lahko dogajajo v stanju miru ali v oboroženih spopadih in so usmerjene v lastno ali tuje prebivalstvo. Pojem »nedržavnega terorizma« označuje terorizem posameznikov ali skupin, ki izvajajo teroristična dejanja, pogojena z različnimi motivi, v določeni družbi (Korošec, 2002).

2.1.1 Ideološki terorizem

Levičarski teroristi se bojujejo proti kapitalističnemu sistemu. Teroristične skupine te vrste izhajajo iz stališča, da je ljudstvo zatirano in ga je treba osvoboditi, tarče so zato mnogokrat kapitalisti, predstavniki »buržoaznih« medijev ipd. Levičarske teroristične skupine so npr.: Rdeča brigada, Rdeča armada itd.

Desničarske teroristične organizacije izhajajo iz skrajno desnih (fašističnih, neonacističnih) ideologij. V dvajsetih in tridesetih letih so bile močne tudi skrajno katoliške (klerofašistične) skupine, ki so z nasiljem obračunavale z nasprotniki. V šestdesetih letih je bila v Franciji dejavna Action dirècte. Danes se v desničarske skupine štejejo tudi »obritoglavci« ali ekstremni nacionalisti in rasisti, ki si prizadevajo za odpravo liberalnih režimov v zahodni Evropi ter vzpostavitev fašističnih držav na »svoji« zemlji. Teroristične desničarske skupine delujejo običajno v »zaščito« desnih vrednot in za obrambo pred nevarnostjo komunizma in liberalizma, mnogokrat se povezujejo znotraj državnih institucij, zlasti tajnih služb (npr. v Italiji organizacija Gladio), z raznimi akcijami, tudi umori in atentati nastopajo proti levici in skušajo preprečiti, da bi prišla na oblast. V preteklosti so bile tudi proti osamosvojitvi kolonij (npr. Organisation Armée Secrète - OAS v Franciji), ki je nastala 1961 da bi s terorističnimi akcijami, tudi atentatom na De Gaulla preprečila pogajanja med alžirsko osvobodilno organizacijo in francosko vlado in osamosvojitev Alžirije).

2.1.2 Nacionalistični terorizem

Nacionalistični (separatistični) terorizem je delovanje nekaterih ekstremnih skupin, ki stremijo k formiranju samostojne države ali boj za pravice naroda (etnične skupnosti), tudi protikolonialni boj. Takšen tip terorizma je bil med najbolj uspešnimi. Po nekaterih ocenah, nacionalistične teroristične organizacije praviloma ne pretiravajo z nasilnimi dejanji. K tem se zatekajo do mere, da postanejo vidni in prepoznavni v svetu, ne gredo pa daleč čez to mejo, saj bi na ta način izgubili mednarodno ali lokalno razumevanje za njihov problem. Nacionalistične teroristične organizacije so npr.: Irish Republican Army (IRA), Euskadi ta Askatasuna (ETA) itd. (Center for Defense Information [CDI], 2007).

2.1.3 Verski terorizem

Terorizem verske narave navadno izvaja nasilje zaradi svojih preroško vodenih nagibov. Verske teroristične organizacije so npr.: Al-Kajda[6], Hamas, Hezbolah, Islamski džihad, Osvobodilni tigri Elama itd. (Tičar, 2010).

2.1.4 Anarhistični terorizem

Gre za obliko, ki napada na prvem mestu oblastniške tarče: vrhnje politične osebnosti, njihove mehanizme in imetje ter državne ustanove in sploh obstoječi sistem države. Anarhisti so med drugim tako eliminirali ameriškega predsednika McKinleya (Tičar, 2010).

2.1.5 Državni terorizem

Državni terorizem je oblika organiziranja terorističnih skupin s podporo radikalnih držav. Prav tako država lahko podpira oziroma izvaja notranjepolitični terorizem proti svojim, navadno političnim nasprotnikom ali etnijam (Tičar, 2010).

2.2 *Oblike terorizma*

V razpravah pogosto primerjamo teroristične napade in možne nevarnosti, ki jih prinašajo sredstva za množično uničevanje ljudi. Govori se predvsem o jedrskem, kemičnem in biološkem orožju. Ni dvoma, da je jedrsko orožje najbolj uničevalno in da ima tudi najhujše posledice, vendar je potrebno ob razvoju informacijskih orodij upoštevati, da so ravno ta lahko sredstvo s katerim se prožijo druge oblike napadov.

2.2.1 Asimetrični kibernetski terorizem

Dogodki v zadnjem času so pokazali, da lahko hekerji, ki delujejo samostojno ali kot majhne skupine, povzročajo veliko gospodarsko ali politično škodo. največjim družbam in državam (Walsh, 2010). Ti kibernetični napadi so

---

[6] Al-Kajda (arabsko: القاعدة al-qāʕida); je mednarodna Islamska teroristična organizacija ustanovljena leta 1988. Ustanovitelji so Azzam (kasneje preimenovan v Usama Bin Laden) in ostali veterani »Afghan Arabs« Sovjetsko - Afghanistanske vojne »Soviet-Afghan War« (Atwan, 2006).

namenjeni za glasno odmevne škodljive operacije, v nasprotju s tiho krajo intelektualne lastnine ali krajo identitete. Napadi so skupaj s politično agendo ali ideologijo tako pripravili temelje za nov tip vojne, v kateri en heker lahko uveljavlja ogromno moč nad tistimi, ki so odvisni od informacijske tehnologije. Napadalci prihajajo iz vsega sveta, končni rezultat pa je enak; škoda blagovne znamke, izgube zaradi izpadov, skupaj s taktiko strahu, ustrahovanja, grožnje in zahteve, kot tudi propaganda (Olman, 2010). Cilji niso samo korporacije in vlade, ampak tudi posamezniki. Kibernetični zločinci opuščajo množično neželeno pošto in prehajajo na usmerjene napade (CISCO, 2011). Tradicionalne metode za informacijsko varnost, v teh primerih niso dovolj za reševanje »Crimeware[7]« napadov (Emigh, 2006), še manj pa za novo obliko terorističnega napada z napredno trajno grožnjo (Advanced Persistent Threats - APT), ki je usmerjena na poslovne in političnih cilje.

2.2.2 Atentati

Uvodoma je potrebno pojasniti, da obstaja več različnih delitev za atentate. Atentate lahko delimo glede na namen (zamenjava ljudi, povzročanja sprememb, utišanja nasprotnikov, propagande del ter zadovoljevanja patoloških potreb (Crotty in drugi, 1970). Cassidy (1977) loči med atentatom kot odrazom šibkosti in atentatom zaradi osebnih oziroma skupinskih koristi.

2.2.3 Biološki terorizem

Posebnost bioterorizma je, da z nasiljem poskuša doseči verske, politične, ekološke ali ideološke cilje ne glede na moralno in politično pravičnost namena. V 90. letih se je število bioloških napadov nenadoma silno povečalo. K sreči je šlo večinoma za potegavščine in slabe šale. Uporabili ali vsaj grozili pa so tudi z mikroorganizmi. Zaskrbljuje vedno več podatkov o biološkem orožju na medmrežju in drugod, ki so dostopni javnosti. V zadnjem času se je povečalo zanimanje za nevarne mikroorganizme, s katerimi bi lahko povzročili

[7] »Crimeware« je zlonamerna programska oprema, ki se tajno namesti na računalnik. Večina teh progamov so trojanci, ki so namenjeni različnim napadom (Anti Phishing Work Group [APWG], 2011).

množična obolenja in umiranja (Podbregar in Ivanuša, 2009). Nerazrešen je še vedno »antraks« v ZDA v l. 2001 in l. 2002 (Likar, 2005).

2.2.4 Jedrski terorizem

Jedrski terorizem se nanaša na več različnih načinov uporabe jedrskih snovi, ki se lahko izkoriščajo kot teroristična taktika. Vključuje napad na jedrski objekt, nakup jedrskega orožja, gradnjo jedrskega orožja ali druge možne načine za razpršitev radioaktivnih snovi (Glaser in Hippel, 2006).

2.2.5 Samomorilski napadi

Samomorilski teroristični napad predstavlja asimetrični pristop vojskovanja, v katerem napadalec nima namena preživeti. Tako samomorilec lahko izvede ukrepe, ki jih ostali, zaradi želje po preživetju, ne morejo (Nedog, 2002). Samomorilski bombni napad je podzvrst samomorilskih terorističnih napadov, izveden s pomočjo aktiviranja eksploziva, ki ga izvajalec nosi na sebi ali pa je eksploziv nameščen v avtu (Weinberg, Pedahzur in Perliger, 2003)

3 BOJ PROTI TERORIZMU IN NJEGOVIM SODOBNIM POJAVNIM OBLIKAM V LUČI PRAVICE DO ZASEBNOSTI

Internet je idealno orodje za tiste, ki radi kršijo določila o spoštovanju zasebnosti, zato se z razlogom pojavi vprašanje, kako se proti temu bojevati oziroma kako učinkovito zagotoviti nadzor tistih, ki nas nadzorujejo. S pojavom interneta je postal pretok informacij hitrejši, večji in tudi lažji. Po drugi strani pa je tudi bistveno več nadzora. Je internet zmanjšal osnovne človekove pravice? V kolikor govorimo o pravici do zasebnosti, je treba vedeti, da zasebnost ni neka absolutna pravica (Kovačič, 2006). V primeru kriminalne dejavnosti ali pri vprašanju varnosti so posegi v zasebnost lahko upravičeni. Bistveno pa je, da so posegi zakoniti. Problem pri elektronskih tehnologijah je v tem, da totalitarni režimi včasih niso imeli tehnologije, da bi na tako lahek način spremljali komunikacije, saj ljudje niso uporabljali interneta ali mobilnih telefonov. Dosjeji v papirnati obliki so sicer obstajali, a iskanje po njih je bilo zelo zamudno. Baze podatkov, danes omogočajo preprosto povezovanje in iskanje podatkov. Največja težava posega v zasebnost je, da je nadzor postal preobsežen. Smo uporabniki tehnologij, ki se dajo lahko nadzorovati in temu se težko izognemo. Z mobilnimi telefoni se beležijo tako podatki o lokaciji uporabnika kot klicih. Lahko ga sicer nehamo uporabljati, vendar bi se težko znašli brez njega. Če se hočemo izogniti videonadzoru, ne smemo v nakupovalne centre, letališča ali v večja mestna središča. Lahko nehamo uporabljati plačilne kartice, toda potem moramo neprestano hoditi v banko. Skratka, težko se izognemo temu, da ne bi bili zabeleženi v kakšni bazi. V kolikor nismo registrirani v nobeni bazi podatkov, praktično nimamo nobenih pravic. Problem je namreč v tem, da so danes zdravstvene, socialne, državljanske in druge pravice vezane na neko obliko nadzora.

Ali obstaja učinkovit način, kako se izogniti najrazličnejšim vrstam nadzora? Nadzoru se je v popolnosti nemogoče izogniti. Na internetu nam slovenska akademski raziskovalni inštitut (Academic and Research Network of Slovenia [ARNES], 2008) podaja splošna navodila, kako zavarovati internetne komunikacije in računalnik pred nepooblaščenim dostopanjem. Težko pa se izognemo beleženju podatkov, o obiskanih spletnih straneh ali o uporabljenih

iskalnikih, katere lahko v analizah uporabijo kriminalisti ali službe državne varnosti, v kolikor imajo za to odredbo. V ta namen bi sicer lahko uporabili sisteme za anonimizacijo, npr. omrežje Tor[8] (Electronic Frontier Foundation [EFF], 2011), Anonym.OS (Kaos.theory, 2006) itd., od katerih pa so nekatere še v razvojni fazi. Sistem Tor zmanjša možnost, da bi vas našli, saj preusmeri promet prek večjega števila naključno izbranih strežnikov v omrežju, kar metodo analize prometa močno oteži, če ne celo prepreči. So pa tisti, ki uporabljajo takšne napredne zaščitne sisteme, lahko označeni za sumljive s strani nadzora. Razlog za izogibanje nadzoru, se večkrat išče v kakšnem kriminalnem naklepu. Res lahko anonimizacijo in šifriranje uporabljajo tudi kriminalci, vendar je to podobno kot z rokavicami. Lahko jih uporabimo za preprečevanje okužb in poškodb, lahko pa jih uporabijo tudi vlomilci, da ne pustijo prstnih odtisov (Kovačič, 2007).

3.1 *Strategije in dejavniki v boju proti terorizmu*

V sistemske pristope k bojevanju proti terorizmu moramo upoštevati naslednje strategije (Čaleta, 2011):

- politične strategije,
- psihološke strategije,
- socialno-ekonomske strategije,
- medijske strategije,
- vojaške strategije,
- policijske strategije,
- strategije uporabe varnostnih in obveščevalnih služb,
- pravne strategije,
- izobraževalne strategije in
- strategije celovitega pristopa.

[8] Tor je sistem (projekt), ki nastaja pod pokroviteljstvom organizacije Electronic Frontier Foundation (EFF). Trenutno gre za razvojno različico zbirke orodij, ki omogočajo anonimno brskanje po spletnih straneh, objavljanje vsebin, anonimno uporabo programov za neposredno sporočanje (IM, IRC, SSH itd.), ki slonijo na TCP (Transmision Control Protocol) protokolu za nadzor prenosa (Kodelja in Banovič, 2008).

3.2 *Ukrepi ZDA in Velike Britanije v boju proti terorizmu*

Terorističnim napadom v New Yourku, so ZDA pri uvajanju vseh mogočih protiterorističnih ukrepov, sledile Veliki Britaniji. V Veliki Britaniji je konec februarja l.2001 začel veljati protiteroristični zakon »Terrorism Act 2000«, v katerem je zapisano, da bodo vse osebe, ki ogrožajo življenja drugih z manipulacijo javnih računalniških sistemov, kaznovane po protiterorističnem zakonu, tako kot vsak drug terorist. V duhu najsvobodnejše države na svetu, je takšna radikalna obravnava bila precedens celo za ZDA. Boj proti vdiralcem v računalniške sisteme, pa se bo še radikaliziral. Tako sodobnim hekerjem[9] ali krekerjem[10] sedaj še ne grozi električni stol, jih pa lahko doleti dosmrtna ječa. Takšni ukrepi se zdijo zagovornikom svoboščin nesprejemljivi, saj se lahko hekerji, ki so bili do sedaj kaznovani predvsem z opozorili ali razmeroma nizkimi kaznimi, dokaj hitro znajdejo za zapahi, celo za desetletje. Resnost namere ZDA v boju proti kibernetskemu terorizmu, priča odločitev o sprejetju ukrepov, ki bi vsem, ki so bili kadarkoli obsojeni zaradi takšnih kršitev, vzeli vzorec DNK, enako kot na primer morilcem, pedofilom in posiljevalcem. Velika Britanija in ZDA sta v svojih zakonodajah sprejela ukrepe za nadzor vseh spletnih aktivnosti, kjer lahko organi za nadzor pregledajo katerekoli elektronsko vsebino. Američanom, ki jim do izvedenih terorističnih napadov ni bilo treba imeti niti osebne izkaznice to pomeni grob poseg v zasebnost. Hkrati pa imajo takšni restriktivni ukrepi tudi druge učinke, ki se kažejo predvsem v gospodarskem nadzoru, nad tehnološko manj razvitimi. Za Veliko Britanijo in ZDA, je vojno kibernetskemu terorizmu napovedal še Svet Evrope[11]. Sporazum je podlaga zakonskim ukrepom, katere naj bi sprejele vse podpisnice članice EU, hkrati pa bo začrtal napotke pri preganjanju računalniškega kriminala in kibernetskega terorizma.

---

[9] Heker; pravi hekerji so ljudje z veliko znanja, ki iščejo luknje, vendar ne za svojo korist (Raymond, 2001).

[10] Kreker; slabi hekerji to počnejo da delajo škodo in se imenujejo krekerji (Ang.: Crackers) (Raymond, 2001).

[11] Svet Evrope je bil ustanovljen 5. maja 1949 s podpisom Londonske pogodbe (Belgija, Danska, Francija, Irska, Italija Luksemburg, Nizozemska, Norveška, Švedska in Anglija) (Arah, 1995).

Skrb glede kibernetskega terorizma narašča vedno bolj, še posebej v tistih vladnih ustanovah, ki se ukvarjajo z nacionalno varnostjo, kar dokazujejo številne konference, poročila in študije, ki se objavljajo vsak dan.

3.3 *EU konvencija o kibernetskemu kriminalu*

Konvencija o kriminalu v kibernetskem (Komisija evropskih skupnosti, 2007) je pravni akt, katerega namen je definirati, kaj je računalniška kriminaliteta, ter postavlja temelje mednarodnemu sodelovanju, v boju proti kibernetskemu kriminalu. Na konferenci l. 2001 v Budimpešti so ZDA in 29 evropskih držav podpisale sporazum, ki je bil osnova za preganjanje računalniškega kriminala, kazniva dejanja prevare na internetu, otroško pornografijo, hkrati pa bo začrtal napotke policistom pri preganjanju računalniškega kriminala (Council of Europe, 2003). Konvencija celovito obravnava kazenskopravno problematiko v kibernetskem prostoru, ki se je v preteklih letih, zaradi posameznih temeljnih značilnosti modernih informacijsko komunikacijskih tehnologij, še posebej pa interneta, razvila v povsem specifično vejo kazenskega prava.

Namen je postaviti internetno poslovanje pod enotno jurisdikcijo, ki vsebuje akte, s katerimi naj bi ponudnike internetnih storitev pravno vključili v boj proti kriminalu. Ustrezna zakonodaja in sodelovanje pristojnih organov, pa še nista dovolj za uspešno zatiranje računalniške kriminalitete. Vsi uporabniki interneta smo potencialne žrtve, zato bomo tudi mi morali prispevati svoj del v zatiranju te vrste kriminala. Kibernetski kriminal vsekakor obstaja in predstavlja resen problem saj se internet kot omrežje širi. Tudi kriminaliteti ponuja vedno nove storitve in možnosti, tako organi pregona in zakonodaja temu zelo težko sledita. Konkretnih rešitev omenjene problematike konvencija sicer ne določa, daje pa državam podpisnicam dovolj natančne smernice, glede bodoče ureditve na področju kriminala v kibernetskem prostoru. Z vidika pregona kaznivih dejanj v kibernetskem prostoru, je nujno potrebno zagotoviti ustrezne instrumente za hitro in učinkovito mednarodno sodelovanje, ki so zaradi geografske nedoločnosti interneta, ključnega pomena.

3.4 *Ukrepi Slovenije v boju proti terorizmu*

Slovenija aktivno sodeluje, podpira in se pridružuje pobudam in ukrepom v boju proti terorizmu v mednarodnih forumih. S pridružitvijo in izvajanjem ukrepov, sprejetih v okviru organizacije združenih narodov (OZN), EU, severnoatlantske pogodbene zveze (North Atlantic Treaty Organization – NATO), evropske organizacije za varnost in sodelovanje (OVSE), se Slovenija nedvoumno in trdno postavlja v protiteroristični tabor. Med dokumenti je potrebno izpostaviti resolucijo varnostnega sveta OZN 1373 (2001), ki je globalna strategija OZN in EU za boj proti terorizmu. Slovenija je pogodbenica univerzalnih konvencij in protokolov ZN na področju boja proti terorizmu in je l. 2005 med prvimi podpisala zadnjo, trinajsto konvencijo o zatiranju dejanj jedrskega terorizma. Ratifikacija konvencije je bila izvedena v l. 2008, saj je bilo potrebno spremeniti ustrezne člene Kazenskega zakonika (Ministrstvo za zunanje zadeve [MZZ], 2011).

Republika Slovenija je 24.7.2002 pristopila h konvenciji o kibernetski kriminaliteti. Določiti meje, kaj natanko je računalniški kriminal in kibernetski terorizem, ni enostavno. Po eni definiciji so računalniška kriminaliteta tista kazniva dejanja, kjer je računalnik sredstvo in predmet storitve. Če so sredstvo storitve, potem govorimo o vdorih, izdelavi pripomočkov, pa tudi računalniškem piratstvu. Kjer pa je računalnik predmet storitve, je kaznivih dejanj precej več - sem sodijo tudi skeniranje bankovcev in različna ponarejanja. Pristojnostim računalniških kriminalistov, se vsako leto pridruži kakšna nova oblika kaznivega dejanja, saj klasična kazniva dejanja prehajajo v virtualni svet.

V Sloveniji se očitno kaže pomanjkanje usposobljenega kadra, ki se bo spoznal na kopico omrežnih in IKT sistemov. Vrhunskih strokovnjakov za omrežja, kodiranja in podobno, ki bi delali za policijsko plačo, ni lahko dobiti (Kebe, 2002). Prav tako kazni v Sloveniji za zdaj še niso tako stroge kot v ZDA, saj kazenski zakonik predvideva do pet let kazni za vdore v računalniške sisteme, pri katerih je povzročena velika materialna škoda. Za kaznivo dejanje pa velja že, če imate v posesti pripomočke za računalniške vdore, pa tudi viruse. Te

dni je vlada v obravnavanje dobila predlog kazenskega zakonika (KZ-1, 2008), ki so ga pripravili na Ministrstvu za pravosodje.

Med drugimi je v KZ-1 naveden tudi 221. člen, ki obravnava napad na informacijski sistem. V predlogu, ki ga bo obravnavala vlada je dodan 5. odstavek, ki se glasi: Kdor poseduje, izdeluje, daje v uporabo, uvaža, izvaža ali drugače zagotavlja pripomočke za vdor v informacijski sistem, se kaznuje z denarno kaznijo ali z zaporom do šestih mesecev. Člen je zelo podoben obstoječemu kazenskemu zakoniku (306. člen) in vsebuje podobno določbo (izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje). Obstoječi zakon, je posedovanje, dajanje v uporabo, itd. pripomočkov za vdor v informacijski sistem kriminaliziral le, kadar je to storjeno z namenom izvršitve kaznivega dejanja. Novi predlog zakona to »malenkost« izpušča in prepoveduje posedovanje (izdelovanje, pridobivanje) pripomočkov za vdor v informacijski sistem brez dodatnih pogojev. Najbolj očiten pripomoček, v praksi so seveda različna varnostna orodja (Network Mapper [NMAP], 2010), namenjena varnostnemu testiranju in s tem posredno povečevanju varnosti. Ne glede na to, je ta orodja mogoče tudi zlorabiti in bodo zato seveda prepovedana. Nekatere napade je mogoče izvesti že z navadnim spletnim brskalnikom, recimo SQL (Standard Query Language) vrivanje (SQL injection) ali trajni napad s križnimi skripti (persistent Cross Site Scripting - XSS). Torej so po interpretaciji novega zakona tudi spletni brskalniki pripomočki za vdor in je zato potrebno osebe, ki jih posedujejo kaznovati. V končni fazi je nesporen pripomoček za vdor v informacijski sistem gotovo kar sam računalnik. V informacijske sisteme namreč, brez računalnika lahko le s težavo vdiramo (morda z mobilnim telefonom?). Vprašanje, ki si ga lahko ob vsem tem zastavimo je: »Kaj ta zakon lahko pomeni v praksi oziroma, kaj pripomoček za vdor v informacijski sistem, natančno je?«.

3.5 *Strategija EU za boj proti kibernetskemu kriminalu*

Resolucija EU za boj proti računalniškemu kriminalu (SEC, 2010) obsega dejavnosti, ki spadajo pod strateško zavezo in sicer:

1. Definiranje uporabljenih izrazov: računalniški sistem, računalniški podatki, ponudnik storitev (Internet Service Provider - ISP), podatki o prometu itd.
2. Kazensko pravo:

   Materialni del: klasificira in definira vrste kaznivih dejanj na štiri sklope: kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov (protipravni dostop do računalniškega sistema, protipravno prestrezanje in motenje podatkov in sistemov ter zloraba naprav), kazniva dejanja povezana s samim računalnikom (računalniško ponarejanje in računalniška goljufija), kazniva dejanja, povezana z vsebino (otroška pornografija), kazniva dejanja povezana s kršitvijo avtorskih in sorodnih pravic.

   Procesni del: splošne določbe, ki zavezujejo države podpisnice k določitvi pristojnih organov in postopkov, določbe, ki opredeljujejo hitro zavarovanje in razkrivanje shranjenih računalniških podatkov, določbe, ki se nanašajo na odrejanje priprave, preiskovanje in zasega shranjenih podatkov, določbe, ki opredeljujejo prestrezanje podatkov v realnem času, določbe, ki opredeljujejo smernice za določitev sodne pristojnosti.
3. Mednarodno sodelovanje: splošna načela mednarodnega sodelovanja, vsebuje načela izročitve storilcev, opredeljuje načela medsebojne pomoči, določbe, ki se nanašajo na neprestano delovanje omrežja.
4. Končne določbe.

Konvencija o računalniški kriminaliteti poskuša rešiti pravne dileme nadzora nad internetom. Je redek primer mednarodnega pravnega akta, ki je bil sprejet v tako kratkem času po zaključku ekspertnega dela ter bil tako široko podprt in je istočasno postal predmet diskusij. Očitajo se mu predvsem preširoka pooblastila organov pregona in odredba kjer bi ISP-ji končno dobili pravno obvezujoče odgovornosti (hranjenje podatkov, poročanje o ilegalnih aktivnostih, obvezno sodelovanje z organi pregona itd.).

3.6 *Zbiranje in uporaba osebnih podatkov v sodnih postopkih*

Zbiranje osebnih podatkov je velik posel, saj so podatki o potrošnikih za podjetja zelo dragoceni. V zameno za osebne podatke podjetja ponujajo številne ugodnosti, a pridobljeni podatki so za njih vredni bistveno več (Kovačič, 2007).

Ameriška in evropska zakonodaja se na tem področju precej razlikujeta. V Evropi je to dobro regulirano, saj je pri zbiranju in obdelavi osebnih podatkov treba spoštovati določena pravila. V praksi se vse kršitve seveda ne dajo odkriti, toda evropske države imajo posebne organe, ki se s tem področjem profesionalno ukvarjajo, zato je to vsaj minimalno urejeno. V ZDA pa so razmere precej drugačne, saj imajo posamezniki v zvezi z osebnimi podatki bistveno manj pravic kot v Evropi, zaradi nižje stopnje regulacije pa prihaja do številnih zlorab.

V Sloveniji je bilo sicer do sprejema EU direktive o hrambi prometnih podatkov, na podlagi katere je bil l. 2006 spremenjen Zakon o elektronskih komunikacijah, prepovedano hraniti prometne podatke. Kar nekaj podatkov pa kaže na to, da so se ti podatki vseeno hranili in so bili celo uporabljeni v sodnih postopkih. Ljudje pa so bili na podlagi zbranih podatkov tudi obsojeni. Nekateri ponudniki dostopa do interneta imajo tudi več let shranjene prometne podatke. Starega zakona o elektronskih komunikacijah, ki je hrambo teh podatkov prepovedoval, številni operaterji niso spoštovali, nezakonito zbrani podatki pa so se celo uporabljali kot dokazno gradivo na sodiščih. Šele po sprejemu evropske direktive se je začelo razmišljati o tem, da je bilo zbiranje prometnih podatkov nezakonito.

Problem je v tem, da številni odvetniki zelo dobro poznajo kazensko zakonodajo, ostalo pa verjetno malce manj. Tu gre za zelo specifične zadeve, pri katerih je potrebno tudi poznavanje tehnologije, ki je pravniki verjetno ne poznajo dovolj. Zato je nujnost organov, kot je informacijski pooblaščenec,

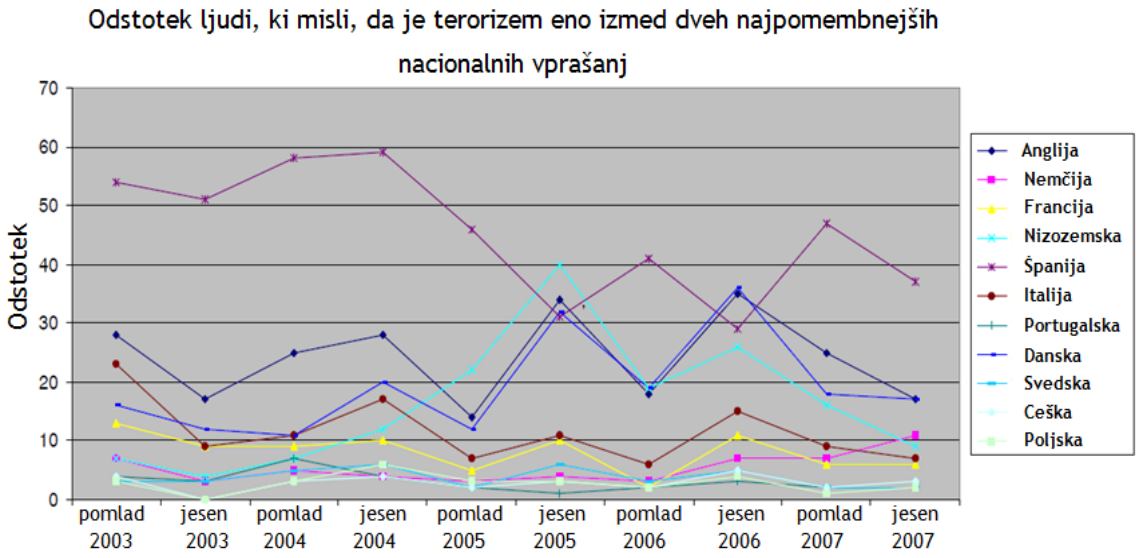
da združujejo strokovnjake s področja prava in informacijsko komunikacijske tehnologije.

3.7 *Percepcija terorizma*

Prejšnja poglavja kažejo, na resnost problematike terorizma in kibernetskega terorizma kot svetovnega pojava. Terorizem večkrat zaseda glavno mesto mednarodnih vladnih konferenc, posvetov in je tako ena izmed najpomembnejših tem tako EU kot ameriškega političnega prostora.

3.7.1 Percepcija terorizma v EU

Dojemanje oz. percepcija državljanov, do nekega pojava je včasih lahko povsem različno, od obravnave tega istega pojava skozi oči neke vladne organizacije ali kar, vlade. Da bi ugotovili percepcijo do terorizma, je nizozemski inštitut za varnost in krizni management (Institute for Safety Security and Crisis Management - COT), opravil raziskavo med državljani EU in analiziral, zaznavanje javnosti v povezavi z grožnjo terorizma. Za to obsežno javnomnenjsko raziskavo, je bil uporabljen tudi eurobarometer, ki se opravi s strani EU dvakrat letno (spomladi in jeseni). Graf na sliki 5, prikazuje odstotek ljudi nekaterih evropskih držav, ki mislijo, da je terorizem eno izmed dveh najpomembnejših nacionalnih vprašanj prebivalcev v državah članicah EU. Iz slike je na primer razviden jasen odmik navzgor, za večino grafov v jeseni 2005, takoj po napadih v Londonu. To je sicer lahko razumljivo za Anglijo, toda zakaj imajo Francija, Nizozemska in Danska podobne trende? Težko je dokazati povezavo nihanja teh grafov izključno s poročanjem medijev o teroristični dejavnosti, ali nekih drugih, osebnih ali nacionalnih dejavnikov anketirancev. Razvidno je, da se strah v vezi s terorizmom ob terorističnem napadu dvigne po vsem svetu, ali vsaj po vsej celini, so pa v istem obdobju padci zaznavanja strahu za nekatere države, kot so Portugalska in Španija. Različne razlage bi lahko bile del odgovora, vsekakor pa je pomemben dejavnik obravnave terorizma v medijih, ugotavljajo na nizozemskem inštitutu za krizni menedžment (Institute for Safety, Security and Crisis Management [COT], 2008).



Slika 5: Percepcija terorizma v enajstih državah EU (COT, 2008)

V nekaterih evropskih državah je sicer zaznava terorizma zelo nizka, vendar je treba poudariti, da prebivalci v večini evropskih držav zaznavajo terorizem kot zelo močno grožnjo varnosti (npr. Španija, Anglija in Danska) in se na teroristične akcije in grožnje tudi bolj intenzivno odzivajo.

3.7.2 Percepcija terorizma v Kanadi

Podobna nacionalna raziskava kot v EU, ki se je osredotočala na predstavo s terorizmom povezanih tveganj, je bila v L. 2008 izvedena v Kanadi (Lemyre, Turner, Lee in Krewski, 2008). Skupno 1.502 odraslih Kanadčanov je bilo udeleženih v telefonskem anketiranju in raziskavi, ki zagotavlja statistično in opisno dojemanje groženj terorizma v Kanadi. Raziskali so posebne vrste in posledice terorizma, kot tudi vire informacij o terorizmu. Na splošno so vprašani poročali, da je terorizem nizka do zmerna nevarnost za Kanadsko prebivalstvo in še manjša nevarnost za posameznika. Izsledki raziskave prav tako navajajo, da je trenutno zelo malo skrbi o terorizmu v Kanadi. Kanadski mediji pa so navedeni kot vir najpogostejših verodostojnih informacij o terorizmu, medtem ko so izvoljeni politiki in vladni uradniki, navedeni kot najšibkejši vir teh informacij. Pregledane so bile tudi demografske razlike v dojemanju terorizma, pri čemer spol predstavlja pomemben dejavnik.

Pomembnost dojemanja terorizma v širšem kontekstu je zelo poudarjena v ugotovitvah kanadske raziskave (Lemyre et al., 2008). Ker v zadnjih letih na kanadski tleh niso imeli terorističnih napadov (kot v ZDA in Veliki Britaniji) je prišlo do tega, da zelo malo Kanadčanov dojema terorizem kot veliko nevarnost za njihovo življenje (samo 13,3% anketirancev navaja, da terorizem predstavlja »visoko tveganje« in le 5,7% vprašanih iz kanadske javnosti navaja, da terorizem predstavlja »veliko nevarnost« za njihovo osebno življenje). Kljub temu, pa je javnost v Kanadi prepoznala nevarnost povezano s terorizmom, kot negotovost (67,6% vprašanih ocenjuje terorizem kot »zmerno tveganje« ali kot »visoko stopnjo negotovosti«). Glede povečanega osebnega nadzora so v 73,5% mnenja, da se nadzor ni povečal oz. občutijo osebni povečan nadzor zaradi tveganja terorizma »skoraj nič«. V zaključku povedo, da je teroristično tveganje sprejemljivo oz. 60,7% vseh vprašanih je mnenja, da je stopnja tveganja v vezi s terorizmom »skoraj nič«.

3.7.3 Percepcija terorizma v Sloveniji

Analize nekaterih kazalcev terorističenega ogrožanja nacionalne varnosti so pokazale, da je stopnja ogroženosti RS nizka (Prezelj, 2006; Meško in Dobovšek, 2007). Pri raziskavah teroristične ogroženosti Republike Slovenije (RS) je potrebno upoštevati vse oblike terorističnega delovanja (temeljne, posebne in podporne), saj nobena družba ni imuna na teroristične grožnje in napade (Sotlar, 2010). Terorističnih groženj ni zaznati z ozemlja RS, ampak predvsem iz tujine. S stališča teroristične ogroženosti RS je zato zelo pomembno poznati teroristično ogroženost sosednjih držav in evroatlantske regije s poudarkom na Jugovzhodni Evropi. Primerjalna analiza rezultatov Slovenskega javnega mnenja v zvezi z zaznavanjem terorizma od l. 1999 do l. 2005 je pokazala, da Slovenci v povprečju zaznavajo terorizem le kot majhno grožnjo (Prezelj, 2006). Zanimivo je, da je bila zaznava terorizma v Sloveniji najvišja l. 1999, torej pred terorističnimi napadi v ZDA l. 2001. Teroristični napadi v ZDA, Angliji in Španiji niso prispevali k večjemu odzivu slovenske javnosti na terorizem kot grožnji nacionalne varnosti.

4 INFORMACIJSKO - KOMUNIKACIJSKA ORODJA TERORIZMA

Internet nudi globalno povezanost, ki je realizirana z naborom protokolov za nadzor storitev ter internetnih protokolov (Transmision Control Protocol - TCP/IP). TCP/IP omogoča komuniciranje med napravami na nizkem nivoju referenčnega modela (OSI), ne glede na tip in proizvajalca. S tem posledično izbriše državne meje in se navidezno obnaša kot eno omrežje. Naslednja prepoznavna lastnost interneta je njegovo lastništvo. Nobena družba, ustanova ali država ga nima pod svojo jurisdikcijo. Kot lastnika lahko uvrstimo kogarkoli, ki je priključen na omrežje. Torej internet ni od nikogar in je od vseh, od ISP-jev, do končnih uporabnikov. Kibernetski teroristi v večini primerov uporabljajo za svoje politične aktivnosti metode zastraševanja in škodovanja, ki so različne tehnike računalniškega kriminala: hacking, phishing, zloraba osebnih podatkov, avtentikacijski napad (DoS) (Schmidt, 2004).

4.1 *Vrste kibernetskega kriminala in terorizma*

Metode, ki jih novodobni teroristi uporabljajo se spreminjajo z razvojem novih tehnologij. Čeprav so te tehnologije pogosto razvite za nekatere druge, nenevarne namene, tehnični napredek zagotavlja teroristom in kibernetičnim teroristom nova orožja za svoj arzenal. Ta nova orožja so: Radiofrekvenčna orožja in razstrelivo, TED (Transient Electromagnetic Device), naprave za TEMPEST monitoring, elektromagnetne bombe (povzročena škoda, je podobna škodi, ki bi nastala ob udaru strele), računalniški virusi in drugi s tem povezani škodljivi računalniški programi. Eksplozija vodikove bombe na visoki nadmorski višini ustvarja močan elektromagnetni pulz na velikem geografskem območju. To povzroča škodljive učinke na električnem omrežju v brezžičnih antenah, telefonskih linijah itd. Strateško jedrsko orožje, ki se uporablja na ta način, z namenom, da moti komunikacije in/ali električno infrastrukturo, se imenuje elektromagnetna bomba. Kibernetski terorizem lahko opredelimo tudi z metodami informacijskega napada. V družbah tretjega vala (informacijskih družbah), tako obstajata dve ključni metodi informacijskega terorističnega napada, pri čemer je (tabela 2):

- IKT kot cilj ali tarča, ki je lahko fizična ali digitalna,

- IKT kot orodje ali sredstvo za večjo operacijo, to sredstvo pa je lahko fizično ali digitalno.

Prva metoda vključuje napad na informacijske sisteme z namenom uničiti ali onesposobiti informacijski sistem ali informacijsko infrastrukturo, ki je odvisna od napadene. Druga metoda vključuje manipuliranje in izkoriščanje informacijskih sistemov, spreminjanje ali krajo podatkov ali prisiljenje sistema, da opravlja funkcije, za katere ni namenjen (Devost, Houghton in Pollard, 1997-1998).

Tabela 2: Metode terorističnega napada (Devost et al.,1997–1998)

		CILJ	
		FIZIČNI	DIGITALNI
ORODJE	FIZIČNI	a) Uporaba fizičnih sredstev za napad na fizične tarče - klasični terorizem.	b) Uporaba fizičnih sredstev oz. orodij za napad na digitalne cilje (npr. napad IRE na London Square Mile, 4. oktobra 1992)
	DIGITALNI	c) Izkoriščanje informacijskih sistemov za uničenje fizičnih ciljev (npr. heker prelisiči kontrolo letenja in zaradi tega strmoglavi letalo)	d) Uporaba digitalnih orodij za digitalne tarče oz. cilje (npr.trojanski konj v javnem omrežju)

Podobno Belič v informacijskem smislu loči štiri oblike delovanja terorističnih organizacij: medsebojne komunikacije, propagandna dejanja, zbiranje informacij, teroristični napadi z uporabo informacijskih orodij – orožij. Prve tri oblike niso nujno uvod v informacijsko izveden teroristični napad, so lahko le pripravljalne stopnje v klasično teroristično dejanje. Pri terorističnih napadih z informacijskimi orodji – orožji pa je nujen jasen cilj napada (npr. elektroenergetski sistem, sistem transporta, borza itd.). Osnovni cilj takšnega napada je onesposobljenje ciljnega informacijskega sistema (Belič, 2001).

Standardizirana klasifikacija računalniškega kriminala ali kibernetskega terorizma, ki bi bila unificirana na svetovnem nivoju torej še ne obstaja. Glede na motiv nastanka, pa ga lahko v grobem razdelimo na (Milković in Justin, 2004);

1. Politično motiviran računalniški kriminal:

- internetno vohunjenje (ang. Cyber espionage),
- računalniška sabotaža,
- vdor v računalniški sistem (ang. Hacking) in
- internetni terorizem.

2. Ekonomsko motiviran računalniški kriminal:
- internetne goljufije pri trgovanju (ang. Consumer fraud),
- vdor v računalniški sistem (ang. Hacking),
- kraja internetnega časa in storitev,
- črne kopije, piratstvo (ang. Softwarepiracy),
- industrijsko vohunjenje (ang. Industrial espionage),
- žaljenje preko interneta (ang. Libel),
- otroška pornografija (ang. Child pornography),
- pranje denarja,
- neupravičeno prilaščanje intelektualne lastnine (ang. Copyright infringement),
- zloraba elektronske pošte (pošiljanje kriptirane vsebine za organizirani kriminal),
- neupravičena pridobitev tujih gesel (ang. Password sniffing),
- zapora strežbe (ang. Denial Of Service - DOS) in
- napeljevanje h kaznivim dejanjem in podajanje navodil preko interneta za izvananje le-teh (nasilje, rasizem, nacizem¸ izdelava bomb ter pridelava drog).

3. Škodljiva dejanja, ki nimajo vseh značilnosti kaznivih dejanj:
- zanikanje (ang. Repudiation) pošiljanja oziroma prejemanja,
- nadlegovanje (ang. Harassment) npr. bombardiranje poštnih strežnikov,
- izguba zaupnosti (ang. Lost of Confidentiality),
- izguba integritete (ang. Alteration),
- zlorabljanje programske opreme, npr. zadnja vrata (ang. Backdor),
- trojanski konji, črvi[12] (ang. Worm) in
- maskiranje v zakonite uporabnike, oponašanje (ang. Spooofing).

4. Neškodljiva nadležna dejanja:

[12] Črvi (Klez, Bugbear, MyDoom, Sasser, Sircam, CodeRed, BadTrans itd.).

- prvo-aprilske šale, potegavščine in urbane legende (ang. Hoaxes, Urban legends),
- besedni napadi (ang. Flamming),
- odvečna pošta in
- zloraba IRC-a (ang. Internet Relay Chat).

Kot je razvidno, je nabor možne kriminalitete s pomočjo interneta zelo velik. Velika večina teh, z IKT povezanih kriminalnih dejanj pa lahko najdemo v različnih oblikah kibernetičnega terorizma. Poznan je tudi nov termin, s katerim se označuje zlonamerna kodo, ki opravlja nelegalna dejanja z nevednostjo uporabnika, ki je programsko opremo pognal in katerih namen je doprinesti finančno korist avtorju programa Crimeware. Crimeware predstavlja podkategorijo širšega pojma Malware[13], ki označuje nezaželjene programe, (zlonamerna koda oziroma programska oprema), ki tečejo na računalniku z namenom, da v računalniškem sistemu povzroči škodo. Poznani so glavni načini, kako se Crimeware širi (Emigh, 2006):

- Socialni inženiring, s katerim prepričamo uporabnika da odpre okužen email.
- Napadi tipa cross-site scripting.
- Izkoriščanje varnostnih lukenj.
- Vstavljanje Crimeware programov v piratski programski opremi.

Crimeware je bil ustvarjen z različno paleto tehnologij in vsaka kategorija ima sebi specifično točko okužbe in specifično točko ogrožanja podatkov, zaradi česar vsak posamezni Crimeware program potrebuje specifične ukrepe. Koristi jih za izvajanje DOS napadov, razpošiljanje nezaželene pošte in številna druga dejanja, ki imajo vsa neko finančno korist za napadalca.

4.2 *Problematika kibernetskega terorizma v sedanjem času*

Za lažje razumevanje kibernetskega terorizma v praksi, v nadaljevanju navajamo nekaj napadov, poizkusov napadov ter posledic, te oblike

[13] Malware (virus, črv, trojanski konj, Spyware, Adware itd.) (Skoudis in Zeltser, 2003).

terorizma. Med zadnje primere spadajo obsežni kibernetski napadi na Estonijo l. 2007 (CRS, 2008) in pretrganje medcelinskih kablov l. 2008.

DOS kibernetski napad izveden l. 2001, je onemogočil delovanje sistema za vodenje ladij v pristanišču Houston, kjer bi lahko prišlo do hude nesreče (Villiers, 2006).

Računalniški črv »Slammer«, je vstopil v sistem podjetja FirstEnergy Corp. prek omrežja ene od pogodbenih partneric, od koder se je prek linije za prenos podatkov T1, prenesel v sistem jedrske elektrarne David-Besse. V elektrarni je zaradi preobremenitev omrežja, prišlo do 5-urnega izpada sistema za kontrolo centralnega računalnika (Safety Parameter Display), ki nadzira hladilni sistem, temperaturo reaktorjev sredice, senzorje za nadzor zunanjega sevanja itd. Naključje, ki je rešilo podjetje pred katastrofo, je bilo to, da reaktor ni deloval od l. 2002, ker so na lupini reaktorjev odkrili razpoke (Poulsen, 2003).

V ZDA je l. 1996, prišlo do napada, ki je rezultiral v tem, da je virus simultano klical številko za klic v sili 911 in s tem sprožil ogromno lažnih klicev. V takšnem primeru morda pomoči ni mogel priklicati kdo, ki jo je nujno potreboval.

Leta 2004 se je začel največji DOS napad v zgodovini interneta na spletno stran podjetja Santa Cruz Operation (SCO), ki je primoral podjetje, da so prestavili spletno stran. Vodilni SCOja in Microsofta (MS) so razpisali zelo visoke denarne nagrade, na lov za storilci pa se je podala FBI in tajna služba ZDA (US Secret Service). Posebnost tega napada je, da je prvi te vrste, ki je označen za kibernetski terorizem.

Eden izmed bivših pogodbenih partnerjev ameriške mornarice, je v računalniški sistem, namenjen navigaciji podmornic, namestil zlonamerno kodo in tako onesposobil tri izmed petih računalnikov. Podmornice imajo med gibanjem zelo omejeno zmožnost zaznavanja predmetov, ki se nahajajo

neposredno pred njimi, zato so v veliki meri odvisne od računalniškega omrežja. Med gibanjem podmornice je zaznavanje predmetov s sonarjem moteno zaradi gibanja vode ob trupu podmornice. V kolikor bi si napadalec prizadeval zgolj za potvarjanje podatkov in ne toliko za onesposobitev računalniškega sistema, bi se lahko zgodilo, da bi prišlo do trčenja med dvema jedrskima podmornicama. Ker se je napad zgodil v italijanski vojaški bazi, v kateri je stacionirana ameriška 6. flota, bi morebitno trčenje podmornic ogrozilo življenje na področju Sredozemlja (Bratuša, 2007).

Kot primer kibernetskega terorizma, lahko navedemo tudi »spletno vohunjenje« na Kitajskem, katerega namen je bilo rušenje oblasti. Zaradi tega je utrpela izgubo zaupnih podatkov, saj so se na spletu znašle nekatere državne skrivnosti. Kitajska je zaradi tega sprejela ukrepe v smislu poostrene cenzure, novih varnostnih teles in komercialen nadzor.

Vsi našteti primeri nakazujejo, da bodo kibernetični napadi v prihodnosti, postali resna teroristična grožnja varnosti.

4.3 *Osnovna orodja in tehnike hekerjev ter teroristov (kibernetski terorizem v praksi)*

Na začetku obdobja interneta, ko zakoni o njegovi uporabi še niso bili niti približno definirani, je bil neodkrit virtualen svet, če karikiramo, kakor Amerika pred Kolumbom. Lahko si ga uporabljal svobodno, brez pretiranega strahu, da se bo v računalniku pojavil črv, da bo nekdo uničil podatke ali da nikoli ne prispe stvar, ki ste si jo kupili po eBayu[14]. Kljub izdelanim varnostnim mehanizmom podjetja, namreč še zmeraj prihaja do zlorab. Super hitri razvoj tehnologije je veliko pripomogel, da tudi razvoj kriminalnih del napreduje. Ključno je, da so kriminalci v velikem številu vedno bili korak pred razvojem, oziroma korak pred policijo.

[14] eBuy je podjetje z internetno prodajo (www.ebuy.com), ki preko svoje infrastrukture in spletne strani omogoča prodajo, nakupovanje in dražbe po vsem svetu.

Osnovna orodja in tehnike hekerjev so trojanski konji, skenerji, vohljači socialni inženiring, steganografija itd. Dodatna hekerska orodja so razbijalci gesel ter orodja za skrivanje in krajo identitete, brisanje sledi itd. (Emigh, 2006). Med uničevalne programe in tehnike pa spadajo še virusi, črvi in DOS. Teroristične organizacije in kriminalne združbe pri svojem delovanju vse bolj uporabljajo novo tehnologijo. To dokazujejo vsakdanji primeri, saj se po svetu vrstijo aretacije, pri katerih imajo pripadniki različnih terorističnih celic pri sebi najmodernejšo računalniško opremo. Po terorističnih napadih v ZDA l. 2001, se je med varnostnimi strokovnjaki okrepilo mnenje, da bodo informacijski sistemi ena od naslednjih tarč (Weimann, 2005). Za povečanje učinkovitosti odkrivanja teroristov, je potrebno povečati nadzor nad ljudmi ter sprejeti dodatne varnostne ukrepe.

Soočanje z dinamično globalizacijo informacijskih družb v povezavi s tehnološkimi izboljšavami (npr. lokalne brezžične povezave) povečuje možnosti medsebojnega povezovanja. Širjenje storitev in uporabnikov pa povečuje tudi ranljivost in ogroženost, ki se je večina med nami sploh ne zaveda. V poročilu ameriškega sveta za znanost in tehnologijo (National Science and Technology Council [NSTC], 2006) so opredelili naslednje tehnološke trende, ki povzročajo skrbi in povečujejo ranljivost informacijske infrastrukture:

- vse večja kompleksnost informacijskih sistemov predstavlja varnostni izziv za razvijalce in uporabnike,
- telekomunikacijska infrastruktura se vedno bolj razvija, pri čemer se tradicionalni telefonski sistem in informacijska tehnologija vse bolj združujeta v enotno platformo.

4.3.1 Financiranje terorizma

Teroristične organizacije so zelo različne, od velikih, paradržavnih organizacij do majhnih, decentraliziranih in samostojnih mrež. Teroristi za finančne zahteve odražajo raznolikost, ki se bistveno razlikujejo med organizacijami. Financiranje je potrebno tako za financiranje posebnih terorističnih operacij, izpolnitev širše organizacijskih ciljev razvoja in vzdrževanja organizacije, kot

za ustvarjanje ugodnega okolja, ki je potrebno za ohranitev svoje dejavnosti. Neposredni stroški izvedbe posameznih napadov so nizki v primerjavi s škodo, ki jo lahko prinesejo. Vendar pa vzdrževanje terorističnih mrež, ali posebnih celic zahteva tudi oskrbo za zaposlovanje, načrtovanje in izvedbo naročil napadov, kar predstavlja pomemben odliv sredstev. Pomembna infrastruktura je potrebna za vzdrževanje mednarodne teroristične mreže in spodbuja svoje cilje v daljšem časovnem obdobju. Organizacije zahtevajo veliko sredstev za ustvarjanje in vzdrževanje infrastrukture, organizacijsko podporo za vzdrževanje ideologije terorizma s pomočjo propagande, ter za financiranje domnevno zakonite dejavnosti, potrebne za zagotavljanje tančice legitimnosti teroristične organizacije (FATF, 2009).

Finančna sredstva za terorizem lahko prihajajo iz široke palete možnih virov, med katerimi so (Kendry, 2007):

- državno financiranje,
- ustvarjanje prihodka iz zakonitega poslovanja (Podbregar, Pleteršek in Ivanuša, 2010),
- ustvarjanje nezakonitega prihodka (včasih v partnerstvu s skupinami organiziranega kriminala) z ugrabitvami, tihotapljenjem priseljencev, žensk, mamil ter prodajo lahkega orožja in osebne oborožitve,
- zloraba dobrodelnih donacij,
- prispevki radikalnih diaspor,
- neformalna denarna nakazila z uporabo plačilnega sistema, preko mreže ponudnikov finančnih storitev (ki delajo na podlagi zaupanja, z minimalnimi evidencami in lahko regulatorno strukturo) ter
- kraja, tihotapljenje in korupcija (zlasti v povezavi z nafto).

Po napadih v ZDA septembra 2001, poskušajo različne agencije (Financial Transactions Reports Analysis Centre of Canada - FINTRAC, 2011; FATF, 2009) po vsem svetu, z različnimi študijami ugotoviti panoge in sektorje, ki so se preko finančnih storitev uporabljale za financiranje terorističnih napadov. Odkritih sicer ni bilo nobenih empiričnih dokazov, so pa študije pokazale, da so nekateri vrednostni papirji bili uporabljeni bodisi za financiranje napadov

ali pa za samo pridobivanje finančnih sredstev (na primer s prodajo zalog letalskega prevoznika ali hotelov (FATF, 2009). Čeprav so teroristične operacije in asimetrično bojevanje relativno poceni, vzdrževanje teroristične organizacije stane veliko denarja.

4.3.2 Kibernetski terorizem in mediji

Tarča informacijskega kriminala, so zelo pogosto tudi mediji, zaradi namena zastraševanja. Mediji so namreč tisti, ki lahko v javnosti vzbujajo občutek ogroženosti s terorističnimi napadi. Glavna in najpogosteje uporabljena oblika psihološkega bojevanja je propaganda v smislu načrtnega širjenja novic, informacij, specifičnih argumentov in pozivov z namenom vplivati na prepričanja, mnenja in delovanja določenih skupin. Nekdanja britanska premierka Teacherjeva je večkrat poudarila, da so mediji kisik za terorizem (Muller, Spaaij in Ruitenberg, 2003). Ameriška in britanska vlada preko medijev opozarjata, da bi naj bile na udaru državne spletne strani z zaupnimi in osebnimi podatki in borze. Po mnenju Saydijarija (2004), so v nevarnosti jedrski sistemi in elektrarne. Ohromitev enega največjih generatorjev električne energije za severovzhodni del ZDA v Detroitu, bi lahko povsem ohromilo življenje na tem območju. V kolikor odštejemo dejansko možnost, da bi bilo omogočeno upravljanje jedrske elektrarne izključno preko interneta, je očitno, da je bila objavljena vsebina, medijska manipulacija teroristov. Manipulacija elektronskih medijev z namenom terorističnе grožnje, se kaže na spletnih straneh Hezbolaha[15], kjer si lahko ogledamo videoposnetke napadov na različne izraelske tarče in posnetke žrtev izraelskih bombardiranj. Hesbollah je med zadnjimi spopadi z Izraelom vdrl v komunikacijski sistem izraelskih oboroženih sil, prav tako pa se v islamskem svetu vse pogosteje govori o t.i. info-jihadu, kot IKT za potrebe svete vojne (Golpira, 2006). Na teh spletnih straneh, so navedene različne deklaracije, govori in politične izjave pripadnikov. Nadalje so ameriški mediji razkrili, da Amazon[16] in

[15] Hezbolah (stranka boga) velja za eno izmed najbolj radikalnih skupin, katere glavni cilj je oblikovanje islamske republike po zgledu Irana (Isserof, 2006).

[16] Amazon je največje ameriško podjetje za internetno prodajo knjig na svetu (Golob, 2005).

računalniški gigant Microsoft (MS) oglašujeta svoje izdelke oziroma storitve na Hezbolahovih spletnih straneh. Ob tem, se seveda zastavlja vprašanje: »Ali MS in Amazon podpirata Hezbolah?«. Obe korporaciji sta sicer odločno zanikali poslovanje s to organizacijo, ob tem pa so oglase umaknili še isti dan, ko so novico o tem objavili ameriški mediji.

Al-Kajda, velja za informacijsko zelo dobro opremljeno teroristično skupino. V terorističnih skrivališčih, so našli prenosne računalnike in sodobne komunikacijske naprave. V računalnikih je bilo nameščenih veliko sodobnih hekerskih orodij. Obveščevalci odkrivajo tudi mnoge komunikacijske poti, ki jih ubira Al-Kajda in ugotavljajo, da so tehnološko napredni, saj komunicirajo prek interneta, svoja sporočila pa skrivajo na vse mogoče načine, tudi s steganografijo (poglavje 5.3.4).

Preiskave skrivališč, ki so bile opravljene po terorističnih napadih v ZDA l. 2001, nam lahko nakažejo smer delovanja teroristov v prihodnosti. Problem organiziranega spletnega kriminala so predvsem neomejujoči zakoni in finančna sredstva, kar mu zagotavlja korak prednosti pred preganjalci.

4.3.3 Internet kot orodje kriminala in terorizma

Goljufati preko interneta, pomeni zavajanje in oškodovanje z uporabo interneta kot orodja (International Fraud Compliant Center [IFCC], 2006). Razumevanje pojma goljufija navaja na dejstvo, da oškodovanec sam posreduje podatke, ki lahko posledično povzročijo materialno škodo ali krajo zaupnih podatkov (Milkovič in Justin, 2004). Goljufije preko interneta se pojavljajo znotraj elektronskega poslovanja[17] in so razporejene v devet osnovnih kategorij:

1. Prevara finančne institucije; napačen prikaz resničnega stanja ali s prikrivanjem materialnih dejstev osebe, organizacije finančni ustanovi za udejstvovanje goljufivih dejanj. Primer je zloraba ali uporaba kreditne

[17] Splošna definicija elektronskega poslovanja (ang. Electronic Commerce) sicer ne obstaja, vendar pa v osnovi zajema kakršno koli elektronsko posredovanje podatkov, nakupovanje, plačevanje.

kartice s strani zanjo nepooblaščene osebe. V to kategorijo se še uvršča zloraba osebnih podatkov za poneverbo identitete (Brumnik in Podbregar, 2010). Tu so mišljeni rojstni datumi, razne identifikacijske številke in identifikacijska imena.

2. Prevare pri igrah na srečo; sodelovanje v zrežiranih stavah ali stave na dogodkih, ki ne obstajajo.
3. Komunikacijske prevare; prikrita uporaba sistemov, omrežij. Nedovoljeno priključevanje predvsem na brezžične poveze in satelitsko komunikacijo (Cooperative Association for Internet Data Analysis [CADIA], 2011).
4. Prevare okoriščanja s sredstvi; posamezniki ali organizacije se s pomočjo poneverbe pri državnih ustanovah poskušajo dokopati do energijskih virov (električna energija, nafta itd.).
5. Zavarovalniška goljufija; napačna identifikacija zavarovanca pri zavarovalnici oziroma lažnivo navajanje podatkov za uveljavljanje zavarovanja. Sem spadajo prijave škode in poškodb, katerih nikoli ni bilo in uprizorjene nesreče.
6. Prevare državnih ustanov; lažno prikazovanje predvsem materialnega stanja z namenom izogibanja plačilu davkov, ponarejanja valut itd.
7. Investicijska goljufija: sem sodijo predvsem denarna vlaganja v razne denarne piramide.
8. Poslovne goljufije; podjetje namenoma lažno predstavi oziroma prikriva dejansko stanje. Sem sodi prikrivanje bankrota in kršenje avtorskih pravic.
9. Prevara zaupanja; oškodovanec je prepričan v poceni nakup, visoko obrestno posojilo, zelo ugodno finančno ponudbo. Slednje predstavljajo večino goljufij preko interneta in se delijo na:
   - Organizacija lažnih dražb na internetu (Kupljeno in plačano blago, ki pa ni nikoli dostavljeno).
   - Nigerijska pisma; so pisma, ki se širijo v obliki zelo ugodnih finančnih ponudb. Vsebujejo svojevrsten način predstavitve in ponujajo zelo visoke dobičke ob minimalnem vlaganju.

Teroristične organizacije na internetu lahko delujejo na več možnih načinov: zbiranje občutljivih podatkov o tarčah, zbiranje finančne podpore,

povezovanje med različnimi skupinami, izsiljevanje, propaganda (Kimmage, 2008), psihološki vplivi, goljufije ter prikrite operacije (Thomas, 2003).

4.3.4 Steganografija

Beseda steganografija izvira iz Grščine in pomeni »zakrito pisanje«. Na kratko pa steganografija predstavlja metode skrivanja informacij v druge informacije (Kahn, 1967). Praktično to pomeni, da nam steganografija omogoči da neko sporočilo skrijemo v npr. sliko, zvočno datoteko ali celo v drugo tekstovno datoteko. Postopek bi lahko primerjali z vodnim tiskom, le da gre v tem primeru za neke vrste »elektronski vodni tisk« Steganografija je relativno mlada veda, saj se je začela intenzivneje razvijati šele sredi devetdesetih let z razvojem računalnikov (Johnson, 1995). Njen izvor sega v antično Grčijo, pred drugo svetovno vojno pa je ta tehnika pomenila bolj ali manj pisanje z nevidnim črnilom (Kahn, 1967). Steganografija ima široko polje uporabnosti, od skrivanja informacij, označitev avtorskih pravic datotek (zvočnih in slikovnih), nevidno kodiranje itd. in jo v grobem ločimo na:

- watermarking - vodni tisk (skrivanje informacij o avtorskih pravicah) in
- fingerprinting - puščanje prstnih odtisov (skrivanje serijskih številk v datoteko).

Posebej uporabna je steganografija lahko v povezavi z kriptografijo, ki je povsem preprosta. Datoteko, za katere vsebino želimo da ostane tajna, najprej zakodiramo s programom PGP (Pretty Good Privacy), nato pa kodirano datoteko vstavimo v sliko ali zvočno datoteko. Omogoča komuniciranje, ne da bi potrebovali varen kanal (Lah, 2003). Končni rezultat je torej zakodirano in skrito sporočilo. Razvitih je bilo že kar nekaj steganografskih metod, vse pa v bistvu izkoriščajo »prazen prostor« v datotekah ali na nosilcih digitalnih podatkov.

Razvite so različne metode za skrivanje podatkov (Lah, 2003):

- skrivanje podatkov v slikovne datoteke s pomočjo navideznega povečanja števila barv,

- skrivanje podatkov v zvočne datoteke z za človeško uho neopaznim popačenjem digitalne oblike zvoka,
- skrivanje podatkov na neuporabljene sektorje disket in CDjev,
- skrivanje podatkov v datoteke HTML (Hyper Text Markup Language),
- skrivanje podatkov v ASCII (American Standard Code for Information Interchange) datoteke (s pomočjo zamika kazalca za začetek datoteke) in
- obstajajo programi, ki binarno datoteko pretvorijo v nesmiseln tekst, ki pa je statistično podoben tekstu v poljubnem naravnem jeziku (seveda je potrebno imeti slovar za ta jezik).

Na Internetu je moč najti precej steganografskih programov (Johnson, 2011), vendar nekateri še ne delujejo povsem ali pa so močno nestabilni, saj je steganografija še zmeraj v razvoju. Enega prvih boljših programov je Brown razvil l. 1994 in se imenuje S-Tools (Johnson in Jajodia, 1998). Omenjeni program za kodiranje sporočila (v obliki datoteke) uporablja več algoritmov, podatke pa skriva v grafične in zvočne datoteke.

4.3.5 (Spletna) zloraba osebnih podatkov

V svetu, danes kar 10 milijonom ljudi letno ukradejo identiteto ali zlorabijo osebne podatke (Sullivan, 2004). V poročilu komisije (9/11 Commission, 2004) za teroristične napade 9/11 v ZDA, so navedeni predlogi za obravnavo problematike spletne zlorabe podatkov tesno povezani s terorizmom. V poročilu je lažna identiteta navedena kot ključno orodje za teroriste saj so potne listine enako pomembne kot orožje, navaja poročilo. Ob številnih vstopnih točkah ljudi, je kontrola kritične infrastrukture, zadnja priložnost, da se preveri identifikacija. Terorizem in zloraba osebnih podatkov gresta z roko v roki, pravijo strokovnjaki. Priročnik za usposabljanje pripadnikov Al-Kaide vsebuje napotke za pripravnike, da zapustijo taborišče s petimi lažnimi identitetami, pravi Collins, ki uporablja izvod priročnika po usposabljanju uslužbencev organov pregona. Teroristični osumljenec al-Marri, ki je bil domnevno povezan s terorističnim napadom v ZDA l. 2011, je bil aretiran s prenosnim računalnikom na katerem so bili podatki 1000 ukradenih kreditnih kartic, skupaj z množico internetnih zaznamkov, ki kažejo na krajo identitete.

Presenetljivo pa je, da so ugrabitelji letal v jutru 11. septembra uporabljali svoja prava imena, ob vkrcanju na lete (Identity Theft Protection Resource Center [ITPRC], 2011).

Sistemske napake pri identifikaciji, so v poročilu komisije 9/11 (2004) večkrat izpostavljene in celo dobro poznane. V ZDA namreč obstaja mnogo različnih agencij, kjer lahko izdajo različne dokumente (dovoljenja za vožnjo itd.) na osnovi rojstnih listov in ravno ti dokumenti, poznan kot »dokumenti o izvoru«, so večkrat temeljni izvor kraje identitete. Zaradi obstoja različnih formatov teh dokumentov, je skoraj nemogoče, da na kraju samem identificirajo ponaredke in zato že dolgo velja napotek varnosti v ZDA, da vozniško dovoljenje, ni nezanesljiv način za identifikacijo osebe. Kongresni preiskovalci pod krinko, so tako lahko pridobili veljavna vozniška dovoljenja, v pisarnah za registracijo motornih vozil po vsej državi, na osnovi lažnih dokumentov, kot je potrdilo o rojstvu. Enako so preiskovalne ekipe uporabile ponarejene identifikacijske dokumente, za vstop na omejena področja vladnih poslopij in letališčih v l. 2002 (ITPRC, 2011). Tabela 3 opisuje in definira spletno zlorabo podatkov v štirih korakih.

Tabela 3: Postopek spletne kraje identitete (Emigh, 2005)

Načrtovanje	Phisherji se odločijo, kateri cilj (podjetje, državne ustanove itd.) bodo napadli in kako priti do e-pošte uporabnikov tega podjetja. Pogosto uporabljajo velike količine e-poštnih sporočil in naslovov podobno kot spammerji.
Priprava	Ko enkrat vedo, katero podjetje bodo napadli in kdo so njihove žrtve phisherji razvijejo metodo za pošiljanje sporočil in za nabiranje podatkov, ki so jih zbrali. Pogosto to vsebuje e-poštni naslov na internetni strani.
Napad	To je del postopka, ki je ljudem najbolj znan. V njem pa pošljejo sporočilo ki je podobno sporočilu ki bi ga uporabnik drugače sprejel od podjetja.
Zbiranje	Phisherji zbirajo podatke ki so jih uporabniki vpisali na internetno stran.
Zloraba osebnih podatkov ali prevara	Phisherji uporabljajo podatke, ki so jih zbrali, da izvršujejo ilegalne nakupe ali pa podatke uporabijo za kake druge prevare. Četrtina od žrtev si po napadu nikoli ne opomore.

4.4 *Informacijska orodja ter policijsko - obveščevalna dejavnost proti kibernetskemu terorizmu*

ZDA so l. 1994 sprejele zakon za telefonske komunikacije (Digitalyderl Telephony Act), po katerem bi morali proizvajalci telekomunikacijske opreme puščati neke varnostne luknje zaradi nadzora. Prisluhe in nadzore torej vršijo različni državni represivni organi. Poleg tega, nas na internetu nadzirajo tudi velike korporacije. Zavedati se moramo torej tudi možnosti sodelovanja teh korporacij z državnimi organi, ki jim odstopajo naše podatke. V ZDA primer takšnega sodelovanja razkriva tožba organizacije za elektronske svoboščine proti telekomunikacijskemu podjetju, ki je Ameriški nacionalni agenciji (NSA) nezakonito omogočili dostop do podatkov o ameriških uporabnikih telefonije in interneta. Znan je tudi primer kitajskih oporečnikov, ki so jih identificirali in zaprli na podlagi podatkov, ki so jih kitajske oblasti pridobile od ameriške korporacije Yahoo. Tudi Google se je v preteklosti že uklonil pritiskom Kitajske.

Pravzaprav sta 20. in 21. stoletje obdobje obveščevalne dejavnosti v smislu avtomatičnega pridobivanja, analize in interpretacije informacij. Tako naj bi obveščevalne službe v prihodnje oblikovale elektronske baze, v katere bi uvrščale svoje obveščevalne izdelke, uporabniki pa bi med slednjimi sami izbirali (deskanje) ustrezne informacije (Podbregar, 2010). EU te aktivnosti opravlja že vsaj od l. 1996, teroristični napadi 2001 pa so to samo pospešili. Predlogi za povečanje nadzora in mednarodno sodelovanje na tem področju, so bili pripravljeni že pred 11. Septembrom 2011. Na spletu lahko najdemo seznam omrežij (Cryptome, 2011), ki naj bi bila kakorkoli povezana, ali so pod kontrolo ameriške varnostne službe NSA (National Security Agency). Med nadzorovana omrežja s strani NSA spadajo tudi nekatera, ki se nahajajo v Sloveniji (Akademska in raziskovalna mreža Slovenije - ARNES, Telekom, Mobitel itd.)

Razumljivo je, da zaradi uspešnosti preventivnega protiterorističnega delovanja, represivni organi želijo čim več nadzora. Do teh tendenc bi morali politika in javnost zavzeti neko distanco in prevelike »apetite« represivnih

organov omejiti. Problem je, ker se nadzorovalna tehnologija lahko obrne tudi proti državi. Obstoječo nadzorovalno tehnologijo, ki je bila vzpostavljena za namene zakonitega nadzora, namreč lahko zlorabijo tudi kriminalne ali teroristične združbe. Tipična primera sta bili prisluškovalni aferi v Grčiji in Italiji. Telefonske centrale imajo namreč celo vrsto funkcionalnosti za izvajanje prisluhov. V Grčiji je napadalcem (verjetno kakšna tajna služba, lahko pa tudi kriminalna združba) uspelo izrabiti varnostno ranljivost v modulu telefonske centrale, namenjene zakonitemu prisluškovanju. Več kot pol leta so prisluškovali okoli 100 politikom, med drugim tudi predsedniku vlade (Kovačič, 2007).

4.5 *Biometrija kot informacijsko orodje za boj proti terorizmu*

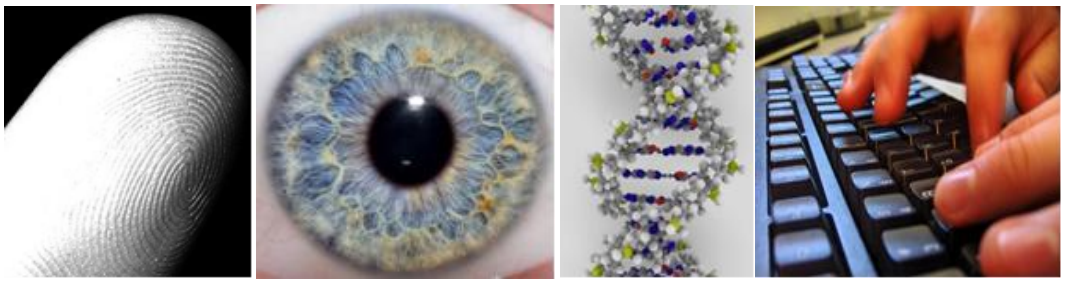
Zaradi povečevanja mobilnosti populacije ter posledično globalizacije terorizma, je nujna razpoložljivost globalnih informacij, s katerimi lahko identificiramo človeka, vedno večja. Inteligentni biometrični sistemi lahko z novimi algoritmi opazijo sumljivo ali deviantno obnašanje posameznika, ki ima lažno identiteto ali pa celo pravo, vendar se njegovo vedenje iz kakršnihkoli razlogov razlikuje od običajnega. Odstopanje se kaže v odklonskosti od običajnega vedenja (npr. oseba je pod vplivom opojnih substanc ali ima porušeno duševno ravnotežje) ali pa od posameznikovih lastnih biometričnih značilk (npr. glede na starost, videz itd.) (Brumnik, 2011). Zagotoviti moramo verodostojne in hitro dosegljive informacije ter upoštevati njihovo morebitno zaupnost. »Teroristu je mogoče slediti edino s pomočjo biometrije« (Kirkpatrick, 2001). O uporabnosti biometričnih sistemov v boju proti terorizmu je dosti napisanega tako v strokovni literaturi kot znanstvenih člankih. V Sloveniji smo implementirali Schengenski Informacijski Sistem (SIS), ki omogoča vpogled v skupno evropsko bazo ter na osnovi tega lažjo identifikacijo terorista.

Z biometrijo smo lahko identificirani skozi fizične značilnosti (obraz, oči, prstni odtis, DNK itd.) in biološke lastnosti (glas, podpis, hoja in dinamika

tipkanja). Biometrijo lahko uporabimo v dveh primerih: za identifikacijo ali prepoznavanje posameznika na osnovi primerjave podatkov z vsemi shranjenimi podatki v bazi ter za verifikacijo (avtentikacijo) oz. potrditev, kjer v procesu identifikacije ugotovimo ali res gre za tisto osebo, za katero se izdaja (Brumnik, 2011). Poznamo različne načine ali modalnosti biometrične identifikacije in verifikacije oseb (Jain et al., 2002):

- Prstni odtisi (slika 6.a) so vzorci, prisotni na človeškem prstu in so edinstveni za vsakega človeka (razlikujejo se tudi glede na vsak prst).
- Prepoznavanje geometrije obraza je najbolj sprejemljiv biometrični podatek in je najbolj splošna metoda identifikacije, ki jo uporabljamo pri vizualni komunikaciji. Kljub temu pa se tudi ta tehnologija spopada z različnimi težavami, kot so procesi staranja, obrazno izražanje itd.
- Geometrija rok temelji na identifikaciji človeka glede na obliko roke, npr. velikost in širino prstov.
- DNK (slika 6.c) je zares edinstvena koda vsakega posameznika (razen enojajčnih dvojčkov, ki imata isti DNK vzorec).
- Vsak posameznik ima edinstveno strukturo šarenice (slika 6.b). Natančnost in hitrost sistemov, ki temeljijo na šarenici, sta obetavni, izvedljiv pa je tudi identifikacijski sistem velikega obsega. Vsaka šarenica je unikatna, podobno kot pri prstnem odtisu pa se tudi šarenici dvojčkov razlikujeta. Šarenico je zelo težko ponarediti, ugotavljanje umetnih dodatkov pa je dokaj enostavno. S spreminjanjem osvetlitve lahko še dodatno ugotovimo, ali se oko pravilno odziva, s tem pa, ali gre za živ objekt. Zajemanje slike šarenice je manj vsiljivo kot pri mrežnici, ker se šarenica lepo vidi tudi z razdalje nekaj metrov.
- Žilna sistema mrežnice levega in desnega očesa se močno razlikujeta, enak pojav zaznamo tudi pri levem in desnem prstnem odtisu.
- Preverjanje podpisa temelji na načinu pisanja, ki pa je velikokrat odvisen od trenutnega čustvenega in fizičnega stanja posameznika. Poznamo statično (le geometrijska oblika podpisa, npr. velikost in oblika črk) in dinamično (ne samo oblika podpisa, ampak tudi hitrost, način pisanja) verifikacijo podpisa.

- Prepoznavanje glasu je odvisno predvsem od kvalitete mikrofona in komunikacijskega kanala, prav tako pa tudi od posameznikovega zdravja (prehlad itd.), stresnih in emocionalnih situacij.
- Infrardeča toplotna identifikacija obraza in ostalih delov telesa – termogram: človeško telo oddaja toploto in ta vzorec toplotnih žarkov predstavlja značilnosti vsakega posameznika.
- Dinamika tipkanja (slika 6.d): vsak posameznik na tipkovnico tipka na svojevrsten način. Ta dinamika temelji na časovnih presledkih med tipkanjem (Hocquet, Ramel in Cardot, 2005).
- Prepoznavanje hoje: svojevrstne način hoje, ki pa ni edinstvena za vsakega posameznika, vendar je zadostna značilnost za identificiranje. Seveda pa se skozi obdobja spreminja (pridobitev telesne teže, ob alkoholiziranosti itd.).
- Vonj: vsak posameznik izloča vonj, torej posebne značilnosti kemične sestave vonja.
- Biometrija ušesa je ločevanje glede na obliko in strukturo, vendar pa vsak posameznik nima edinstvenega ušesa.



a. prstni odtis b. šarenica c. DNK d. tipkanje

Slika 6. Pregled nekaterih biometrij (Information Telecommunication Union [ITU], 2009)

5 BIOMETRIČNI IDENTIFIKACIJSKI SISTEMI

Skupna značilnost biometričnih identifikacijskih sistemov so značilke (osebne lastnosti), ki z različnimi posredovalci ali nosilci informacij omogočajo zanesljivo elektronsko prepoznavo elementa identifikacije in razlikovanje med pooblaščenimi in nepooblaščenimi uporabniki (Trast International, 2010). Identifikacijo lahko opravljamo ročno ali pa se izvaja avtomatično, pri čemer se identifikacijski elementi v sistemu samodejno identificirajo preko medija.

5.1 *Identifikacija in verifikacija (avtentikacija)*

Pogosto se zgodi, da pojem avtentikacija uporabljamo pri verifikaciji in nasprotno (National Science and Technology Council [NSCT], 2006). Avtentikacija pomeni določanje osebe na podlagi njenih biometričnih podatkov. Največkrat imamo bazo biometričnih podatkov, s katero primerjamo trenutno zajete podatke, dokler ne najdemo najbolj sovpadajočih. Iščemo med N osebami v bazi, zato tudi pogosto rečemo, da je to 1:*N* (one-to-many comparison). Pri identifikaciji iščemo identiteto osebe (npr. ime). Pri verifikaciji pa preverjamo, ali je oseba res tista, za katero se predstavlja (Mraović, 2003). V tem primeru imamo samo eno primerjavo 1:1 (one-to-one comparison). Ker vemo, kdo naj bi ta oseba bila (poznamo ime), primerjamo s senzorjem odčitane podatke s podatki te osebe, ki so shranjeni v bazi.

5.1.1 Področja uporabe biometrične tehnologije

V širšem pogledu uporabo biometrije lahko razdelimo na tri področja (Brumnik, 2011):

- sodna medicina (preiskave, identifikacija trupel in določanje starševstva),
- civilna družba (identiteta državljana, distribuiranje socialnega prispevka, prečkanje mej in vozniški izpit) in
- komercialni nameni (bankomati, kreditne kartice in omejevanje dostopa).

Biometrijo pa lahko uporabljamo kot element verifikacije ali identifikacije uporabnika pri:

- dostopu do računalnika,

- dostopu do baz podatkov (prepustne kartice, novinarske kartice, izmenljive kartice, identifikacijske kartice),
- prehodu čez mejo,
- telefoniji,
- odklepanju do avtomobila, hiše,
- dostopu do zavarovanih območij (laboratoriji, vojaški objekti, tajne obveščevalne službe, tiskarne denarja, potnih listov),
- verifikaciji na potovanjih (letališča, potovalni čeki, vavčerji),
- verifikaciji pri poslovanju (bančne kartice, čeki, internetno poslovanje, pogodbe, obrazci) in za
- sledenju ter identifikaciji ljudi.

Vlogo biometrije pri varnostnih vprašanjih pa je mednarodno združenje biometrične industrije po terorističnih napadih l. 2001 videlo kot (Anžič, 2005):

- pomoč pripadnikom organom pregona v nevsiljivem posameznem izločanju potencialnih prestopnikov in iskanih kriminalcev na letališčih in drugih varnostno tveganih javnih območjih brez pridržanja ali kake druge nevšečnosti za nedolžne ljudi,
- avtentifikacijo identitete za promet preko mednarodnih mej, povečanje varnosti in ostale mejne formalnosti za legitimne potnike,
- zaščito občutljivih območij pred vdori nepooblaščenih s sredstvi efektivne fizične kontrole dostopa,
- preprečitvijo nepooblaščenega dostopa do občutljivih informacij in podatkov ter
- zaščito nacionalne komunikacijske infrastrukture.

5.2 *Biometrični sistemi*

Biometrija je veda o prepoznavanju identitete posameznika glede na njegove edinstvene lastnosti. Je proces zbiranja, proučevanja in shranjevanja podatkov o posameznikovih fizičnih lastnostih in vedenjskih značilnostih z namenom identifikacije in avtentikacije. Biometrične fizične značilnosti so prstni odtis, oblika obraza, geometrija roke, geometrija prsta, žilni sistem

roke, žilni sistem obraza, žilni sistem mrežnice, telesni vonj, vzorec šarenice, oblika linij prsta in linija gub na dlani. K vedenjskim značilnostim pa lahko štejemo strukturo glasu, statični podpis, dinamični podpis, značilno tipkanje itd. Odčitavanje biometričnih značilnosti je proces preverjanja ali dodeljevanja identitete in ravno v tem se identifikacija in verifikacija razlikujeta. Osebna identifikacija je proces, pri katerem naprava poveže določeno osebo z njeno identiteto. Pomeni, da osebi dodelimo identiteto glede na prej odvzete biometrične značilnosti iz baz podatkov. Verifikacija (avtentikacija) pa pomeni preverjanje, ali je oseba, za katero se predstavlja, res ta oseba.

Biometrični sistemi se sami po sebi zelo razlikujejo, če ne gledamo na tip značilnosti, ki jo pregledujemo. Pozorni moramo biti na naslednje dejavnike (Brumnik, 2011):

- delovanje: natančnost, hitrost, velikost, vpliv zunanjih dejavnikov,
- sprejemljivost: ali so ljudje, vključeni v takšen način preverjanja identitete, pripravljeni delovati s takšnim sistemom in
- ukanljivost: kako hitro lahko sistem prevaramo.

Pomemben dejavnik pri zagotavljanju varnosti je identifikacija osebe oz. preverjanje, ali je oseba res ta, za katero se izdaja. Preverjanje mora biti zanesljivo, hitro, ne sme posegati v telo in na voljo mora biti za primerno ceno. Zavedati se je treba, da razvoj ter implementacija biometričnih sistemov v procesu identifikacije ni cilj, pač pa pot. Neprestano se spreminjajo okolje, ranljivost informacijskih sistemov ter grožnje. V preteklosti je tovrstno preverjanje temeljilo na identifikacijski kartici, obesku, geslu, PIN (Personal Identification Number) kodi, podpisu ali celo na prepoznavanju osebe s strani varnostnika ali vratarja in večinoma je tako še danes. Toda vsi ti načini so glede na zahteve v sodobnem svetu postali nezanesljivi in zelo omejeni. Biometrija ponuja enostavno, zanesljivo in cenovno ugodno rešitev pri preverjanju identitete uporabnikov, ki jo lahko uporabimo tudi na nenadzorovanih in oddaljenih območjih. Prihodnost identifikacije je torej na strani biometrije.

5.3 *Učinkovitost biometričnih sistemov (HBSI)*

Učinkovitost se v kontekstu raziskave doktorske naloge nanaša tudi na lastnosti sistema, ki z razmeroma nizko kompleksnostjo dosega visoko hitrost identifikacije (Kukula in Proctor, 2009). Merilo za oceno učinkovitosti (Human-Biometric Sensor Interaction - HBSI) je percepcija ljudi glede hitrosti in učljivosti identifikacijskega sistema. Na razmerje med delovno uspešnostjo in kompleksnostjo biometričnega sistema vplivajo dejavniki: procesorska moč, izbira kriptoalgoritma, izbira tipa biometričnega senzorja, določitev deleža napačnih odobritev (False Acceptance Rate – FAR) in deleža napačnih zavrnitev (False Rejection Rate - FRR).

5.4 *Varnost in zasebnost osebnih podatkov pri uporabi biometrije*

Zasebnost je definirana kot: »Zahteva posameznika, da se sam odloči, kdaj, kako in v kakšni obliki bodo njegovi osebni podatki posredovani drugim« (Electronic Privacy Information Center, 2004). Da bi to dosegli, je treba razvijati dinamično in globalno strategijo, ki mora temeljiti na kulturi varnosti. Spoprijemanje z varnostnimi izzivi informacijske družbe zahteva tridelni pristop: posebne ukrepe za zagotavljanje varnosti omrežij in informacij, ustrezno zakonodajo o elektronskih komunikacijah (ki mora ustrezno obravnavati tudi vprašanja zasebnosti in varstva podatkov) in boj proti kibernetičnemu kriminalu. Te tri vidike bi bilo sicer do neke mere mogoče razvijati ločeno, vendar številne oblike medsebojne odvisnosti in prepletenosti govorijo v prid oblikovanja usklajene strategije in enotnega okvira za izvedbo in izboljšanje skladnega pristopa k varnosti omrežij in informacij (VOI). Čeprav sta zagotavljanje VOI in varovanje zasebnosti nedvomno izjemno pomembni, pa je obenem treba vsaj ohraniti že doseženo raven svobode izražanja oz. ta nikakor ne sme biti prizadeta. Zakonodajni okvir, ki obravnava področje elektronskih komunikacij, je treba dopolniti z določbami, povezanimi z varnostjo, v tistih delih, v katerih je trenutno veljavna zakonodaja šibka. Pri tem se je mogoče nasloniti na direktivo o zasebnosti in elektronskih komunikacijah (2002/58/ES), po kateri so ponudniki javno dostopnih komunikacijskih storitev dolžni zagotavljati varnost storitev,

ki jih ponujajo. Direktiva prav tako določa ukrepe zoper nezaželeno elektronsko pošto (spam) in vohunsko programsko opremo (spyware). Zasebnost osebnih podatkov ali informacijska zasebnost je zahteva posameznika, da podatki o njem samem (osebni podatki) niso avtomatično na razpolago drugim osebam in organizacijam. Kadar pa so posredovani drugim, mora imeti možnost kontrole podatkov in nadzora uporabe (Clarke, 2006).

Informacijska zasebnost so pravila za upravljanje zbirk osebnih podatkov, kot so finančne informacije, medicinske kartoteke in zapisi, ki jih upravljajo vladne agencije. Informacijska zasebnost je znana tudi kot »varovanje podatkov«. S filozofskega vidika naj bi bilo sodobno razumevanje in obravnavanje zasebnosti tako imenovana Moorova (1997) teorija nadzora, po kateri v dobi računalništva ni mogoče imeti popolnega nadzora nad lastnimi osebnimi podatki. Po teoriji nadzora Frieda (1970) je posameznikova zasebnost odvisna od nadzora nad njegovimi lastnimi informacijami. Teorija omejenega dostopa (restricted access theory) po Gavisonovi, definira zasebnost kot omejitev dostopa drugim do posameznikovih podatkov. Pri tem upošteva tajnost, anonimnost in samoto. Teorije Frieda in Gavisonove zagovarjajo stališče, da ohranja posameznik zasebnost v odnosu do drugih samo, če je situacija takšna, da je zaščiten pred motenjem, vmešavanjem in dostopom do informacij.

5.5 *Kriptologija kot tehnologija za izboljšanje zasebnosti v biometriji*

Biometrija ima z vidika posameznika nedvomno določene praktične prednosti. Kot vsaka druga tehnologija se lahko uporabi na način, ki je prijazen do posameznikove zasebnosti, lahko pa gre za občutne posege v zasebnost in učinek »velikega brata«. Praktične prednosti biometrije so praviloma vidne na prvi pogled, to pa ne velja za nekatere vidike, ki dokazujejo, da tudi biometrija ni vsemogočna in popolna. Biometrični ukrepi so po naravi stvari takšni, da pomenijo velik poseg v zasebnost in dostojanstvo posameznika, zato je treba vse pogoje za njihovo uporabo razlagati v luči njune zaščite in

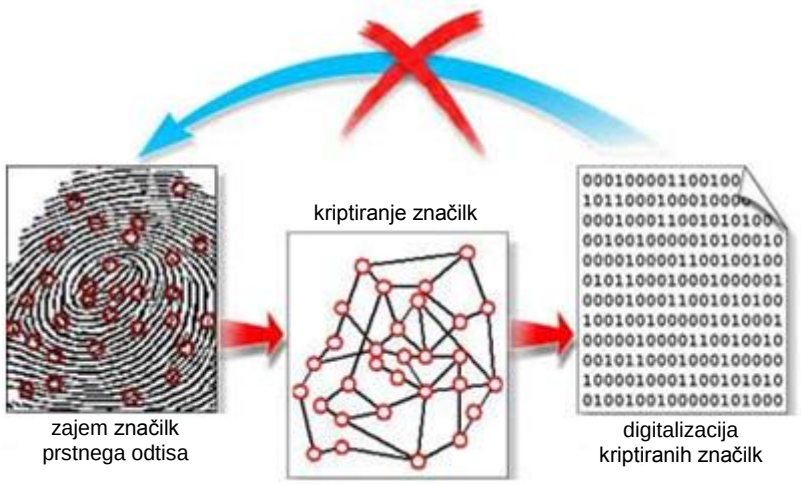
izhajati iz ZVOP-1-UPB1[18], ki določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. Potreba po varni izmenjavi podatkov je stara že tisočletja in se je skozi čas prilagajala metodam šifriranja v posameznem obdobju. Če je bilo šifriranje podatkov nekdaj predvsem potreba vojske in bank, se je krog uporabnikov danes močno povečal. Glavni razlog je razširjenost svetovnega spleta in vsega, kar ta omogoča. S tem se na eni strani pojavlja širok krog uporabnikov, ki želijo varno izmenjevati podatke, na drugi pa odprto javno omrežje s številnimi možnostmi zlorab. Rešitev je uporaba kriptografske opreme, ki se zaradi velikega povpraševanja uporabnikov vse bolj izpopolnjuje in standardizira.

Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). Uporabljata se še pojma enkripcija (šifriranje) in dekripcija (dešifriranje). Beseda kriptologija izvira iz grškega izraza »kryptos logos«, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil Browne l. 1658 (Kovačič, 2006). Sporočilo po nekem postopku (algoritmu, metodi) spremenimo v kriptirano sporočilo, pri čemer uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemo ključ (slika 7). Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila. Šifriranje podatkov je ključnega pomena za ohranitev tajnosti njihove vsebine. Osnovno sporočilo navadno imenujemo čistopis (cleartext, plaintext), zašifrirano pa šifropis ali tajnopis (kriptogram, ciphertext). Bolj kot so podatki tajni, močnejši mora biti šifrirni algoritem.

[18] Na podlagi 153. člena Poslovnika državnega zbora je Državni zbor Republike Slovenije na seji 27. septembra 2007 potrdil uradno prečiščeno besedilo Zakona o varstvu osebnih podatkov, ki obsega: a) Zakon o varstvu osebnih podatkov – ZVOP-1 (Uradni list RS, št. 86/04 z dne 5. 8. 2004), b) Zakon o informacijskem pooblaščencu – ZInfP (Uradni list RS, št. 113/05 z dne 16. 12. 2005), c) Zakon o spremembah in dopolnitvah Zakona o ustavnem sodišču – ZUstS-A (Uradni list RS, št. 51/07 z dne 8. 6. 2007) in d) Zakon o spremembah in dopolnitvah Zakona o varstvu osebnih podatkov – ZVOP-1A (Uradni list RS, št. 67/07 z dne 27. 7. 2007).

Biometrična aplikacija mora glede varnosti (Uludag in Jain, 2003) zagotoviti:

- zaupnost (ang. confidentiality),
- celovitost (ang. integrity),
- overjanje (ang. authentication),
- preprečevanje tajenja/prikrivanja (ang. nonrepudiation) in
- kontrolo dostopa (ang. access control).



Slika 7: Kriptografija značilk prstnega odtisa (Biometric Visions, 2008)

Najnovejše raziskave na tem področju potekajo v smeri kvantne kriptografije (Knil, 2010). Kvantna kriptografija je novejše temeljno znanstveno področje, ki uporablja principe kvantne fizike za doseganje absolutne varnosti pri prenosu informacije v telekomunikacijah. Začetki kvantne kriptografije segajo v leto 1984, ko sta Bennet in Brassard razvila protokol varne distribucije ključev BB84.

5.6 *Zahtevan varnostni nivo*

Posameznik ali družba, ki želita uporabljati biometrično tehnologijo, morata določiti zahtevan varnostni nivo delovanja takšnega sistema. Obstajajo nizek, srednji in visok varnostni nivo. Če zadostuje nizek ali srednji nivo, imamo na voljo vse vrste identifikacijskih tehnik, če pa je zahtevan visok nivo, smo omejeni na tiste tehnike, ki delujejo na osnovi unikatne telesne značilnosti (Liu in Silverman, 2001).

II EMPIRIČNI DEL

6 CILJI IN NAMEN RAZISKOVALNEGA DELA

Pomen našega dela je opraviti raziskavo med slovensko populacijo v smislu dojemanja in sprejemanja biometričnih identifikacijskih tehnologij, ki jih lahko uporabimo tudi za namene bojevanja proti terorizmu. Tehnologija mora biti prijazna za uporabnika, vendar ne sme posegati v osnovne človekove pravice (Jain, Bolle in Pankanti, 2002; Jain, 2010), hkrati pa mora služiti namenu odkrivanja storilcev kaznivih dejanj in teroristov.

Po svetu se je v preteklosti biometrija uveljavila kot antropološka znanstvena disciplina. Danes pa se vse bolj uporablja v kontekstu aplikativnih znanosti v boju proti terorizmu, kar bo obravnavala tudi naša empirična raziskava. V Združenih državah Amerike so se z aktivnostmi na tem področju začeli ukvarjati v šestdesetih letih prejšnjega stoletja, najprej sicer v povezavi s forenzičnimi vedami. Danes se pomena biometrije čedalje bolj zavedamo tudi na območju Evropske unije (EU), na kar med drugim kaže tehnični dokument EUR 21585 EN, ki ga je pripravil JRC (2005) za Evropski parlament. S težnjo po zagotovitvi varnosti s kar najmanjšim vplivom na svoboščine državljanov, bomo v raziskavi osvetlili problematiko varovanja osebnih podatkov v identifikacijskih postopkih. Pri tem pa je nujno zavedanje, da se že dotikamo tudi vprašanja družbene sprejemljivosti biometrične tehnologije (JRC, 2005). Metode biometrične identifikacije omogočajo zbiranje osebnih podatkov, ki jih nato obdelamo z namensko IKT, kar omogoča višji in poglobljen nivo ugotavljanja morebitnih varnostnih anomalij. V odvisnosti od varnostnih dejavnikov (varnostne ocene tveganja) bomo raziskali biometrične metode oz. sisteme biometričnih kombinacij pristopne kontrole, v smislu optimalne ravni ustrezanja varnosti varovanega objekta ali subjekta (parametri varnosti - družbena sprejemljivost). Predvidevamo, da je družbena sprejemljivost biometričnega sistema v prvi vrsti odvisna od zaupanja v takšno tehnologijo in nadalje, od zmožnosti uporabe takšnega sistema (njegove učinkovitosti). Eden ključnih mehanizmov v boju proti terorizmu tako postaja uporaba metod za nadzor oseb (Gams, 2001). ZDA so zato sprejele vrsto zakonov, ki omogočajo

obširnejše zbiranje (osebnih) podatkov in elektronski nadzor. Zaradi odvisnosti družbe od IKT, lahko v prihodnosti kibernetski terorizem, predstavlja najsodobnejšo in tehnološko najbolj sofisticirano obliko terorističnega delovanja (Chen, Reid in Sinai, 2008).

6.1 *Opredelitev problema*

Problematika sistemov za identifikacijo oseb, zadnja leta pridobiva pomen tako v Sloveniji kot v EU ter drugod po svetu. Gre za strateško vprašanje tako Slovenije kot geopolitičnih povezav EU in NATO v katere je vključena, saj je vprašanje varnosti in potencialnih terorističnih napadov čedalje bolj v ospredju. V okviru raziskave bomo preučili percepcijo slovenske družbe do terorizma, skozi pripravljenost za odpovedovanje osebnim svoboščinam. Osebne svoboščine, ki bodo v raziskavi identificirane skozi varnost osebnih podatkov, pa se moramo državljani v določenih situacijah za zagotavljanje varnosti, tudi odpovedati. Zanimajo nas torej dejavniki, ki so za slovensko družbo pomembni, da bi se ta bila pripravljena odpovedati neki določeni stopnji osebnih svoboščin. Neposredna povezava osebnih svoboščin s sprejemljivostjo nadzornih in identifikacijskih tehnologij bo raziskana v disertaciji. Na osnovi dejavnikov, ki jih bomo raziskali skozi raziskavo, bomo konstruirali odločitveni model sprejemljivosti identifikacijske tehnologije.

6.2 *Cilji in namen raziskovalnega dela*

Raziskava vsebuje pregled sodobnih elektronskih tehnologij v obveščevalni dejavnosti. Hkrati z raziskavo ocenjujemo aplikativno vrednost uporabe (učinkovitost) identifikacijskih tehnologij. Z raziskavo med drugim želimo doseči tudi pravilnost obravnave besede kibernetski terorizem, glede na kritično obravnavo samega obstoja pojava. IKT bomo raziskali kot orodje v rokah teroristov in v smeri njene uporabe v boju proti terorizmu, še zlasti proti specifični pojavni obliki, informacijskega terorizma - kraji identitete. Večkrat je rezultat pretirane domišljije s strani medijev in državnih organov, preplah v javnosti. Nepoznavanje osnovnih zakonitosti veljavnih znotraj informacijskega sveta, rezultira v nekem konceptu kibernetskega terorizma, ki pa je za nekoga lahko tudi samo fantazijski konstrukt. Eden od rezultatov

bo preslikava obstoječega koncepta terorizma, v digitalno sfero računalniške tehnologije, ki ima izredno kompleksno naravo. Schmitz je s pomočjo funkcijske dekompozicije opredelil štiri nivoje sistemov kritične infrastrukture: fizični, kibernetski, organizacijski in strateško-poslovni (Schmitz, 2003).

Raziskava v okviru doktorskega dela obravnava problematiko uporabe biometričnih identifikacijskih sistemov za potrjevanje identitete oseb skozi prizmo pravice do zasebnosti. Predstavljene so nadzorne tehnologije, pripadajoča zakonodaja ter družbena sprejemljivost biometričnih identifikacijskih sistemov ter principov. Tovrstni sistemi kontrole pristopa ter identifikacije so namenjeni za uporabo kot varnostni mehanizem pri vstopu v določen realen ali virtualen prostor, lahko pa tudi pri vstopu na ozemlje neke države, ko je treba potrditi avtentičnost ali identificirati osebo. Sistem preprečuje nepooblaščenim osebam vstop v varovane prostore, hkrati pa omogoča natančno evidenco gibanja posameznikov po varovanem objektu, kompleksu ali območju države.

Osrednji del raziskave podrobneje opisuje problematiko informacijskega terorizma in z njim povezanih informacijsko-identifikacijskih tehnologij. Biometrija kot pomemben del IKT, lahko kriminalcem in teroristom omogoča uspešno izogibanje zakonu, preko kraje identitete (Biegelman, 2009; Siegel, 2009; Andress, Winterfeld in Rogers, 2011; Vacca, 2003).

Biometrija pa je lahko kot del IKT, v največjo pomoč pri iskanju storilcev kriminalnih in terorističnih dejanj ter hkrati nudi pomembne logistične informacije glede pozicije in gibanja posameznih operativcev (Boyd, 2009; Woodward, Webb, Newton, Bradley in Rubenson, 2001).

Še posebej je ugotavljanje identitete oteženo pri kriminalnih in terorističnih aktivnostih v kibernetskem prostoru, kjer se identiteta lahko skrije na takšen ali drugačen način, zato bomo tej tematiki posvetili del naše študije (Janczewski, 2005; Kumar, Srivastava in Lazarević, 2005). Ob vse večjem

uvajanju biometričnih tehnologij na področju bojevanja proti terorizmu, bomo raziskali parametre družbene sprejemljivosti biometričnega sistema v identifikacijskem procesu. Namen raziskave je opraviti pregled relevantne literature v smeri terorizma, biometrije, zasebnosti ter kibernetske kriminalitete in raziskati raven sprejemljivosti biometričnega sistema glede na različne varnostne stopnje ali zahteve po identifikaciji, predvsem v zvezi z varnostnimi tveganji. V primerjalni študiji sprejemljivosti identifikacijskih sistemov bomo relevantne parametre s pomočjo spletnega anketiranja raziskali na območju Slovenije, za biometrične sisteme, ki se poleg kartičnih in ostalih konvencionalnih identifikacijskih sistemov, v tem času največ uporabljajo.

Povečan obseg kriminalitete in teroristični napadi so v družbi okrepili zavest o pomenu zagotavljanja varnosti oseb, (realnega in virtualnega) prostora ter informacij oz. kritične infrastrukture (CRS, 2003). Bistveno je zagotoviti učinkovit nadzor vstopa in gibanja v varovanih prostorih. Zahteve po nadzornih sistemih postajajo vse pogostejše in se uveljavljajo na območjih, kot so mejni prehodi, letališča ter pomembni turistični in poslovni objekti. Na področju osebne identifikacije so čedalje bolj pomembne in razširjene biometrične identifikacijske metode, ki omogočajo višjo raven varnosti pri nadzoru oseb (Dorizzi, 2006). Takšni prijemi lahko zagotovijo večjo stopnjo osebne varnosti, učinkovitejše izvajanje osebnih pravic ter varnejšo državno in evropsko mejo. Teroristom je mogoče slediti in jih odkrivati s pomočjo biometrije (Kirkpatrick, 2001; Boyd, 2009). Pri tem je potrebno upoštevati, da varnostne situacije niso vedno enake, tudi znotraj istega sistema varovanja ne. Možen odgovor na potrebna prilagajanja posameznim varnostnim situacijam je kombiniranje različnih identifikacijskih metod. Izbira, usklajevanje in uravnoteženje varnostnih prijemov, vključno z metodo identifikacije, so bistveni, saj omogočajo ustrezno prilagajanje varnostnim potrebam. Kombinirane identifikacijske sisteme je bistveno težje zaobiti kot enega samega, ne glede na to, da so nekateri sistemi izredno zanesljivi že sami po sebi (JRC, 2005).

Študija družbene sprejemljivosti v zvezi s percepcijo varnosti oz. zlorabe osebnih podatkov v primeru biometrične identifikacije, omogoča vpogled v stanje slovenskega prostora, glede poznavanja biometričnih identifikacijskih tehnologij ter njene razširjenosti glede uporabe. Za ugotovitev družbene sprejemljivosti biometrične tehnologije, bomo v prvi vrsti določili:

- stopnjo poznavanja tehnologije,
- stopnjo njene uporabe in
- pogoje pod katerimi se je slovenska populacija pripravljena odreči neki stopnji zasebnosti, za neko določeno stopnjo izboljšanja varnosti.

S statističnimi metodami lahko potem nadalje ustrezno določimo parametre (dejavnike), ki najbolj vplivajo na družbeno sprejemljivost biometrične tehnologije in raziskovalne parametre.

6.3 *Opredelitev hipotez*

Glavni namen raziskave je bil testirati naslednje hipoteze:

Hipoteza 1: Varnost osebnih podatkov ne vpliva znatno na oceno sprejemljivosti uporabe sistemov množičnega nadzora (identifikacije) v varnostnih sistemih.

Hipoteza 2: Sprejemljivost nadzornih tehnologij se viša z višanjem starostne stopnje in niža z višanjem izobrazbene stopnje anketirancev.

Hipoteza 3: Biometrični sistemi za množični nadzor v procesih identifikacije so učinkovitejši kot sedaj poznani alternativni (kartični) sistemi.

6.4 *Metode, tehnike in orodja uporabljena v raziskovanju*

V raziskavi so uporabljene naslednje metode in tehnike dela:

- eksplorativni pristop, zaradi interdisciplinarnosti tudi multimetodski,
- pregled znanstvene in strokovne literature, analiz in obstoječih raziskav na področju (biometričnih) identifikacijskih tehnologij, terorizma in zasebnosti,

- anketiranje s pet stopenjsko Likertovo lestvico z več sklopi odprtih in zaprtih vprašanj,
- empirično testiranje hipotez,
- analitično raziskovanje povezanosti dejavnikov sprejemljivosti in njihovega vpliva na uspešnost implementacije ter uporabe biometričnega sistema v namene preprečevanja kriminalitete in terorizma in
- analiza vgrajenosti demografskih dejavnikov in njihove povezanosti z družbeno sprejemljivostjo biometričnega sistema.

Zbiranje podatkov smo izvajali preko interneta s programskim orodjem Fluid Survey. Pri statistični obdelavi in oblikovanju zaključkov smo uporabili orodja programskega paketa SPSS za statistično obdelavo in določanje ocen družbene sprejemljivosti biometrične tehnologije. Glede na cilj raziskave, to je izboljšan parametrični raziskovalni model interdisciplinarnega raziskovanja percepcije terorizma, biometrije in zasebnosti, sledi optimizacija z vključevanjem dinamičnih spremenljivk, do katerih lahko pride v procesu identifikacije. Optimiranje poteka v smeri minimiranja posega v zasebnost uporabnikov. Sočasno bomo empirično obdelovali podatke in razvijali statistični model za določanje sprejemljivosti biometričnih sistemov.

Predvidena orodja empiričnega raziskovanja so:

- programski paket za statistično analizo (SPSS) in za določanje ocen karakteristik družbene sprejemljivosti biometrične tehnologije,
- teorija zasebnosti, nadzornih sistemov in terorizma,
- vprašalnik na osnovi pet stopenjske Likertove lestvice,
- panel anketirancev pripravljen v skladu z mednarodnim ISO standardom,
- internet, kot orodje za anketiranje anketirancev,
- korelacijska in faktorska analiza vgrajenih dejavnikov družbene sprejemljivosti biometrične tehnologije,
- multipla regresijska analiza,
- t-test, analiza variance (ANOVA) ter
- Bonferroni post-hoc testi.

6.5 *Omejitve*

Raziskava se loteva ugotavljanja prepoznavnosti in sprejemljivosti določenih tipov biometričnih identifikacijskih sistemov (biometrija na osnovi prepoznave prstnega odtisa, oblike roke, podpisa, ožilja roke, šarenice, obraza s pomočjo kamere, šarenice, DNK in glasu). Ostale nekonvencionalne biometrične metodologije (biometrija na osnovi prepoznave ušesa, nohtov, ozobja, hoje, porologije, itd.), ki zajemajo manjši tržni delež uporabe (International Biometric Group, 2009) v tej raziskavi ne bodo obravnavane.

V raziskavi bomo upoštevali populacijo anketirancev na območju celotne Slovenije v starosti od 18 do 59 let, ki imajo dostop do interneta, ga tudi znajo uporabljati ter tako izpolnjujejo osnovni pogoj računalniške pismenosti oz. poznavanja informacijske tehnologije.

7 KVANTITATIVNA RAZISKAVA SPREJEMLJIVOSTI BIOMETRIJE

V raziskavi smo ocenili dejavnike sprejemljivosti biometričnih identifikacijskih sistemov. Podatke za oceno karakteristik družbene sprejemljivosti biometrične identifikacije smo pridobili s pomočjo anketiranja primerno velikega vzorca anketirancev v Sloveniji.

7.1 *Osnovne značilnosti in postopek raziskave*

7.1.1 Oblikovanje merskega inštrumenta

Za potrebe raziskovanja identifikacijskih sistemov in percepcije splošne javnosti glede terorizma, smo na podlagi teoretičnega ozadja, merskih inštrumentov oblikovali anketni vprašalnik. Udeleženci raziskave so bili izprašani z anketnim vprašalnikom. Vprašalnik smo prilagodili potrebam raziskave slovenskega prostora in vključili tudi demografska vprašanja (izobrazba, zaposlitveni status, regija, politična opredelitev). Pred izpolnjevanjem so bili seznanjeni z namenom raziskave in navodili za izpolnjevanje anketnega vprašalnika. Da smo zadostili potrebam preverjanja vseh treh hipotez, smo na podlagi prejetega teoretičnega ozadja pripravili tudi dodatna vprašanja. Končni vprašalnik je tako sestavljen iz prilagojenih merskih inštrumentov, ki so bili sestavljeni za potrebe raziskave na podlagi ustreznega teoretičnega ozadja. Anketa se je izpolnjevala v elektronski obliki.

Anketni vprašalnik je zajel naslednje podatke:

- splošno poznavanje (biometričnih) identifikacijskih tehnologij
- sprejemljivost identifikacijskih tehnologij in varnost osebnih podatkov (osrednji del vprašalnika) ter
- splošne socialno demografske podatke (spol, starost, izobrazba, regija in poklic).

7.1.2 Pilotna raziskava

Ustreznost (razumljivost besedila, težavnost vprašalnika itd.) merskega inštrumenta smo preverili s pilotnim testiranjem. K reševanju ankete smo

povabili ljudi različnih profilov (spol, starost, zaposlitveni status, izobrazba). Anketni vprašalnik je sestavljen iz dveh delov: iz vprašanj, ki se nanašajo na identifikacijske sisteme in iz sociodemografskih vprašanj. Na osnovi rezultatov pilotskega testiranja strukture vprašalnika smo izboljšali vprašanja (Kobeja, 2002). Izvedba pilotskega testiranja vprašanj nam je bila v pomoč tudi pri določitvi časovne norme za izvedbo ankete in pri potrditvi razumljivosti vprašanj.

7.1.3 Potrditev končnega vprašalnika

Anketni vprašalnik je osnova empiričnega dela raziskave in za kasnejšo analizo rezultatov, zato mora biti sistematično strukturiran, pridobljeni podatki pa morajo biti nadzorovani. Preden začnemo z anketiranjem, moramo opraviti pripravljalne postopke, med katere glede na pomembnost sodita vzorčenje in izoblikovanje vprašalnika (Toš, 1988).

Vprašalnik smo zastavili v pet sklopov tako, da v začetku preverimo poznavanje identifikacijske tehnologije anketirancev. Na večino vprašanj, vprašani odgovarja tako, da izbira med ponujenimi odgovori. Osrednji del vprašalnika so sestavljala vprašanja zaprtega tipa, ki se nanašajo na dejavnike sprejemljivosti identifikacijske tehnologije v družbi. Bila so razdeljena na tri sklope in sicer: dejavniki sprejemljivosti biometrične tehnologije za različne situacije (od vsakdanjih življenjskih situacij za primere identifikacije, do terorističnih napadov itd.), dejavniki varnosti osebnih podatkov in dejavniki, ki se nanašajo na percepcijo terorizma. Vprašanja v tem delu so zaprtega tipa, Likertova lestvica ocen odgovorov je zastavljena od vrednosti 1 do vrednosti 5. Ocena 1 pomeni, da ima dejavnik percepcije terorizma in kriminalitete neznaten vpliv na določitve kriterijev sprejemljivosti biometrične tehnologije v družbi, ocena 5 pa, da ima dejavnik percepcije terorizma zelo velik vpliv na kriterije sprejemljivosti biometrične tehnologije. V zadnjem delu vprašalnika pa so nas zanimali socialno demografski podatki udeležencev v raziskavi.

Po pilotni raziskavi smo na podlagi odziva testnih anketirancev vprašalnik ustrezno popravili, uredili in tudi potrdili. Večina sprememb se je nanašala na opise dodatnih razlag vprašanj, da so bila le-ta bolj razumljiva za splošno javnost. Vprašalnik smo korigirali, glede na pripombe anketirancev in na cilje merjenih dejavnikov in vsebuje 22 vprašanj s podsklopi vprašanj in trditev.

7.1.4 Preverjanje zanesljivosti anketnega vprašalnika

Zanesljivost merjenja je stopnja, do katere omogoča raziskava v zaporednih merjenjih in enakih okoliščinah pridobivanje enakih rezultatov (Carmines in Zeller, 1979). Za namen preverjanja zanesljivosti anketnega vprašalnika smo uporabilo statistiko Cronbach alfa, ki je namenjena ugotavljanju, kako dobro skupina spremenljivk ali postavk meri posamezno enodimenzionalno latentno sestavo. V primeru več razsežnostne strukture je vrednost koeficienta alfa nizka. V primeru, da so korelacije med postavkami nizke, je tudi vrednost Cronbach alfe nizka. V primeru, da se povprečna medsebojna korelacija povečuje, se povečuje tudi alfa. Ko so medsebojne korelacije postavk visoke, je to dokaz, da merijo isti osnovni problem oz. predmet. Sklepamo, da je zanesljivost dobra oz. visoka. V teoriji je ocenjeno, da so vrednosti alfe, ki se gibljejo okoli 0,60 še sprejemljive (Pahor, 2010).

Preračunane vrednosti koeficienta Cronbach alfa, za postavke v okviru posameznih sklopov vprašalnika in tudi posamično za vsa vprašanja (tabela 4), ki smo jih uporabili v raziskavi kažejo na vrednosti nad 0,6 (0,626). Na osnovi teh ugotovitev podamo sklep, da je zanesljivost vprašalnika dobra.

Tabela 4: Vrednosti koeficienta Cronbach alfa

Spremenljivka	Lestvica povp. (izključena spremenlj.)	Spremenlj. lestvice (izključena spremenlj.)	Popravljena spremenlj.-celotna korelacija	Cronbach's Alpha (izključena spremenlj.)
Registracija delovnega časa zaposlenih.	2149,35	423,692	,000	,627
Preverjanje identitete zaposlenih pred vstopom v zavarovan arhiv ali	2149,35	423,692	,000	,627

kakšno drugo zavarovano delovno območje.				
Preverjanje identitete pred vstopom na letalo.	2149,35	423,692	,000	,627
Preverjanje identitete potnikov pri vstopu v tujo državo.	2149,35	423,692	,000	,627
Preverjanje identitete obiskovalcev podjetji, javnih ali vladnih ustanov.	2149,35	423,692	,000	,627
Preverjanje identitete obiskovalcev podjetji, javnih ali vladnih ustanov pri vstopu na območje označeno z znakom »samo za zaposlene«.	2149,35	423,692	,000	,627
Prepoznava prstnega odtisa.	2146,17	419,241	,121	,624
Prepoznava oblike roke.	2147,96	409,680	,366	,615
Prepoznava podpisa.	2146,35	418,510	,118	,624
Prepoznava ožilja roke.	2148,30	411,676	,265	,618
Prepoznava obraza s pomočjo kamere.	2146,48	410,443	,355	,616
Prepoznava šarenice s pogledom v skener.	2147,00	410,727	,301	,617
Prepoznava DNK: analiza vzorca krvi, las itd.	2146,87	413,209	,223	,619
Prepoznava glasu.	2146,91	400,538	,532	,607
Izkušnje biometrični sistemi	2149,35	423,692	,000	,627
Izkušnje v preteklosti	2148,30	424,767	-,058	,635
če se uporablja biometrična identifikacija, se mora okrepiti varstvo zasebnosti in pošteno ravnanje s podatki.	2145,61	429,340	-,314	,632
Organizacija, ki zbira biometrične podatke, mora uporabnike jasno	2145,52	424,897	-,085	,628

obvestiti o potrebnosti in načinu zbiranja in obdelave podatkov.				
Organizacije lahko biometrične podatke zbirajo zgolj na način, ki je bil uporabniku predhodno opisan.	2145,57	426,984	-,199	,630
Skrivno zbiranje biometričnih podatkov ni dovoljeno.	2145,39	424,522	-,102	,628
Biometričnih podatkov se ne sme povezovati z drugimi osebnimi podatki.	2146,00	422,091	,010	,628
Zgoraj naštete trditve se lahko kršijo, če gre za interese državne varnosti.	2147,52	393,897	,443	,603
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	2147,22	400,360	,374	,609
Kot sredstvo za pomoč pri preprečevanju težjih kaznivih dejanj.	2145,78	422,996	,000	,628
Pri preverjanju identitete kupca orožja v bazi pravnomočno obsojenih kriminalcev.	2145,78	418,087	,122	,624
Za preverjanje identitete pri plačilu s kreditno kartico.	2146,74	398,292	,485	,606
Pri dvigovanju denarja na bankomatu.	2146,78	399,269	,448	,607
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	2146,61	412,522	,197	,620
Pri preverjanju preteklosti posameznika.	2147,26	403,656	,294	,613
Pri vpisu v šolo.	2147,87	380,573	,810	,587

Pri kontroli potnih listov.	2146,30	410,221	,505	,615
V potnih listih.	2146,22	403,905	,512	,610
Ob vstopu v državne stavbe.	2146,78	384,542	,673	,592
Na letališčih pri prijavi na let.	2146,48	394,988	,544	,602
Na vozniškem dovoljenju.	2147,30	393,130	,562	,601
Pri izposoji avtomobila (rent a car).	2147,52	400,715	,408	,609
Zaupanje - državni organi	2147,39	411,794	,160	,621
Zaupanje - privatne organizacije	2148,43	393,075	,685	,599
Varnost osebnih podatkov	2145,52	424,261	-,045	,628
Pri plačilu s plačilnimi karticami trgovcev (Pika, Magna, ipd.).	2146,04	420,771	,060	,626
S karticami zvestobe (Mercator, Petrol, Spar, Tuš, ipd.).	2146,61	445,158	-,460	,649
Pri registraciji v spletne trgovine (mimovrste, enaa, eventim ipd.).	2146,04	416,771	,172	,622
Pri naročanju telekomunikacijskih storitev (mobilna telefonija, stacionarna telefonija, internet).	2146,22	415,996	,161	,622
S pomočjo zdravstvenih kartic in zdravstvenih kartonov.	2145,74	424,838	-,062	,629
Za varovanje zaupnih podatkov, ki jih pri svojem delu zbirajo kriminalisti in policija.	2146,39	414,976	,208	,621
Pri kriminalističnem delu na mestih zločina, če so podatki zbrani na mestu zločina primerjajo z bazami	2146,09	416,538	,215	,621

podatkov pravnomočno obsojenih zločincev.				
Za izdelavo baz s podatki o resnih kriminalcih in zločincih.	2145,78	423,996	-,028	,628
Pri delu prometne policije, če policist ustavi prometnega prekrškarja in hkrati primerja njegove podatke s podatki o obsojencih na begu.	2146,78	413,996	,150	,622
Terorizem	2147,22	387,996	,468	,599
Primerjava sistemov	2148,57	419,893	,209	,624
Letnica rojstva	182,13	285,028	,087	,822
[Spol]	2149,04	421,680	,093	,625
[Šola]	2146,70	426,221	-,110	,630
[Izkušnje1] Sistemi preverjanja dostopa.	2148,74	422,929	,025	,627
[Aktivnost]	2146,48	425,079	-,058	,633
Klasični (kartični) sistemi	2147,09	411,719	,231	,618
Biometrični sistemi	2146,43	413,621	,224	,620

7.1.5 Vzorčenje

Izbira vzorca je potekala naključno s pomočjo programske opreme (random selection), pri čemer se določene kvote definirajo vnaprej. Kvote se določijo na podlagi lastnosti in strukture celotne slovenske populacije (npr. starost, spol, izobrazba) oziroma glede na lastnosti internetno aktivne populacije ali ciljne skupine, ki jo je določil naročnik, v našem primeru 500 oseb v starostnem razponu 18-59 let.

7.1.6 Uteževanje vzorca

Kljub načrtni izbiri kvot prihaja pri anketiranju vedno do določenih odstopanj glede na idealen vzorec izbrane realne populacije (18-59 let), zato rezultate po končanem anketiranju utežimo (*ponderiramo*). Podatke smo utežili na podlagi podatkov SURS po spolu, starosti in regiji. V bazi sta na voljo dve uteži, neporezana (št. 1) in porezana (št. 2). Porezana je pripravljena na

intervale in zato ne popači strukture. Ker je bil izhodiščni vzorec sorazmerno dober, so razlike med porezano in neporezano utežjo minimalne, vseeno pa pri statistični obdelavi uporabimo porezane uteži.

7.1.7 Anketiranje

Anketiranje je potekalo v času med 3. 8. 2011 in 16. 8. 2011. Anketirance smo k reševanju povabili s povabilom preko spletnega portala www.fluidsurveys.si. Sodelovanje v anketi je bilo prostovoljno, vsem anketirancem pa smo zagotovili anonimnost. Vseh sodelujočih udeležencev-anketirancev je bilo 551. V celoti je bilo rešenih 510 anket ali 99,80 %. Izločili smo 10 anket ali 1,96 % in sicer vse tiste, ki so končali z reševanjem v manj kot 4 minutah (8 anket), z neustrezno letnico rojstva (1 anketa) in podvojenim vnosom glede na povabilo k anketi (1 anketa). V bazi je bilo tako pred uteževanjem 500 anket. Podrobni datumi in časi reševanja posameznega udeleženca so na voljo v bazi. Spletni vprašalnik je vseboval tudi spremni dopis s katerim smo anketirancem obrazložili namen raziskave, navodila, čas izvedbe ter zagotovilo za varnost ter anonimnosti podatkov.

Ker smo podatke in informacije zbirali s spletnim vprašalnikom, so bili po koncu anketiranja izpolnjeni vprašalniki shranjeni v ustrezni elektronski bazi podatkov. V Excelu, smo izvedli pripravo podatkov in jih uvozili v program SPSS (Statistical Package for the Social Sciences) za statistično obdelavo, s pomočjo katerega smo kasneje izvedli analize in obdelave podatkov.

7.1.8 Statistična analiza podatkov

Statistična analiza podatkov se je izvedla s korelacijsko in regresijsko metodo ter enosmerno analizo variance (ANOVA) in t-test kjer smo iskali vpliv in statistično pomembno povezanost posameznih dejavnikov v hipotezah in jih tudi merili.

7.2 *Osnovne informacije o spletnem panelu*

Spletni panel predstavljajo internetno aktivne osebe, ki so pripravljene sodelovati v spletnih raziskavah. Trud članov panela se kompenzira oz.

finančno nagradi. Spletni panel, ki je bil uporabljen za raziskavo, je ISO-certificiran (certifikat ISO 26362). Panel je enakomerno sestavljen tako iz aktivno kot tudi pasivno rekrutiranih uporabnikov interneta. EU bazen oseb, ki so pripravljene sodelovati v raziskavah, je v času izvajanja raziskave presegel mejo 250.000 članov. Velikost panela zagotavlja, da ne prihaja do sistematičnih pristranskosti, ki bi lahko bile posledica izbranega medija anketiranja oz. anketiranja istih, rednih uporabnikov.

7.2.1 Sistem za spletno anketiranje

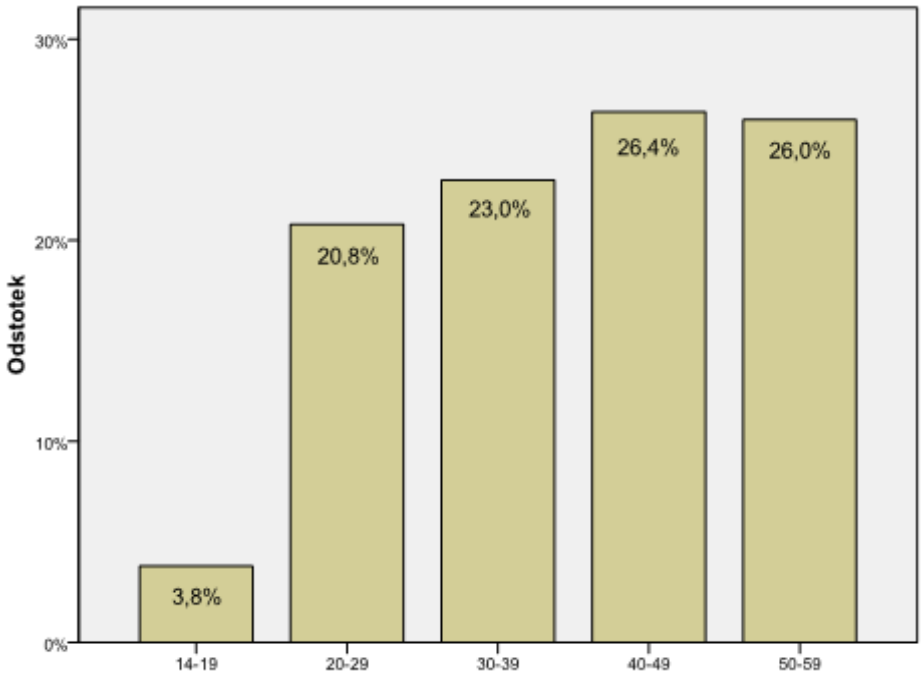
Raziskava je bila izvedena s pomočjo orodja za spletno anketiranje FluidSurveys v slovenščini (www.fluidsurveys.si). Slovensko orodje trenutno v Sloveniji uporablja več kot 1200 podjetji in posameznikov, angleško različico po svetu pa več kot milijon uporabnikov. Anketni vprašalnik smo pripravili v elektronski obliki, kar pomeni, da udeleženci raziskave dobijo spletno (URL) povezavo do spletnega vprašalnika. Povezavo smo dostavili udeležencem spletnega panela. Udeleženci so do ankete lahko dostopali 24 ur na dan iz katerekoli lokacije, kjer je omogočen dostop do interneta (npr. iz službenega ali domačega računalnika, iz pametnega telefona itd.).

7.3 *Reprezentativnost vzorca in demografske značilnosti*

Vzorec je reprezentativen za slovensko populacijo 18-59 let po starosti, kontroliran pa je tudi po izobrazbi, spolu in regijah. V naslednjih tabelah so prikazane frekvence in odstotki demografskih značilnosti anketirancev, ki so sodelovali v anketi o sprejemljivosti biometrije in percepciji terorizma prebivalcev v Sloveniji. Demografski del vprašalnika obsega pet vprašanj.

7.3.1 Letnica rojstva

Anketiranci so bili razdeljeni v pet starostnih razredov (slika 8). V vzorcu največjo frekvenco zasledimo v razredu od 40 do 49 let (26,4 %), kar tudi sovpada s podatkom celotne populacije. Najnižjo frekvenco (3,8 %) pa tvorijo anketiranci v razredu od 14 do 19 let.



Slika 8: Starostna struktura anketirancev

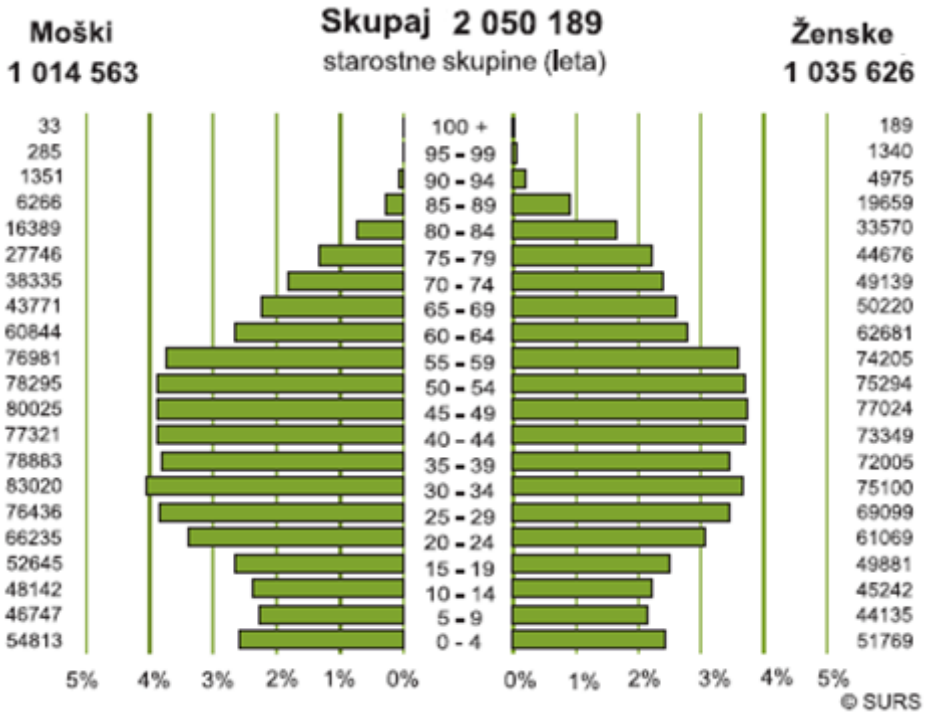
7.3.2 Spol

Iz tabele 5 je razvidno, da je v raziskavi sodelovalo 256 oziroma 51,2 % anketirancev ženskega spola ter 244 oziroma 48,8 % anketirancev moškega spola, kar sovpada demografski strukturi Slovenije (50,5 % ženskega spola in 49,5 % moškega spola; za leto 2010)

Tabela 5: Frekvenca demografskih kazalcev glede na spol

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Moški	244	48,8	48,8	48,8
	Ženski	256	51,2	51,2	100,0
	Skupaj	500	100,0	100,0	

Slika 14 prikazuje starostno strukturo prebivalcev po petletnih skupinah ter spolu v Republiki Sloveniji na dan 1. 1. 2011 (Statistični urad Republike Slovenije [SURS], 2011).



Slika 14: Prebivalstvo RS po petletnih starostnih skupinah in spolu,1. januar 2011 (SURS, 2011)

7.3.3 Izobrazba

Iz tabele 6 je razvidna demografska struktura po izobrazbi.

Tabela 6: Frekvenca demografskih kazalcev glede na izobrazbo

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Nedokončana ali dokončana osnovna šola.	44	8,8	8,8	8,8
	Dveletna ali triletna poklicna srednja šola.	102	20,4	20,4	29,2
	Štiriletna ali petletna srednja šola.	211	42,2	42,2	71,4
	Visokošolski ali univerzitetni študij.	131	26,2	26,2	97,6
	Specializacija, magisterij, doktorat.	12	2,4	2,4	100,0
	Skupaj	500	100,0	100,0	

211 anketirancev, ki so sodelovali v anketi, oziroma 42,2 % ima dokončano štiriletno ali petletno srednjo šolo, 131 oziroma 26,2 % anketirancev ima

visokošolsko ali univerzitetno izobrazbo. 102 oziroma 20,4 % anketirancev ima dokončano dveletno ali triletno poklicno srednjo šolo ter 44 anketirancev oziroma 8,8 % ima nedokončano ali dokončano osnovno šolo. 12 oziroma 2,4 % anketirancev ima dokončano specializacijo, magisterij oziroma doktorat.

7.3.4 Področje dela

S tabelo 7 želimo prikazati, s katerimi aktivnostmi lahko anketiranci najbolje opišejo organizacijo, v kateri so zaposleni. 143 oziroma 28,6 % anketirancev umesti svojo zaposlitev v ostale gospodarske družbe. 94 anketirancev oziroma 18,8 %, jih je zaposleno v javnem sektorju, upravi ali šolstvu. 32 oziroma 6,4 % anketirancev opiše za glavno aktivnost podjetja kjer so zaposleni, razvoj, proizvodnjo ali dobavitelj informacijske tehnologije. 15 oziroma 3,0 % anketirancev je opisalo aktivnosti svoje organizacije kot razvoj, proizvodnjo ali dobavitelj varnostne tehnologije. 93 anketirancev oziroma 18,6 % se je uvrstilo v skupino ostalo ter 123 oziroma 24,6 % se je opredelilo kot nezaposlen.

Tabela 7: Frekvenca anketirancev glede na področje dela

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Razvoj, proizvodnja ali dobavitelj informacijske tehnologije	32	6,4	6,4	6,4
	Razvoj, proizvodnja ali dobavitelj varnostne tehnologije.	15	3,0	3,0	9,4
	Ostale gospodarske družbe.	143	28,6	28,6	38,0
	Javni sektor/uprava/šolstvo.	94	18,8	18,8	56,8
	Ostalo.	93	18,6	18,6	75,4
	Nisem zaposlen/a.	123	24,6	24,6	100,0
	Skupaj	500	100,0	100,0	

7.3.5 Regija

V tabeli 8 je prikazana demografska struktura anketirancev glede na regijo prebivanja.

Tabela 8: Frekvenca anketirancev glede na regijo

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Pomurska regija	33	6,6	6,6	6,6
	Podravska regija	80	16,0	16,0	22,6
	Koroška regija	21	4,2	4,2	26,8
	Savinjska regija	56	11,2	11,2	38,0
	Zasavska regija	14	2,8	2,8	40,8
	Spodnjeposavska regija	11	2,2	2,2	43,0
	Jugovzhodna Slovenija	31	6,2	6,2	49,2
	Osrednjeslovenska regija	138	27,6	27,6	76,8
	Gorenjska regija	47	9,4	9,4	86,2
	Notranjsko - kraška regija	15	3,0	3,0	89,2
	Goriška regija	32	6,4	6,4	95,6
	Obalno - kraška regija	22	4,4	4,4	100,0
	Skupaj	500	100,0	100,0	

Največ 138 anketirancev oziroma 27,6 %, je iz osrednjeslovenske regije, 47 oziroma 9,4 % anketirancev je iz gorenjske regije, 56 oziroma 11,2 % anketirancev je iz savinjske regije, 80 oziroma 16,6 % anketirancev je iz podravske regije, 33 oziroma 6,6 % anketirancev je iz pomurske regije, 32 oziroma 6,4 % anketirancev je iz goriške regije, 31 oziroma 6,2 % anketirancev je iz jugovzhodne Slovenije, 22 oziroma 4,4 % anketirancev je iz obalno-kraške regije, 21 oziroma 4,2 % anketirancev je iz koroške regije, 15 oziroma 3,0 % anketirancev je iz notranjsko-kraške regije, 14 oziroma 2,8 % anketirancev je iz zasavske regije in 11 oziroma 2,2 % anketirancev je iz spodnje posavske regije.

8 ANALIZA REZULTATOV

Opisno statistiko smo uporabili za prikaz značilnosti vzorca populacije (frekvence in odstotki) ter rezultatov anketnega vprašalnika (frekvence in odstotki ter povprečne vrednosti in standardni odkloni).

8.1 *Poznavanje identifikacijskih sistemov*

V prvem sklopu vprašanj smo želeli ugotoviti, koliko izkušenj imajo anketiranci z identifikacijskimi sistemi.

8.1.1 Uporaba različnih identifikacijskih sistemov

Tabela 9 nam prikazuje podatke za vprašanje, s katerim smo želeli ugotoviti »*Katere načine sistemov preverjanja dostopa najbolj pogosto uporabljajo v vsakodnevnem življenju?*«.

Tabela 9: Frekvence uporabe sistemov preverjanja dostopa

	Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Kartični sistem (npr. registracija s kartico pri vstopu na delovno mesto	128	25,6	25,6	25,6
Klasični ključi (npr. vsakokratna uporaba ključev za odpiranje vrat)	343	68,6	68,6	94,2
Biometrični sistemi (npr. prepoznava prstnega odtisa – položimo prst na čitalec)	9	1,8	1,8	96,0
Varnostniki (npr. pregled in registracija pri varnostniku pred vstopom v parlament)	9	1,8	1,8	97,8
Drugo, prosimo vpišite:	11	2,2	2,2	100,0
Skupaj	500	100,0	100,0	

Prišli smo do ugotovitve, da kar 343 oziroma 68,6 % anketirancev še vedno uporablja klasični ključ za vstop v varovane prostore. 128 anketirancev oziroma 25,5 % pa uporablja kartični sistem. V enakem deležu 1,8 % oziroma 9 anketirancev je tistih, ki uporabljajo biometrični sistem ter pregled in

registracijo pri varnostniku. Ugotavljamo, da je biometrija v slovenskem prostoru torej še relativno malo v uporabi, kar bi lahko pripisali zelo restriktivni zakonodaji na tem področju. 11 anketirancev oziroma 2,2 %, je navedlo drugačen način sistemskega preverjanja dostopa, ki ne zapade pod zgoraj naštete metodologije.

Nadaljevanje raziskave se nanaša na identifikacijo v splošnem pogledu. Želeli smo ugotoviti, v kakšnih okoliščinah so se anketiranci že srečali z identifikacijo. Tabela 10 prikazuje frekvenco v primeru identifikacije pri registraciji delovnega časa. Ugotavljamo, da se je 371 anketirancev oziroma 74,2 % že srečalo z registracijo delovnega časa zaposlenih.

Tabela 10: Frekvence za registracijo delovnega časa zaposlenih

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	371	74,2	100,0	100,0
Manjkajoči		129	25,8		
Skupaj		500	100,0		

V tabeli 11 je prikazana frekvenca anketirancev, ki se je srečala s preverjanjem identitete pri vstopu v zavarovan arhiv ali kakšno drugo zavarovano delovno območje. 157 anketirancev oziroma 31,4 % se je že srečalo s preverjanjem identitete v takšnih okoliščinah.

Tabela 11: Frekvence za preverjanje identitete zaposlenih pred vstopom v zavarovan arhiv ali kakšno drugo zavarovano delovno območje

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	157	31,4	100,0	100,0
Manjkajoči		343	68,6		
Skupaj		500	100,0		

Tabela 12 nam prikazuje, da se je 225 anketirancev oziroma 45,0 % že srečalo s preverjanjem identitete pred vstopom na letalo.

Tabela 12: Frekvence za preverjanje identitete pred vstopom na letalo

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	225	45,0	100,0	100,0
Manjkajoči		275	55,0		
Skupaj		500	100,0		

324 anketirancev oziroma 64,8 % se je že srečalo z preverjanjem identitete potnikov pri vstopu v tujo državo (tabela 13).

Tabela 13: Frekvence za preverjanje identitete potnikov pri vstopu v tujo državo

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	324	64,8	100,0	100,0
Manjkajoči		176	35,2		
Skupaj		500	100,0		

229 anketirancev oziroma 45,8 % se je že srečalo z preverjanjem identitete obiskovalcev podjetij, javnih ali vladnih ustanov (tabela 14).

Tabela 14: Frekvence za preverjanje identitete obiskovalcev podjetij, javnih ali vladnih ustanov

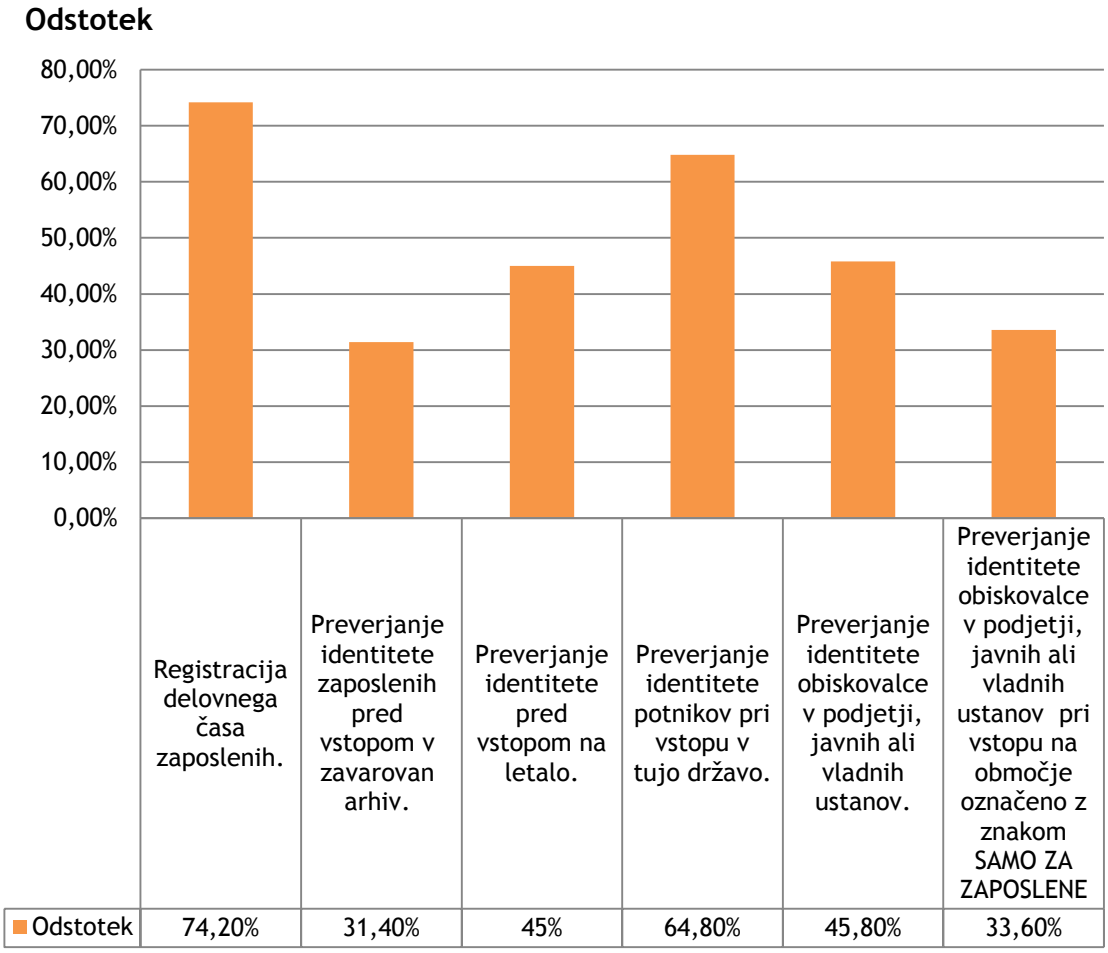
		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	229	45,8	100,0	100,0
Manjkajoči		271	54,2		
Skupaj		500	100,0		

Tabela 15 prikazuje rezultate za primere, ko so se anketiranci srečali s preverjanjem identitete kot obiskovalci podjetij, javnih ali vladnih ustanov pri vstopu na območje označeno z znakom samo za zaposlene. 168 anketirancev oziroma 33,6 % se je srečalo z identifikacijo v teh primerih.

Tabela 15: Frekvence za preverjanje identitete obiskovalcev podjetji, javnih ali vladnih ustanov pri vstopu na območje označeno z znakom »samo za zaposlene«

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	168	33,6	100,0	100,0
Manjkajoči		332	66,4		
Skupaj		500	100,0		

Slika 9 prikazuje delež sistemov za identifikacijo glede na namen uporabe.



Slika 9: Odstotek identifikacijskih sistemov v uporabi glede na namen uporabe

Z raziskovanjem v prvem sklopu vprašanj, smo prišli do ugotovitve, da so se anketiranci največ srečevali s preverjanjem identitete pri registraciji delovnega časa ter s preverjanjem identitete pri vstopu v tujo državo.

Najmanj anketirancev se je srečalo s preverjanjem identitete pred vstopom v zavarovan arhiv ali kakšno drugo zavarovano delovno območje.

Podobno kot pri predhodnem vprašanju, smo v nadaljevanju želeli ugotoviti »*V kolikšni meri anketiranci poznajo biometrične sisteme za identifikacijo?*«. Anketiranci so poznavanje posameznega biometričnega sistema ocenjevali na pet stopenjski lestvici, pri čemer je ocena ena pomenila »sploh nisem seznanjen« ter ocena pet »zelo dobro sem seznanjen«.

8.1.2 Prstni odtis

Tabela 16 prikazuje porazdelitev seznanjenosti z biometričnim sistemom na osnovi prepoznavanja prstnega odtisa.

Tabela 16: Frekvence za poznavanje identifikacije na osnovi prstnega odtisa

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh nisem seznanjen/a	29	5,8	5,8	5,8
	2 Slabo seznanjen/a	49	9,8	9,8	15,6
	3 Srednje	141	28,2	28,2	43,8
	4 Dobro seznanjen/a	163	32,6	32,6	76,4
	5 Zelo dobro seznanjen/a	118	23,6	23,6	100,0
	Skupaj	500	100,0	100,0	

Prišli smo do ugotovitve, da je 163 anketirancev oziroma 32,6 % dobro seznanjenih s takšnim načinom preverjanja identitete. 141 anketirancev oziroma 28,2 % je srednje seznanjenih ter 118 anketirancev oziroma 23,6 % je zelo dobro seznanjenih s prepoznavanjem prstnega odtisa kot biometričnim sistemom preverjanja identitete. 49 anketirancev oziroma 9,8 %, je slabo seznanjenih ter 29 anketirancev oziroma 5,8 %, pa sploh ni seznanjenih s prepoznavanjem prstnega odtisa kot biometričnim sistemom preverjanja identitete. Ugotavljamo, da je slovensko prebivalstvo v povprečju dobro seznanjeno z biometrično identifikacijo na osnovi prstnega odtisa.

8.1.3 Geometrija roke

Naslednja vrsta biometričnega sistema preverjanja identitete je prepoznava na osnovi oblike roke, kjer ugotavljamo, da je z njim zelo dobro seznanjeno 17 anketirancev oziroma 3,4 %. Med tem ko 160 anketirancev oziroma 32,0 % s to vrsto biometričnega sistema sploh ni seznanjeno. 155 anketirancev oziroma 31,0 % je s tem načinom slabo seznanjeno.

Tabela 17: Frekvence za poznavanje identifikacije na osnovi prepoznave oblike roke

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh nisem seznanjen/a	160	32,0	32,0	32,0
	2 Slabo seznanjen/a	155	31,0	31,0	63,0
	3 Srednje	116	23,2	23,2	86,2
	4 Dobro seznanjen/a	52	10,4	10,4	96,6
	5 Zelo dobro seznanjen/a	17	3,4	3,4	100,0
	Skupaj	500	100,0	100,0	

23,2 % anketirancev je srednje seznanjeno in 52 anketirancev oziroma 10,4 % je s prepoznavanjem oblike roke kot načinom preverjanja identitete dobro seznanjenih (tabela 17).

8.1.4 Prepoznava podpisa

Z biometričnim sistemom na osnovi prepoznavanja podpisa je dobro seznanjenih 150 anketirancev oziroma 30,0 % (Tabela 18).

Tabela 18: Frekvence za poznavanje identifikacije na osnovi prepoznave podpisa

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh nisem seznanjen/a	31	6,2	6,2	6,2
	2 Slabo seznanjen/a	64	12,8	12,8	19,0
	3 Srednje	129	25,8	25,8	44,8
	4 Dobro seznanjen/a	150	30,0	30,0	74,8
	5 Zelo dobro seznanjen/a	126	25,2	25,2	100,0
	Skupaj	500	100,0	100,0	

129 oziroma 25,8 % anketirancev je s takim načinom preverjanja srednje seznanjena ter 126 oziroma 25,2 % je zelo dobro seznanjena. 64 oziroma 12,8 % anketirancev je s takim biometričnim sistemom slabo seznanjena. 31 oziroma 6,2 % anketirancev sploh ni seznanjenih s prepoznavanjem podpisa kot načinom biometričnega sistema preverjanja identitete. Največ anketirancev je s prepoznavo podpisa dobro seznanjenih.

8.1.5 Ožilje roke

Tebela 19 se nanaša na prepoznavo ožilja roke, kot načinom biometričnega sistema preverjanja identitete.

Tabela 19: Frekvence za poznavanje identifikacije na osnovi prepoznave ožilja roke.

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh nisem seznanjen/a	275	55,0	55,0	55,0
	2	Slabo seznanjen/a	136	27,2	27,2	82,2
	3	Srednje	61	12,2	12,2	94,4
	4	Dobro seznanjen/a	21	4,2	4,2	98,6
	5	Zelo dobro seznanjen/a	7	1,4	1,4	100,0
	Skupaj		500	100,0	100,0	

275 anketirancev oziroma 55,0 % s takim načinom preverjanja sploh ni seznanjenih. 136 oziroma 27,2 % anketirancev je slabo seznanjenih ter 61 oziroma 12,2 % anketirancev je srednje seznanjenih. 21 oziroma 4,2 odstotka anketirancev je s prepoznavo ožilja roke dobro ter 7 oziroma 1,4 % anketirancev zelo dobro seznanjenih

8.1.6 Prepoznava obraza s kamero

Tabela 20 podaja frekvence v vezi s poznavanjem biometrične identifikacije obraza. 138 oziroma 27,6 % anketirancev je z biometrijo na osnovi prepoznave obraza s pomočjo kamere srednje seznanjena ter 123 oziroma 24,6 % anketirancev je dobro seznanjenih. 99 oziroma 19,8 % anketirancev je slabo seznanjenih.

Tabela 20: Frekvence za poznavanje identifikacije na osnovi prepoznave obraza s pomočjo kamere

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh nisem seznanjen/a	69	13,8	13,8	13,8
	2	Slabo seznanjen/a	99	19,8	19,8	33,6
	3	Srednje	138	27,6	27,6	61,2
	4	Dobro seznanjen/a	123	24,6	24,6	85,8
	5	Zelo dobro seznanjen/a	71	14,2	14,2	100,0
	Skupaj		500	100,0	100,0	

71 oziroma 14,2 % anketirancev je s prepoznavo obraza s pomočjo kamere zelo dobro seznanjenih ter 69 oziroma 13,8 % anketirancev sploh ni seznanjenih s to vrsto biometričnega sistema preverjanja identitete.

8.1.7 Šarenica

Spodnja tabela 21 se nanaša na prepoznavo šarenice s pogledom v skener kot načinom biometričnega sistema preverjanja identitete.

Tabela 21: Frekvence za poznavanje identifikacije na osnovi prepoznave šarenice s pogledom v skener

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh nisem seznanjen/a	112	22,4	22,4	22,4
	2	Slabo seznanjen/a	117	23,4	23,4	45,8
	3	Srednje	142	28,4	28,4	74,2
	4	Dobro seznanjen/a	88	17,6	17,6	91,8
	5	Zelo dobro seznanjen/a	41	8,2	8,2	100,0
	Skupaj		500	100,0	100,0	

142 oziroma 28,4 % anketirancev je s takim načinom preverjanja srednje seznanjenih. 117 oziroma 23,4 % anketirancev je slabo seznanjenih ter 112 oziroma 22,4 % anketirancev s tem načinom biometrije sploh ni seznanjenih. 88 anketirancev oziroma 17,6 odstotka je s prepoznavo šarenice s pogledom v skener dobro ter 41 oziroma 8,2 % anketirancev zelo dobro seznanjenih.

8.1.8 DNK

Tabela 22 se nanaša na prepoznavo DNK kot načina biometričnega sistema preverjanja identitete.

Tabela 22: Frekvence za poznavanje identifikacije na osnovi prepoznave DNK (analiza vzorca krvi, las itd.)

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh nisem seznanjen/a	102	20,4	20,4	20,4
	2	Slabo seznanjen/a	78	15,6	15,6	36,0
	3	Srednje	133	26,6	26,6	62,6
	4	Dobro seznanjen/a	111	22,2	22,2	84,8
	5	Zelo dobro seznanjen/a	76	15,2	15,2	100,0
	Skupaj		500	100,0	100,0	

133 oziroma 26,6 % anketirancev je s takim načinom preverjanja srednje seznanjenih. 78 oziroma 15,6 % anketirancev je slabo seznanjenih ter 102 oziroma 20,4 % anketirancev s tem načinom sploh ni seznanjenih. 111 oziroma 22,2 % anketirancev je s prepoznavo DNK dobro ter 76 oziroma 15,2 % anketirancev zelo dobro seznanjenih.

8.1.9 Prepoznava glasu

Tabela 23 se nanaša na prepoznavo glasu kot vrsto biometričnega sistema preverjanja identitete. 165 oziroma 33,0 % anketirancev je s takim načinom preverjanja srednje seznanjenih.

Tabela 23: Frekvence za poznavanje identifikacije na osnovi prepoznave glasu

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh nisem seznanjen/a	73	14,6	14,6	14,6
	2	Slabo seznanjen/a	96	19,2	19,2	33,8
	3	Srednje	165	33,0	33,0	66,8
	4	Dobro seznanjen/a	109	21,8	21,8	88,6
	5	Zelo dobro seznanjen/a	57	11,4	11,4	100,0
	Skupaj		500	100,0	100,0	

96 oziroma 19,2 % anketirancev je slabo seznanjenih ter 73 oziroma 14,6 % anketirancev s tem sploh ni seznanjenih. 109 oziroma 21,8 % anketirancev je s prepoznavo glasu dobro ter 57 oziroma 11,4 % anketirancev zelo dobro seznanjenih.

8.2 *Izkušnje z biometričnimi identifikacijskimi sistemi*

8.2.1 Pretekle izkušnje z biometričnimi identifikacijskimi sistemi

Tabela 24 se nanaša na vprašanje, kjer smo želeli ugotoviti, če so anketiranci v preteklosti že imeli izkušnje z biometrijo.

Tabela 24: Frekvence za pretekle izkušnje z biometričnimi sistemi

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Da	167	33,4	33,4	33,4
	Ne	333	66,6	66,6	100,0
	Skupaj	500	100,0	100,0	

Ugotavljamo, da 333 oziroma 66,6 % anketirancev s to vrsto sistemov za preverjanja identitete v preteklosti še ni imelo izkušenj. 167 oziroma 33,4 % anketirancev pa je že imelo izkušnje z biometrijo.

8.2.2 Izkušnje z biometričnimi identifikacijskimi sistemi glede na njihovo vrsto

Tabela 25 zajema le tiste anketirance, ki so v preteklosti imeli izkušnje z biometrijo. Zanimalo nas je s katero vrsto biometričnega sistema so se srečali. Največ, 80 oziroma 47,9 % anketirancev je imelo izkušnje s prepoznavo prstnega odtisa. 44 oziroma 26,3 % anketirancev je imelo izkušnje s prepoznavo podpisa. 23 oziroma 13,8 % anketirancev je imelo izkušnje s prepoznavo obraza s pomočjo kamere. Izkušnje s prepoznavo šarenice so imeli 4 oziroma 2,4 % anketirancev. V enakem številu so bili tisti, ki so imeli izkušnje s prepoznavo DNK.

Tabela 25: Frekvence preteklih izkušenj z biometričnimi sistemi glede na vrsto sistema

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Prepoznava prstnega odtisa (položimo prst na čitalec).	80	16,0	47,9	47,9
	Prepoznava oblike roke (členkov in prstov), ki jo izvedemo z	3	,6	1,8	49,7
	Prepoznava podpisa.	44	8,8	26,3	76,0
	Prepoznava obraza s pomočjo kamere.	23	4,6	13,8	89,8
	Prepoznava značilnosti šarenice s pogledom v skener.	4	,8	2,4	92,2
	Prepoznava DNK: analiza vzorca krvi, las, itd.	4	,8	2,4	94,6
	Prepoznava glasu.	9	1,8	5,4	100,0
	skupaj	167	33,4	100,0	
Manjkajoči		333	66,6		
Skupaj		500	100,0		

9 oziroma 5,4 % anketirancev je imelo izkušnje s prepoznavo glasu, ter najmanj, 3 oziroma 1,8 % anketirancev so imeli izkušnje s prepoznavo oblike roke kot načinom biometričnega sistema preverjanja identitete.

8.3 *Zbiranje in ravnanje z osebnimi podatki za potrebe biometrične identifikacije*

V nadaljevanju so prikazane trditve v vezi s strinjanjem glede načina zbiranja in ravnanja z osebnimi podatki, kjer so anketiranci na Likertovi lestvici izrazili svoje strinjanje oziroma ne strinjanje z dano trditvijo. Ocena ena je pomenilo »sploh se ne strinjam« ter ocena pet »popolnoma se strinjam«.

8.3.1 Zbiranje in ravnanje z osebnimi podatki

V tabeli 26 prikazujemo strinjanje s trditvijo »*V kolikor se uporablja biometrična identifikacija, se mora okrepiti varstvo zasebnosti in pošteno ravnanje s podatki!*«.

Tabela 26: Frekvence odgovorov glede uporabe biometrične identifikacije, varstva zasebnosti in poštenega ravnanja s podatki

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh se ne strinjam	5	1,0	1,0	1,0
	2	Ne strinjam se	5	1,0	1,0	2,0
	3	Neodločen	34	6,8	6,8	8,8
	4	Strinjam se	161	32,2	32,2	41,0
	5	Popolnoma se strinjam	295	59,0	59,0	100,0
	Skupaj		500	100,0	100,0	

Ugotavljamo, da se 295 anketirancev oziroma 59,0 % s to trditvijo popolnoma strinja. 161 anketirancev oziroma 32,2 %, se strinja ter 34 oziroma 6,8 % anketirancev je glede te trditve neodločenih. V kakšnem enakem razmerju 5 oziroma 1,0 % anketirancev se ne strinja oziroma se sploh ne strinja s trditvijo, da če se uporablja biometrična identifikacija, se mora okrepiti tudi varstvo zasebnosti in pošteno ravnanje s podatki.

8.3.2 Obveščanje glede zbiranja osebnih podatkov

V tabeli 27 prikazujemo strinjanje s trditvijo »*V kolikor organizacija zbira biometrične podatke, mora uporabnike jasno obvestiti o potrebnosti in načinu zbiranja in obdelave podatkov!*«. Ugotovili smo, da se 332 anketirancev oziroma 66,4 % s to trditvijo popolnoma strinja. 128 oziroma 25,6 % anketirancev se strinja ter 31 oziroma 6,2 % anketirancev je glede te trditve neodločenih. 5 oziroma 1 odstotek anketirancev se ne strinja ter 4 oziroma 0,8 % anketirancev se sploh ne strinja s trditvijo, da mora organizacija, ki zbira biometrične podatke, uporabnike jasno obvestiti o potrebnosti in načinu zbiranja in obdelave podatkov.

Tabela 27: Frekvence odgovorov glede obveščanja o potrebnosti in načinu zbiranja in obdelave podatkov

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh se ne strinjam	4	,8	,8	,8
	2	Ne strinjam se	5	1,0	1,0	1,8
	3	Neodločen	31	6,2	6,2	8,0
	4	Strinjam se	128	25,6	25,6	33,6
	5	Popolnoma se strinjam	332	66,4	66,4	100,0
	Skupaj		500	100,0	100,0	

8.3.3 Način zbiranja osebnih podatkov

S tabelo 28 smo želeli ugotoviti strinjanje z naslednjo trditvijo »*Organizacije lahko biometrične podatke zbirajo zgolj na način, ki je bil uporabniku predhodno opisan*«.

Ugotavljamo, da se 319 anketirancev oziroma 63,8 % s to trditvijo popolnoma strinja. 137 oziroma 27,4 % anketirancev se strinja ter 36 oziroma 7,2 % anketirancev je glede te trditve neodločenih. 5 oziroma 1 % anketirancev se ne strinja ter 3 oziroma 0,6 % anketirancev se sploh ne strinja s trditvijo, da lahko organizacije biometrične podatke zbirajo zgolj na način, ki je bil uporabniku predhodno opisan.

Tabela 28: Frekvence odgovorov glede načina zbiranja biometričnih podatkov

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh se ne strinjam	3	,6	,6	,6
	2	Ne strinjam se	5	1,0	1,0	1,6
	3	Neodločen	36	7,2	7,2	8,8
	4	Strinjam se	137	27,4	27,4	36,2
	5	Popolnoma se strinjam	319	63,8	63,8	100,0
	Skupaj		500	100,0	100,0	

Največ anketirancev se popolnoma strinja z načinom zbiranja biometričnih podatkov, ki je bil uporabno opisan.

8.3.4 Dopustnost tajnega zbiranja osebnih podatkov

Nadalje smo želeli ugotoviti strinjanje s trditvijo, da »*Skrivno zbiranje biometričnih podatkov ni dovoljeno!*« (tabela 29).

Tabela 29: Frekvence odgovorov glede dopustnosti skrivnega zbiranja biometričnih podatkov

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh se ne strinjam	6	1,2	1,2	1,2
	2	Ne strinjam se	8	1,6	1,6	2,8
	3	Neodločen	31	6,2	6,2	9,0
	4	Strinjam se	67	13,4	13,4	22,4
	5	Popolnoma se strinjam	388	77,6	77,6	100,0
	Skupaj		500	100,0	100,0	

Prišli smo do ugotovitve, da se 388 oziroma 77,6 % anketirancev, s to trditvijo popolnoma strinja. 67 oziroma 13,4 % anketirancev se strinja ter 31 anketirancev oziroma 6,2 % je glede te trditve neodločenih. 8 oziroma 1,6 % anketirancev se ne strinja ter 6 oziroma 1,2 % anketirancev se sploh ne strinja s to trditvijo.

8.3.5 Povezovanje osebnih podatkov z drugimi podatki

Ugotoviti smo želeli strinjanje s trditvijo, »*Biometričnih podatkov se ne sme povezovati z drugimi osebnimi podatki!*« (tabela 30).

Tabela 30: Frekvence odgovorov glede dopustnosti povezovanja biometričnih podatkov z drugimi osebnimi podatki

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh se ne strinjam	16	3,2	3,2	3,2
	2	Ne strinjam se	15	3,0	3,0	6,2
	3	Neodločen	91	18,2	18,2	24,4
	4	Strinjam se	114	22,8	22,8	47,2
	5	Popolnoma se strinjam	264	52,8	52,8	100,0
	Skupaj		500	100,0	100,0	

Prišli smo do ugotovitve, da se 264 anketirancev oziroma 52,8 % s to trditvijo popolnoma strinja. 114 oziroma 22,8 % anketirancev se strinja ter 91 oziroma 18,2 % anketirancev je glede te trditve neodločena. 15 oziroma 3,0 % anketirancev se ne strinja ter 16 oziroma 3,2 % anketirancev se sploh ne strinja s trditvijo, da biometričnih podatkov se ne sme povezovati z drugimi osebnimi podatki.

8.3.6 Možnost kršitev pravic zasebnosti zaradi interesov nacionalne varnosti

Tabela 31 prikazuje strinjanje s trditvijo, da se »*Prej naštete trditve (»V kolikor se uporablja biometrična identifikacija, se mora okrepiti varstvo zasebnosti in pošteno ravnanje s podatki!«, »V kolikor organizacija zbira biometrične podatke, mora uporabnike jasno obvestiti o potrebnosti in načinu zbiranja in obdelave podatkov!, »Organizacije lahko biometrične podatke zbirajo zgolj na način, ki je bil uporabniku predhodno opisan!«, »Skrivno zbiranje biometričnih podatkov ni dovoljeno*« in »*Biometričnih podatkov se ne sme povezovati z drugimi osebnimi podatki!«) lahko kršijo, če gre za interese državne varnosti*«.

Tabela 31: Frekvence odgovorov glede možnosti kršitev zgoraj naštetih trditev v primeru, če gre za interese državne varnosti

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh se ne strinjam	92	18,4	18,4	18,4
	2 Ne strinjam se	77	15,4	15,4	33,8
	3 Neodločen	140	28,0	28,0	61,8
	4 Strinjam se	92	18,4	18,4	80,2
	5 Popolnoma se strinjam	99	19,8	19,8	100,0
	Skupaj	500	100,0	100,0	

Ugotavljamo, da se 99 anketirancev oziroma 19,8 % s to trditvijo popolnoma strinja. 92 oziroma 18,4 % anketirancev se strinja ter 140 oziroma 28,0 % anketirancev je glede te trditve neodločenih. 77 oziroma 15,4 % anketirancev se ne strinja ter 92 oziroma 18,4 % anketirancev se sploh ne strinja s prejšnjo trditvijo.

8.4 *Sprejemljivost biometričnih sistemov pri odkrivanju kaznivih dejanj*

Naslednjih sedem tabel nam prikazuje »*Sprejemljivost uporabe biometričnih podatkov v različnih situacijah*«, ki so navedene. Anketiranci so svoje strinjanje glede sprejemljivosti oziroma nesprejemljivosti izrazili na Likertovi lestvici, pri čemer je ocena ena pomenilo »sploh ni sprejemljivo« ter ocena pet »zelo sprejemljivo«.

8.4.1 Manjša kazniva dejanja

75 oziroma 15,0 % anketirancev meni, da je uporaba biometričnega sistema kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj zelo sprejemljivo (tabela 32). 215 oziroma 43,0 % anketirancev meni, da je sprejemljivo ter 96 oziroma 19,2 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih.

Tabela 32: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva za pomoč pri preprečevanju manjših kaznivih dejanj

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	43	8,6	8,6	8,6
	2	Ni sprejemljiva	71	14,2	14,2	22,8
	3	Neodločen	96	19,2	19,2	42,0
	4	Sprejemljiva	215	43,0	43,0	85,0
	5	Zelo sprejemljiva	75	15,0	15,0	100,0
	Skupaj		500	100,0	100,0	

71 oziroma 14,2 % anketirancev meni, da ni sprejemljivo ter 43 oziroma 8,6 % anketirancev meni, da uporaba biometričnega sistema kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj sploh ni sprejemljiva.

8.4.2 Težja kazniva dejanja

Nadalje smo ugotavljali frekvence sprejemljivosti biometričnih sistemov v primerih težjih kaznivih dejanj (tabela 33). Ugotavljamo, da 327 anketirancev

oziroma 65,4 % meni, da je uporaba biometričnega sistema kot sredstva za pomoč pri preprečevanju težjih kaznivih dejanj zelo sprejemljiva.

Tabela 33: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva za pomoč pri preprečevanju težjih kaznivih dejanj

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavna	1	Sploh ni sprejemljiva	2	,4	,4	,4
	2	Ni sprejemljiva	6	1,2	1,2	1,6
	3	Neodločen	23	4,6	4,6	6,2
	4	Sprejemljiva	142	28,4	28,4	34,6
	5	Zelo sprejemljiva	327	65,4	65,4	100,0
	Skupaj		500	100,0	100,0	

142 oziroma 28,4 % anketirancev meni, da je sprejemljiva. 23 oziroma 4,6 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih. 6 anketirancev oziroma 1,2 % meni, da ni sprejemljiva ter 2 oziroma 0,4 % anketirancev meni, da uporaba biometričnega sistema kot sredstva za pomoč pri preprečevanju težjih kaznivih dejanj sploh ni sprejemljiva.

8.4.3 Preverba kupcev orožja

Tabela 34 prikazuje frekvence sprejemljivosti biometrije, ko bi tehnologijo uporabljali za preverjanje identitete kupca orožja zaradi morebitnih preteklih kaznivih dejanj.

Tabela 34: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri preverjanju identitete kupca orožja v bazi pravnomočno obsojenih storilcev kaznivih dejanj

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	4	,8	,8	,8
	2	Ni sprejemljiva	4	,8	,8	1,6
	3	Neodločen	34	6,8	6,8	8,4
	4	Sprejemljiva	166	33,2	33,2	41,6
	5	Zelo sprejemljiva	292	58,4	58,4	100,0
	Skupaj		500	100,0	100,0	

292 anketirancev oziroma 58,4 % meni, da je uporaba biometričnega sistema pri preverjanju identitete kupca orožja v bazi pravnomočno obsojenih kriminalcev zelo sprejemljiva. 166 oziroma 33,2 % anketirancev meni, da je sprejemljiva. 34 oziroma 6,8 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih. 4 oziroma 0,8 % anketirancev meni, da ni sprejemljiva ter enako 4 oziroma 0,8 % anketirancev meni, da uporaba biometričnega sistema pri preverjanju identitete kupca orožja v bazi pravnomočno obsojenih storilcev kaznivih dejanj, sploh ni sprejemljiva.

8.5 *Sprejemljivost biometričnih sistemov v vsakdanjem življenju*

Naslednjih šest spremenljivk opisuje sprejemljivost biometrične tehnologije v vsakdanjih različnih življenjskih situacijah.

8.5.1 Plačilo s kreditno kartico

Tabela 35 prikazuje porazdelitev frekvenc v primeru uporabe biometrije pri plačilu s kreditno kartico.

Tabela 35: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri preverjanju identitete pri plačilu s kreditno kartico

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	36	7,2	7,2	7,2
	2	Ni sprejemljiva	73	14,6	14,6	21,8
	3	Neodločen	115	23,0	23,0	44,8
	4	Sprejemljiva	178	35,6	35,6	80,4
	5	Zelo sprejemljiva	98	19,6	19,6	100,0
	Skupaj		500	100,0	100,0	

98 anketirancev oziroma 19,6 % meni, da je uporaba biometričnega sistema za preverjanje identitete pri plačilu s kreditno kartico zelo sprejemljiva. 178 oziroma 35,6 % anketirancev meni, da je sprejemljiva. 115 oziroma 23,0 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih. 73 oziroma 14,6 % anketirancev meni, da metoda za ta namen ni sprejemljiva ter 36 oziroma 7,2 % anketirancev meni, da uporaba

biometričnega sistema za preverjanje identitete pri plačilu s kreditno kartico sploh ni sprejemljiva.

8.5.2 Uporaba biometrije na bankomatih

Za uporabo biometrije pri identifikaciji na bankomatih (dvigovanje denarja na bankomatu) 104 anketirancev oziroma 20,8 % meni, da je uporaba biometričnega sistema zelo sprejemljiva (tabela 36). 166 anketirancev oziroma 33,2 % meni, da je sprejemljivo. 104 oziroma 20,8 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih. 86 oziroma 17,2 % anketirancev meni, da biometrija ni sprejemljiva ter 40 oziroma 8,0 % anketirancev meni, da uporaba biometričnega sistema pri dvigovanju denarja na bankomatu sploh ni sprejemljiva.

Tabela 36: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri dvigovanju denarja na bankomatu

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	40	8,0	8,0	8,0
	2	Ni sprejemljiva	86	17,2	17,2	25,2
	3	Neodločen	104	20,8	20,8	46,0
	4	Sprejemljiva	166	33,2	33,2	79,2
	5	Zelo sprejemljiva	104	20,8	20,8	100,0
	Skupaj		500	100,0	100,0	

Zaključimo lahko, da največ anketirancev podpira biometrično tehnologijo za identifikacijo pri dvigovanju denarja na bankomatih.

8.5.3 Dostopanje do zaupnih zdravstvenih in finančnih podatkov

Za dostopanje do zaupnih podatkov kot so osebni zdravstveni podatki in podatki o financah se je 147 oziroma 29,4 % anketirancev opredelilo, da je uporaba biometričnega sistema zelo sprejemljiva (tabela 37). 182 oziroma 36,4 % anketirancev meni, da je sprejemljiva. 86 oziroma 17,2 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih.

Tabela 37: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	34	6,8	6,8	6,8
	2	Ni sprejemljiva	51	10,2	10,2	17,0
	3	Neodločen	86	17,2	17,2	34,2
	4	Sprejemljiva	182	36,4	36,4	70,6
	5	Zelo sprejemljiva	147	29,4	29,4	100,0
	Skupaj		500	100,0	100,0	

51 oziroma 10,2 % anketirancev meni, da biometrija ni sprejemljiva za te namene ter 34 oziroma 6,8 % anketirancev meni, da uporaba biometričnega sistema pri dostopanju do zaupnih podatkov kot so osebni zdravstveni podatki in podatki o financah sploh ni sprejemljiva.

8.5.4 Preverba preteklosti posameznika

90 anketirancev oziroma 18,0 % meni, da je uporaba biometričnega sistema pri preverjanju preteklosti posameznika zelo sprejemljiva (tabela 38). 136 oziroma 27,2 % anketirancev meni, da je sprejemljiva. 126 oziroma 25,2 % anketirancev je glede uporabe biometričnega sistema v ta namen neodločenih. 91 oziroma 18,2 % anketirancev meni, da biometrija ni sprejemljiva ter 57 oziroma 11,4 % anketirancev meni, da uporaba biometričnega sistema pri preverjanju preteklosti posameznika sploh ni sprejemljiva.

Tabela 38: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri preverjanju preteklosti posameznika

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	57	11,4	11,4	11,4
	2	Ni sprejemljiva	91	18,2	18,2	29,6
	3	Neodločen	126	25,2	25,2	54,8
	4	Sprejemljiva	136	27,2	27,2	82,0
	5	Zelo sprejemljiva	90	18,0	18,0	100,0
	Skupaj		500	100,0	100,0	

Pri naslednjih dveh spremenljivkah smo želeli, da bi anketiranci pomislili na koristi in pozabili oziroma zanemarili dejstvo ogrožanja zasebnosti. Želeli smo izvedeti ali se zdi sprejemljiva uporaba biometričnih podatkov pri vpisu v šolo ter pri kontroli potnih listov. Anketiranci so svoje strinjanje glede sprejemljivosti oziroma nesprejemljivosti izrazili na Likertovi lestvici, pri čemer je ocena ena pomenilo »sploh ni sprejemljivo« ter ocena pet »zelo sprejemljivo«.

8.5.5 Vpis v šolo

Prišli smo do ugotovitve, da se 117 anketirancev oziroma 23,4 % sploh ne strinja s trditvijo, da bi ob vpisu v šolo uporabili biometrične podatke (tabela 39). 110 oziroma 22,0 % anketirancev meni, da ni sprejemljivo. 136 oziroma 27,2 % anketirancev je bila neodločenih.

Tabela 39: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri vpisu v šolo

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	117	23,4	23,4	23,4
	2	Ni sprejemljiva	110	22,0	22,0	45,4
	3	Neodločen	136	27,2	27,2	72,6
	4	Sprejemljiva	101	20,2	20,2	92,8
	5	Zelo sprejemljiva	36	7,2	7,2	100,0
	Skupaj		500	100,0	100,0	

101 oziroma 20,2 % anketirancev meni, da je to sprejemljivo ter 36 oziroma 7,2 % anketirancev, da je uporaba biometričnih podatkov ob vpisu v šolo zelo sprejemljiva.

8.5.6 Kontrola potnih listov

Glede uporabe biometričnih podatkov za kontrolo potnih listov smo prišli do ugotovitve, da se 133 anketirancev oziroma 26,6 % s tem zelo strinja (tabela 40). 261 anketirancev oziroma 52,2 % meni, da je uporaba sprejemljiva. 69 oziroma 13,8 % anketirancev je neodločenih. 18 oziroma 3,6 % anketirancev meni, da to ni sprejemljivo. 19 oziroma 3,8 % anketirancev je mnenja, da

uporaba biometričnih podatkov pri kontroli potnih listov, sploh ni sprejemljiva.

Tabela 40: Frekvence sprejemljivosti biometrične tehnologije, kot sredstva pri kontroli potnih listov

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	19	3,8	3,8	3,8
	2	Ni sprejemljiva	18	3,6	3,6	7,4
	3	Neodločen	69	13,8	13,8	21,2
	4	Sprejemljiva	261	52,2	52,2	73,4
	5	Zelo sprejemljiva	133	26,6	26,6	100,0
	Skupaj		500	100,0	100,0	

Največ anketirancev je mnenja, da je biometrija pro kontroli potnih listov sprejemljiva.

8.6 *Sprejemljivost biometričnih sistemov za primere protiterorističnih aktivnosti*

Pri naslednjih petih spremenljivkah smo želeli, da bi anketiranci pomislili na teroristične napade in njihovo preprečevanje ter se v ta namen opredelili glede uporabe biometričnih podatkov za preverjanje identitete. Anketiranci so svoje strinjanje glede sprejemljivosti oziroma nesprejemljivosti izrazili na Likertovi lestvici, pri čemer je ocena ena pomenila »sploh ni sprejemljivo« ter ocena pet »zelo sprejemljivo«.

8.6.1 Identifikacija s potnimi listi

Prišli smo do ugotovitve (tabela 41), da se 193 oziroma 38,6 % anketirancev zelo strinja s trditvijo, da bi v potnih listih uporabili biometrične podatke za preverjanje identitete. 242 oziroma 48,4 % anketirancev meni, da je to sprejemljivo. 38 oziroma 7,6 % anketirancev je neodločenih. 15 anketirancev oziroma 3,0 % meni, da to ni sprejemljivo.

Tabela 41: Frekvence sprejemljivosti uporabe biometrične tehnologije v potnih listih

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	12	2,4	2,4	2,4
	2	Ni sprejemljiva	15	3,0	3,0	5,4
	3	Neodločen	38	7,6	7,6	13,0
	4	Sprejemljiva	242	48,4	48,4	61,4
	5	Zelo sprejemljiva	193	38,6	38,6	100,0
	Skupaj		500	100,0	100,0	

12 oziroma 2,4 % anketirancev je mnenja, da uporaba biometričnih podatkov za preverjanje identitete v potnih listih sploh ni sprejemljiva.

8.6.2 Vstop v državne ustanove

150 anketirancev oziroma 30,0 % se zelo strinja s trditvijo, da bi ob vstopu v državne stavbe uporabljali biometrične podatke za preverjanje identitete (tabela 42). 226 oziroma 45,2 % anketirancev meni, da bi to bilo sprejemljivo. 70 oziroma 14,0 % anketirancev je neodločenih. 40 oziroma 8,0 % anketirancev meni, da to ni sprejemljivo ter 14 oziroma 2,8 % anketirancev meni, da uporaba biometričnih podatkov za preverjanje identitete ob vstopu v državne stavbe sploh ni sprejemljiva.

Tabela 42: Frekvence sprejemljivosti uporabe biometrične tehnologije ob vstopu v državne stavbe

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	14	2,8	2,8	2,8
	2	Ni sprejemljiva	40	8,0	8,0	10,8
	3	Neodločen	70	14,0	14,0	24,8
	4	Sprejemljiva	226	45,2	45,2	70,0
	5	Zelo sprejemljiva	150	30,0	30,0	100,0
	Skupaj		500	100,0	100,0	

Največ anketirancev je mnenja, da je uporaba biometrije pri vstopu v državne ustanove, sprejemljiva.

8.6.3 Prijava za let z letalom

V nadaljevanju smo prišli do ugotovitve (tabela 43), da se 204 anketiranci oziroma 40,8 % zelo strinja s trditvijo, da bi na letališčih pri prijavi na let uporabljali biometrične podatke za preverjanje identitete.

Tabela 43: Frekvence sprejemljivosti uporabe biometrične tehnologije na letališčih pri prijavi na let

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	12	2,4	2,4	2,4
	2	Ni sprejemljiva	20	4,0	4,0	6,4
	3	Neodločen	56	11,2	11,2	17,6
	4	Sprejemljiva	208	41,6	41,6	59,2
	5	Zelo sprejemljiva	204	40,8	40,8	100,0
	Skupaj		500	100,0	100,0	

208 anketirancev oziroma 41,6 % meni, da je to sprejemljivo. 56 oziroma 11,2 % anketirancev je glede tega neodločenih. 20 oziroma 4,0 % anketirancev meni, da to ni sprejemljivo ter 12 oziroma 2,4 % anketirancev meni, da uporaba biometričnih podatkov za preverjanje identitete na letališčih pri prijavi na let sploh ni sprejemljiva.

8.6.4 Vozniška dovoljenja

Glede uporabe biometričnih podatkov za preverjanje identitete preko vozniškega dovoljenja (tabela 44) ugotavljamo, da se 82 oziroma 16,4 % anketirancev s tem zelo strinja. 186 oziroma 37,2 % anketirancev meni, da je to sprejemljivo. 124 oziroma 24,8 % anketirancev je glede tega neodločenih. 74 oziroma 14,8 % anketirancev meni, da to ni sprejemljivo ter 34 anketirancev oziroma 6,8 % meni, da uporaba biometričnih podatkov za preverjanje identitete na vozniškem dovoljenju sploh ni sprejemljiva.

Tabela 44: Frekvence sprejemljivosti uporabe biometrične tehnologije na vozniškem dovoljenju

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	34	6,8	6,8	6,8
	2	Ni sprejemljiva	74	14,8	14,8	21,6
	3	Neodločen	124	24,8	24,8	46,4
	4	Sprejemljiva	186	37,2	37,2	83,6
	5	Zelo sprejemljiva	82	16,4	16,4	100,0
	Skupaj		500	100,0	100,0	

8.6.5 Izposoja vozila

V tabeli 45 so ugotovitve glede preverjanja identitete z uporabo biometričnih podatkov pri izposoji avtomobila. 76 oziroma 15,2 % anketirancev se s tem zelo strinja. 162 oziroma 32,4 % anketirancev meni, da je sprejemljivo. 125 oziroma 25,0 % anketirancev je v vezi s tem neodločenih.

Tabela 45: Frekvence sprejemljivosti uporabe biometrične tehnologije pri izposoji avtomobila (rent a car)

			Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1	Sploh ni sprejemljiva	48	9,6	9,6	9,6
	2	Ni sprejemljiva	89	17,8	17,8	27,4
	3	Neodločen	125	25,0	25,0	52,4
	4	Sprejemljiva	162	32,4	32,4	84,8
	5	Zelo sprejemljiva	76	15,2	15,2	100,0
	Skupaj		500	100,0	100,0	

89 anketirancev oziroma 17,8 % meni, da to ni sprejemljivo ter 48 oziroma 9,6 % anketirancev, da uporaba biometričnih podatkov za preverjanje identitete pri izposoji avtomobila, sploh ni sprejemljiva.

8.7 *Zaupanje biometrični identifikaciji*

Pri naslednjih dveh vprašanjih nas je zanimalo mnenje glede zaupanja v zbiranje biometričnih podatkov, kadar jih zbirajo državni organi ali če jih zbirajo privatne organizacije. Anketiranci so svoje zaupanje izrazili na

Likertovi lestvici, pri čemer je ocena ena pomenila »sploh ne zaupam« ter ocena pet »zelo zaupam«.

8.7.1 Uporaba biometrije s strani državnih organov

Iz spodnje tabele 46 lahko ugotovimo, da 99 anketirancev oziroma 19,8 % pri zbiranju biometričnih podatkov sploh ne zaupa državnim organom ter, da jim 54 oziroma 10,8 % anketirancev ne zaupa.

Tabela 46: Frekvence zaupanja glede uporabe biometrične tehnologije - državni organi

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ne zaupam	99	19,8	19,8	19,8
	2 Ne zaupam	54	10,8	10,8	30,6
	3 Neodločen	157	31,4	31,4	62,0
	4 Zaupam	129	25,8	25,8	87,8
	5 Zelo zaupam	61	12,2	12,2	100,0
	Skupaj	500	100,0	100,0	

157 oziroma 31,4 % anketirancev je pri tem vprašanju neodločenih. 129 oziroma 25,8 % anketirancev jim zaupa ter 61 oziroma 12,2 % anketirancev državnim organom pri zbiranju biometričnih podatkov zelo zaupa.

8.7.2 Uporaba biometrije s strani privatnih organizacij

Nadalje ugotavljamo (tabela 47), da 171 anketirancev oziroma 34,2 % pri zbiranju biometričnih podatkov privatnim organizacijam sploh ne zaupa ter, da jim 90 anketirancev oziroma 18,0 % ne zaupa. 178 oziroma 35,6 % anketirancev je pri tem vprašanju neodločenih. 48 anketirancev oziroma 9,6 % zaupa ter 13 oziroma 2,6 % anketirancev privatnim organizacijam pri zbiranju biometričnih podatkov zelo zaupa.

Tabela 47: Frekvence zaupanja glede uporabe biometrične tehnologije - privatne organizacije

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ne zaupam	171	34,2	34,2	34,2
	2 Ne zaupam	90	18,0	18,0	52,2
	3 Neodločen	178	35,6	35,6	87,8
	4 Zaupam	48	9,6	9,6	97,4
	5 Zelo zaupam	13	2,6	2,6	100,0
	Skupaj	500	100,0	100,0	

8.8 *Frekvence opravljenih letalskih letov*

Nadalje nas je zanimalo, koliko letalskih letov so anketiranci (kot potniki) v zadnjem letu opravili.

Tabela 48 prikazuje, da 283 anketirancev oziroma 56,6 % v zadnjem letu sploh ni letelo. Enkrat je letelo 59 anketirancev oziroma 11,8 % ter 77 anketirancev oziroma 15,4 % je letelo dvakrat. Trikrat je letelo 20 anketirancev oziroma 4,0 % ter štirikrat 15 anketirancev oziroma 3,0 %. Petkrat je letelo 12 anketirancev oziroma 2,4 odstotke. So tudi taki anketiranci, ki so leteli več kot petkrat oziroma več kot deset, dvajset in tudi več kot štirideset in petdeset krat v zadnjem letu.

Tabela 48: Frekvence opravljenih letalskih letov v preteklem letu

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	0	283	56,6	56,6	56,6
	1	59	11,8	11,8	68,4
	10	4	,8	,8	69,2
	12	3	,6	,6	69,8
	13	1	,2	,2	70,0
	14	1	,2	,2	70,2
	15	2	,4	,4	70,6
	19	1	,2	,2	70,8
	2	77	15,4	15,4	86,2
	20	2	,4	,4	86,6
	22	1	,2	,2	86,8

23	1	,2	,2	87,0
25	1	,2	,2	87,2
3	20	4,0	4,0	91,2
4	15	3,0	3,0	94,2
43	1	,2	,2	94,4
5	12	2,4	2,4	96,8
52	2	,4	,4	97,2
6	7	1,4	1,4	98,6
8	6	1,2	1,2	99,8
9	1	,2	,2	100,0
Skupaj	500	100,0	100,0	

8.9 *Varnost osebnih podatkov*

Pomembnost varnosti osebnih podatkov v različnih situacijah smo preverjali v sklopu naslednjih vprašanj tako, da so anketiranci svoje strinjanje izrazili na Likrtovi lestvici, pri čemer je ocena ena pomenila »ne pomembna« ter ocena pet »zelo pomembna«.

8.9.1 Pomembnost varnosti osebnih podatkov

Tabela 49 nam prikazuje, kako pomembna se zdi anketirancem varnost osebnih podatkov ne glede na identifikacijski sistem in namen zbiranja podatkov.

Tabela 49: Frekvence ocen pomembnosti varnosti osebnih podatkov

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	2 Ne pomembno	2	,4	,4	,4
	3 Neodločen	14	2,8	2,8	3,2
	4 Pomembno	74	14,8	14,8	18,0
	5 Zelo pomembna	410	82,0	82,0	100,0
	Skupaj	500	100,0	100,0	

Ugotovimo lahko, da 410 anketirancev oziroma 82,0 % meni, da se njim zdi varnost osebnih podatkov zelo pomembna. 74 anketirancev oziroma 14,8 % meni, da je pomembna. 14 anketirancev oziroma 2,8 % je bilo pri tem vprašanju neodločenih. 2 anketiranca (0,4 %) menita, da varnost osebnih podatkov ni pomembna. Naslednjih pet podpoglavij se nanaša na varnost

osebnih podatkov pri različnih primerih vsakdanjega izpostavljanja, ko plačujemo s plačilnimi karticami različnih trgovcev.

8.9.2 Brezgotovinski promet (Pika, Magna itd.)

Tabela 50 nam prikazuje mnenje anketirancev glede varnosti osebnih podatkov pri plačilu s Pika, Magna itd. 243 oziroma 48,6 % anketirancev meni, da je varstvo podatkov zelo pomembno. 141 oziroma 28,2 % anketirancev meni, da je pomembno. 65 oziroma 13,0 % anketirancev je glede tega neodločenih. 31 oziroma 6,2 % anketirancev meni, da varnost podatkov ni pomembna ter 20 oziroma 4,0 % anketirancev meni, da varnost podatkov pri plačilu z zgoraj navedenimi plačilnimi karticami sploh ni pomembna.

Tabela 50: Frekvence ocen pomembnosti varnosti osebnih podatkov pri plačilu s plačilnimi karticami trgovcev (Pika, Magna, ipd.)

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ni pomembna	20	4,0	4,0	4,0
	2 Ni pomembno	31	6,2	6,2	10,2
	3 Neodločen	65	13,0	13,0	23,2
	4 Pomembno	141	28,2	28,2	51,4
	5 Zelo pomembna	243	48,6	48,6	100,0
	Skupaj	500	100,0	100,0	

8.9.3 Brezgotovinski promet (Mercator, Petrol, Spar,Tuš itd.)

Spodnja tabela 51 nam prikazuje, da pri uporabi kartic zvestobe 172 oziroma 34,4 % anketirancev meni, da je varstvo podatkov zelo pomembno.

Tabela 51: Frekvence ocen pomembnosti varnosti osebnih podatkov pri plačilu s karticami zvestobe (Mercator, Petrol, Spar, Tuš, ipd.)

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ni pomembna	43	8,6	8,6	8,6
	2 Ni pomembno	51	10,2	10,2	18,8
	3 Neodločen	106	21,2	21,2	40,0
	4 Pomembno	128	25,6	25,6	65,6
	5 Zelo pomembna	172	34,4	34,4	100,0
	Skupaj	500	100,0	100,0	

128 oziroma 25,6 % anketirancev meni, da je pomembno. 106 oziroma 21,2 % anketirancev je glede tega neodločenih. 51 oziroma 10,2 % anketirancev meni, da varnost podatkov ni pomembna ter 43 oziroma 8,6 % anketirancev meni, da varnost podatkov pri uporabi kartic zvestobe sploh ni pomembna.

8.9.4 Brezgotovinski promet (Mimovrste, Enaa, Eventim itd.)

Iz tabele 52 je razvidno, da je varstvo podatkov zelo pomembno pri registraciji v spletne trgovine za 275 anketirancev oziroma 55,0 %. 130 oziroma 26,0 % anketirancev jih meni, da je pomembno. 61 oziroma 12,2 % anketirancev je glede tega neodločenih.

Tabela 52: Frekvence ocen pomembnosti varnosti osebnih podatkov pri registraciji v spletne trgovine (Mimovrste, Enaa, Eventim ipd.)

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ni pomembna	13	2,6	2,6	2,6
	2 Ni pomembno	21	4,2	4,2	6,8
	3 Neodločen	61	12,2	12,2	19,0
	4 Pomembno	130	26,0	26,0	45,0
	5 Zelo pomembna	275	55,0	55,0	100,0
	Skupaj	500	100,0	100,0	

21 oziroma 4,2 % anketirancev meni, da varnost podatkov ni pomembna ter 13 oziroma 2,6 % anketirancev meni, da varnost podatkov sploh ni pomembna pri registraciji v spletne trgovine.

8.9.5 Brezgotovinski promet (mobilna telefonija, stacionarna telefonija, internet itd.)

Spodnja tabela 53 nam prikazuje, da je pri telekomunikacijskih storitvah varnost osebnih podatkov zelo pomembna za 249 anketirancev oziroma 49,8 %. 147 oziroma 29,4 % anketirancev meni, da je varnost podatkov pomembna. 77 oziroma 15,4 % anketirancev je v vezi s tem neodločenih. 16 oziroma 3,2 % anketirancev meni, da varnost podatkov ni pomembna ter 11 oziroma 2,2 % anketirancev meni, da sploh ni pomembna varnost podatkov pri naročanju telekomunikacijskih storitev.

Tabela 53: Frekvence ocen pomembnosti varnosti osebnih podatkov pri telekomunikacijskih storitvah (mobilna telefonija, stacionarna telefonija, internet)

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ni pomembna	11	2,2	2,2	2,2
	2 Ni pomembno	16	3,2	3,2	5,4
	3 Neodločen	77	15,4	15,4	20,8
	4 Pomembno	147	29,4	29,4	50,2
	5 Zelo pomembna	249	49,8	49,8	100,0
	Skupaj	500	100,0	100,0	

8.9.6 Osebni podatki v zdravstvu (zdravstvene kartice, zdravstveni kartoni itd.)

Tabela 54 nam prikazuje, da 345 oziroma 69,0 % anketirancev meni, da je zelo pomembno, da pri uporabi zdravstvenih kartic in zdravstvenih kartonov ohranimo varnost podatkov. 105 oziroma 21,0 % anketirancev meni, da je to pomembno. 42 oziroma 8,4 % anketirancev je glede tega neodločenih. 6 oziroma 1,2 % anketirancev meni, da varnost podatkov ni pomembna ter 2 anketiranca (0,4 %) menita, da ohranitev varnosti podatkov pri uporabi zdravstvenih kartic in zdravstvenih kartonov sploh ni pomembna.

Tabela 54: Frekvence ocen pomembnosti varovanja osebnih podatkov zdravstvenih kartic in zdravstvenih kartonov

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ni pomembna	2	,4	,4	,4
	2 Ni pomembno	6	1,2	1,2	1,6
	3 Neodločen	42	8,4	8,4	10,0
	4 Pomembno	105	21,0	21,0	31,0
	5 Zelo pomembna	345	69,0	69,0	100,0
	Skupaj	500	100,0	100,0	

Največ anketirancev je mnenja, da je varovanje osebnih podatkov v zdravstvu zelo pomembno.

8.10 *Uporaba biometričnih podatkov*

V nadaljevanju ugotavljamo,v kolikšni meri anketiranci podpirajo uporabo biometričnih sistemov pri delu policije. Anketiranci so svoje (ne)podpiranje izrazili na Likertovi lestvici, pri čemer je ocena ena pomenila »sploh ne podpiram« ter ocena pet »popolnoma podpiram«.

8.10.1 Delo kriminalistov

Ugotovili smo (tabela 55), da 166 oziroma 33,2 % anketirancev popolnoma podpira uporabo biometrije za varovanje in zbiranje zaupnih podatkov pri delu kriminalistov in policije. 237 oziroma 47,4 % anketirancev to podpira. 73 oziroma 14,6 % anketirancev je glede tega neodločenih.

Tabela 55: Frekvenca strinjanja z uporabo biometričnih podatkov, ki jih pri svojem delu zbirajo kriminalisti in policija

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ne podpiram	10	2,0	2,0	2,0
	2 Ne podpiram	14	2,8	2,8	4,8
	3 Neodločen	73	14,6	14,6	19,4
	4 Podpiram	237	47,4	47,4	66,8
	5 Popolnoma podpiram	166	33,2	33,2	100,0
	Skupaj	500	100,0	100,0	

14 oziroma 2,8 % anketirancev tega ne podpira ter 10 oziroma 2,0 % anketirancev tega, da bi kriminalisti in policija pri svojem delu uporabili biometrijo za varovanje zaupnih podatkov, sploh ne podpira. Največ anketirancev podpira uporabo biometričnih podatkov, ki jih pri svojem delu zbirajo kriminalisti in policija.

8.10.2 Preiskava mesta zločina

Iz tabele 56 je razvidno, da 266 oziroma 53,2 % anketirancev pri kriminalističnem delu na mestih zločina, ko se podatki zbrani na mestu zločina primerjajo z bazami podatkov pravnomočno obsojenih zločincev, popolnoma podpira uporabo biometričnih podatkov. 197 oziroma 39,4 % anketirancev to podpira. 27 oziroma 5,4 % anketirancev je glede tega neodločenih.

Tabela 56: Frekvenca strinjanja z uporabo biometričnih podatkov pri kriminalističnem delu na mestih zločina, če se podatki zbrani na mestu zločina primerjajo z bazami podatkov pravnomočno obsojenih zločincev

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ne podpiram	3	,6	,6	,6
	2 Ne podpiram	7	1,4	1,4	2,0
	3 Neodločen	27	5,4	5,4	7,4
	4 Podpiram	197	39,4	39,4	46,8
	5 Popolnoma podpiram	266	53,2	53,2	100,0
	Skupaj	500	100,0	100,0	

7 oziroma 1,4 % anketirancev tega ne podpira ter 3 oziroma 0,6 % anketirancev sploh ne podpira uporabe biometričnih podatkov pri kriminalističnem delu na mestih zločina, kadar se podatki zbrani na mestu zločina primerjajo z bazami podatkov pravnomočno obsojenih zločincev.

8.10.3 Izdelava baz podatkov kriminalcev

Iz tabele 57 je razvidno, da pri izdelavi baz s podatki kriminalcev 297 anketirancev oziroma 59,4 %, popolnoma podpira uporabo biometričnih podatkov. 166 oziroma 33,2 % anketirancev to podpira. 29 oziroma 5,8 % anketirancev je glede tega neodločenih.

Tabela 57: Frekvenca strinjanja z uporabo biometričnih podatkov za izdelavo baz s podatki o resnih kriminalcih in zločincih

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ne podpiram	2	,4	,4	,4
	2 Ne podpiram	6	1,2	1,2	1,6
	3 Neodločen	29	5,8	5,8	7,4
	4 Podpiram	166	33,2	33,2	40,6
	5 Popolnoma podpiram	297	59,4	59,4	100,0
	Skupaj	500	100,0	100,0	

6 oziroma 1,2 % anketirancev tega ne podpira ter 2 anketiranca (0,4 %) sploh ne podpirata izdelave baz s podatki o kriminalcih in zločincih pri čemer bi uporabili biometrične podatke.

8.10.4 Delo prometne policije za identifikacijo voznikov

V tabeli 58 prikazujemo ugotovitve glede mnenj anketirancev o delu prometne policije, kadar policist ustavi prometnega prekrškarja in hkrati primerja njegove podatke s podatki o obsojencih na begu. 149 anketirancev oziroma 29,8 %, pri tem popolnoma podpira uporabo biometričnih podatkov.

Tabela 58: Frekvenca strinjanja z uporabo biometričnih podatkov pri delu prometne policije, če policist ustavi prometnega prekrškarja in hkrati primerja njegove podatke s podatki obsojencev na begu

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh ne podpiram	21	4,2	4,2	4,2
	2 Ne podpiram	54	10,8	10,8	15,0
	3 Neodločen	91	18,2	18,2	33,2
	4 Podpiram	185	37,0	37,0	70,2
	5 Popolnoma podpiram	149	29,8	29,8	100,0
	Skupaj	500	100,0	100,0	

185 oziroma 37,0 % anketirancev to podpira. 91 oziroma 18,2 % anketirancev je v vezi s tem neodločenih. 54 oziroma 10,8 % anketirancev tega ne podpira. 21 oziroma 4,2 % anketirancev sploh ne podpira tega, da bi prometna policija pri svojem delu (v primeru, ko ustavijo prometnega prekrškarja) primerjala podatke s podatki obsojencev na begu in bi pri tem uporabila biometrične podatke. Največ anketirancev podpira uporabo biometričnih podatkov, pri osebni identifikaciji, ki jo izvaja policija pri kontroli prometa.

8.11 *Percepcija terorističnega napada na ZDA 11/9*

Pri naslednjem vprašanju smo želeli, da bi anketiranci pomislili na teroristični napad, ki se je zgodil 11. septembra l. 2001 v Združenih državah Amerike. Želeli smo, da anketiranci na Likertovi lestvici ocenijo moč terorističnega napada. Tako lahko iz tabele 59 ugotovimo, da se 194 anketirancev oziroma 38,8 % popolnoma strinja, da je bil omenjeni teroristični napad izjemno hud. 133 oziroma 26,6 % anketirancev se strinja da je bil napad hud.

Tabela 59: Frekvenca percepcije terorističnega napada v ZDA 11. Septembra 2011

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Sploh se ne strinjam	33	6,6	6,6	6,6
	2 Se ne strinjam	40	8,0	8,0	14,6
	3 Neodločen	100	20,0	20,0	34,6
	4 Se strinjam	133	26,6	26,6	61,2
	5 Popolnoma se strinjam	194	38,8	38,8	100,0
	Skupaj	500	100,0	100,0	

100 oziroma 20,0 % je glede tega neodločenih. 40 oziroma 8,0 % anketirancev se ne strinja s tem, da bi bil teroristični napad izjemno hud ter 33 oziroma 6,6 % anketirancev se sploh ne strinja s tem, da bi bil teroristični napad 11. Septembra l. 2001 v ZDA izjemno hud.

8.12 *Učinkovitost identifikacijskih sistemov*

V nadaljevanju prikazujemo ugotovitve glede tega, kateri identifikacijski sistem je po mnenju anketirancev bolj učinkovit. Anketiranci so svoje mnenje glede sistemov izrazili na Likertovi lestvici, pri čemer je ocena ena pomenila »slaba učinkovitost« ter ocena pet »odlična učinkovitost«.

8.12.1 Biometrični sistemi

Tako lahko iz spodnje tabele 60 razberemo, da 139 oziroma 27,8 % anketirancev meni, da so biometrični sistemi odlično učinkoviti.

Tabela 60: Frekvenca percepcije učinkovitosti biometričnih sistemov

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Slaba učinkovitost	3	,6	,9	,9
	2	11	2,2	3,3	4,1
	3 Neodločen	67	13,4	19,8	24,0
	4	118	23,6	34,9	58,9
	5 Odlična učinkovitost	139	27,8	41,1	100,0
	Skupaj	338	67,6	100,0	
	Ne morem oceniti	162	32,4		
Skupaj		500	100,0		

118 oziroma 23,6 % anketirancev meni, da so učinkoviti. 67 oziroma 13,4 % anketirancev je glede tega neodločenih. 11 oziroma 2,2 % anketirancev meni, da biometrični sistemi niso učinkoviti ter 3 anketiranci (0,6 %) menijo, da so biometrični sistemi slabo učinkoviti. 162 anketirancev oziroma 32,4 % ni moglo oceniti učinkovitosti biometričnega sistema zaradi pomanjkanja izkušenj.

8.12.2 Kartični sistemi

Nadalje je iz spodnje tabele 61 razvidno, da 66 oziroma 13,2 % anketirancev meni, da imajo kartični identifikacijski sistemi odlično učinkovitost. 151 anketirancev oziroma 30,2 % meni, da so učinkoviti. 159 anketirancev oziroma 31,8 % je gleda tega neodločenih. 48 anketirancev oziroma 9,6 % meni, da kartični identifikacijski sistemi niso učinkoviti ter 22 oziroma 4,4 % anketirancev meni, da so klasični kartični sistemi slabo učinkoviti. 54 oziroma 10,8 % anketirancev ni moglo oceniti učinkovitost kartičnega sistema zaradi pomanjkanja izkušenj.

Tabela 61: Frekvenca percepcije učinkovitosti klasičnih (kartičnih) sistemov

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	1 Slaba učinkovitost	22	4,4	4,9	4,9
	2	48	9,6	10,8	15,7
	3 Neodločen	159	31,8	35,7	51,3
	4	151	30,2	33,9	85,2
	5 Odlična učinkovitost	66	13,2	14,8	100,0
	Skupaj	446	89,2	100,0	
	Ne morem oceniti	54	10,8		
Skupaj		500	100,0		

Ugotovimo še lahko (tabela 62), da 317 anketirancev oziroma 63,4 % meni, da je biometrična tehnologija primernejša od klasičnega – kartičnega sistema.

Tabela 62: Frekvenca primerjave primernosti identifikacijskih sistemov

		Absolutna frekvenca	Relativna frekvenca	Veljavna relativna frekvenca	Kumulativna relativna frekvenca
Veljavno	Klasični (kartični) sistemi	183	36,6	36,6	36,6
	Biometrične tehnologije	317	63,4	63,4	100,0
	Skupaj	500	100,0	100,0	

9 TESTIRANJE HIPOTEZ

Za statistično obdelavo podatkov smo uporabili programski paket SPSS. Uporabljene so bile tako univariatne kot multivariatne statistične metode. Hipoteze smo preverjali s pomočjo korelacijske analize, t-testa, faktorsko analizo in analizo variance (ANOVA). Na raziskovalna vprašanja smo poskušali odgovoriti s pomočjo Pearsonovega koeficienta korelacije in enosmerno analizo variance ter post hoc testi. Preden smo izvedli regresijsko analizo, smo opravili faktorsko analizo, da bi zmanjšali število spremenljivk in ugotovili strukturo našega celostnega vprašalnika.

9.1 *Faktorska analiza po spremenljivkah*

Primernost podatkov za izvedbo faktorske analize smo preverili s pomočjo:

a) opisne statistike: normalna porazdelitev na podlagi vrednosti poševnosti in sploščenosti krivulje; spremenljivke, kjer je vrednost sploščenosti in poševnosti presegla -3 in 3 smo izločili iz nadaljnjih obdelav,

b) pregleda korelacijskih koeficientov, kjer smo zagotovili, da med podatki ni multikolinearnosti (izločili smo eno izmed dveh spremenljivk, pri katerih je bil Pearsonov koeficient korelacije večji od (-)0,9 in manjši od (-)0,1, saj to pomeni, da sta dve spremenljivki v premočni ali prešibki korelaciji in je tako zagotovo ena odveč),

c) Kaiser-Meyer-Olkinove (KMO) mere primernosti vzorca; KMO mera ustreznosti vzorca nam pokaže, ali so podatki ustrezni za faktorsko analizo; višja ko je mera KMO, bolj so podatki ustrezni, optimalno pa je, ko je KMO večja od 0,8, še sprejemljiva mera pa je med 0,5 in 0,6, pod 0,5 podatki niso ustrezni za faktorsko analizo in

d) Cronbachovega koeficienta α, s katerim merimo zanesljivost vprašalnika (Reliability Analysis), kar je lastnost vprašalnika, da daje pri ponovljenih merjenjih istih lastnosti pri istih osebah enake rezultate; vrednosti, ki jih Cronbach α lahko zavzame, so med 0 in 1, pri čemer pomenijo vrednosti nad 0,8 visoko zanesljivost, med 0,6 in 0,8 pa srednjo zanesljivost.

Uporabljena metoda faktorske analize je bila metoda glavnih komponent. Pri večini spremenljivk smo dobili enofaktorske strukture. Pri določanju števila

faktorjev smo se osredotočili na kriterije metode in na uporabnost dobljene rešitve in sicer: lastne vrednosti faktorjev so morale preseči vrednost 1, skupni delež pojasnjene variance je moral biti čim večji oziroma preseči vsaj 50 %, s pomočjo kolenskega diagrama smo pogledali točko preloma krivulje, faktorji pa so morali imeti logično strukturo. Število spremenljivk, ki smo jih vzeli v izvedbo faktorske analize, je bilo odvisno od same vsebine ter kasneje od pregleda komunalitet; spremenljivke z nizkimi komunalitetami smo izločili iz nadaljnjih obdelav.

Opravili smo faktorsko analizo posameznih sklopov celostnega vprašalnika. V vseh primerih smo dobili enofaktorsko strukturo, pri čemer je bila najnižja količina pojasnjene variance 53,4 odstotke, najnižji koeficient ustreznosti vzorčenja (KMO) je bil 0,73 in najnižji α-koeficient zanesljivosti je znašal 0,822. Faktorizacija po spremenljivkah je prikazana v nadaljevanju.

9.1.1 Seznanjenost z biometričnimi sistemi

V faktorsko analizo smo zajeli spremenljivke, ki se nanašajo na vprašanje: »*V kolikšni meri anketiranci poznajo biometrične sisteme za identifikacijo?*«. V tabeli 63 so prikazane spremenljivke - odgovori, njihove faktorske uteži, aritmetične sredine ter standardni odkloni.

Tabela 63: Faktor 1 (Seznanjenost z biometričnimi sistemi)

Spremenljivke	Faktorske uteži	Aritmetična sredina	Standardni odklon
Prepoznava prstnega odtisa.	0,71	3,58	1,12
Prepoznava oblike roke.	0,73	2,22	1,11
Prepoznava podpisa.	0,62	3,55	1,18
Prepoznava ožilja roke.	0,63	1,70	0,94
Prepoznava obraza s pomočjo kamere.	0,77	3,06	1,25
Prepoznava šarenice s pogledom v skener.	0,80	2,66	1,23
Prepoznava DNK: analiza vzorca krvi, las itd.	0,73	2,96	1,34
Prepoznava glasu.	0,81	2,96	1,21
Delež pojasnjene variance	**53,4%**		
Cronbach alpha	**0,874**		
KMO	**0,885**		

Sestavljajo ga spremenljivke poglavij 9.1.2 do 9.1.9, ki predstavljajo kratke odgovore, na podlagi katerih so anketiranci ocenjevali poznavanje posameznega biometričnega sistema na pet stopinjski lestvici, pri čemer je ocena ena pomenila »sploh nisem seznanjen« ter ocena pet »zelo dobro sem seznanjen«. V obdelavo smo vzeli vse spremenljivke in dobili enofaktorsko strukturo (lastne vrednosti večje od 1). S faktorjem »*Seznanjenost z biometričnimi sistemi*« pojasnimo 53,4 % variance. KMO znaša 0,885, α-koeficient zanesljivosti pa znaša 0,874. Najvišjo lastno vrednost (faktorsko utež) ima spremenljivka z odgovorom »*Prepoznava glasu*« in znaša 0,81, najnižjo lastno vrednost pa spremenljivka z odgovorom »*Prepoznava podpisa*« in znaša 0,62.

9.1.2 Sprejemljivost uporabe biometrije za primere vsakdanje uporabe

V faktorsko analizo smo zajeli spremenljivke, ki se nanašajo na mnenja o sprejemljivosti biometričnih sistemov pri vsakdanji uporabi. Sestavljajo ga spremenljivke poglavij 9.5.1 do 9.5.5, ki predstavljajo kratke odgovore, na podlagi katerih so anketiranci izrazili svoje mnenje, glede sprejemljivosti biometričnega sistema na pet stopinjski lestvici, pri čemer je ocena ena pomenila »sploh ni sprejemljiva« ter ocena pet »zelo sprejemljiva«. V obdelavo smo vzeli vse spremenljivke in dobili enofaktorsko strukturo (lastne vrednosti večje od 1). V tabeli št. 64 so prikazane spremenljivke - odgovori, njihove faktorske uteži, aritmetične sredine ter standardni odkloni.

Tabela 64: Faktor 2 (Sprejemljivost uporabe biometrije v vsakdanjem življenju)

Spremenljivke	Faktorske uteži	Aritmetična sredina	Standardni odklon
Za preverjanje identitete pri plačilu s kreditno kartico.	0,84	3,46	1,17
Pri dvigovanju denarja na bankomatu.	0,85	3,42	1,22
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	0,78	3,71	1,18
Pri preverjanju preteklosti posameznika.	0,75	3,22	1,26
Delež pojasnjene variance	**67,2%**		
Cronbach alpha	**0,835**		
KMO	**0,730**		

S faktorjem »*Sprejemljivost uporabe biometrije v vsakdanjem življenju*« pojasnimo 67,2 % variance. KMO znaša 0,730, α-koeficient zanesljivosti pa znaša 0,835. Najvišjo lastno vrednost (faktorsko utež) ima spremenljivka z odgovorom »*Pri dvigovanju denarja z bankomata*« in znaša 0,85, najnižjo lastno vrednost pa spremenljivka z odgovorom »*Pri preverjanju preteklosti posameznika*« in znaša 0,75.

9.1.3 Sprejemljivost uporabe biometrije za primere protiterorističnega delovanja

V faktorsko analizo smo zajeli spremenljivke, ki se nanašajo na mnenja o sprejemljivosti biometričnih sistemov pri protiterorističnemu delovanju. Sestavljajo ga spremenljivke poglavij 9.6.1 do 9.6.5, ki predstavljajo kratke odgovore, na podlagi katerih so anketiranci izrazili svoje mnenje glede sprejemljivosti biometričnega sistema na pet stopinjski lestvici, pri čemer je ocena ena pomenila »sploh ni sprejemljiva« ter ocena pet »zelo sprejemljiva«. V obdelavo smo vzeli vse spremenljivke in dobili enofaktorsko strukturo (lastne vrednosti večje od 1). S faktorjem »*Sprejemljivost uporabe biometrije za primere protiterorističnega delovanja*« pojasnimo 62,8 % variance. KMO znaša 0,830, α-koeficient zanesljivosti pa znaša 0,876. V tabeli 65 so prikazane spremenljivke - odgovori, njihove faktorske uteži, aritmetične sredine ter standardni odkloni.

Tabela 65: Faktor 3 (Sprejemljivost uporabe biometrije za primere protiterorističnega delovanja)

Spremenljivke	Faktorske uteži	Aritmetična sredina	Standardni odklon
Pri kontroli potnih listov.	0,68	3,94	0,94
V potnih listih.	0,82	4,18	0,88
Ob vstopu v državne stavbe.	0,80	3,92	1,00
Na letališčih pri prijavi na let.	0,81	4,14	0,93
Na vozniškem dovoljenju.	0,83	3,42	1,13
Pri izposoji avtomobila (rent a car).	0,76	3,26	1,19
Delež pojasnjene variance	**62,8%**		
Cronbach alpha	**0,876**		
KMO	**0,830**		

Najvišjo lastno vrednost (faktorsko utež) ima spremenljivka z odgovorom »*Na vozniškem dovoljenju*« in znaša 0,83, najnižjo lastno vrednost pa spremenljivka z odgovorom »*Pri kontroli potnih listov*« in znaša 0,68.

9.1.4 Varnost osebnih podatkov

V faktorsko analizo smo zajeli spremenljivke, ki se nanašajo na mnenja glede pomembnosti varnosti osebnih podatkov glede na različne situacije. Sestavljajo ga spremenljivke poglavij od 9.9.1 do 9.9.6, ki predstavljajo kratke odgovore, na podlagi katerih so anketiranci izrazili svoje mnenje glede pomembnosti varnosti osebnih podatkov na pet stopinjski lestvici, pri čemer je ocena ena pomenila »sploh ni pomembna« ter ocena pet »zelo pomembna«. V obdelavo smo vzeli vse spremenljivke in dobili enofaktorsko strukturo (lastne vrednosti večje od 1). S faktorjem »*Pomembnost varnosti osebnih podatkov*« pojasnimo 59,2 % variance. KMO znaša 0,758, α-koeficient zanesljivosti pa znaša 0,822. V tabeli 66 so prikazane spremenljivke - odgovori, njihove faktorske uteži, aritmetične sredine ter standardni odkloni.

Tabela 66: Faktor 4 (Pomembnost varnosti osebnih podatkov)

Spremenljivke	Faktorske uteži	Aritmetična sredina	Standardni odklon
Pomembnost varnosti osebnih podatkov na splošno	0,19	4,78	0,50
Pri plačilu s plačilnimi karticami trgovcev (Pika, Magna ipd.).	0,85	4,11	1,10
S karticami zvestobe (Mercator, Petrol, Spar, Tuš ipd.).	0,87	3,76	1,28
Pri registraciji v spletne trgovine (Mimovrste, Enaa, Eventim ipd.).	0,87	4,27	1,00
Pri naročanju telekomunikacijskih storitev (mobilna telefonija, stacionarna telefonija, internet).	0,84	4,21	0,97
Delež pojasnjene variance	**59,2%**		
Cronbach alpha	**0,822**		
KMO	**0,758**		

Najvišjo lastno vrednost (faktorsko utež) imata spremenljivki z odgovorom »*S karticami zvestobe (Mercator, Petrol, Spar, Tuš ipd.)*« in »*Pri registraciji v spletne trgovine (Mimovrste, Enaa, Eventim ipd.)*« *ter* znaša 0,87, najnižjo lastno vrednost pa spremenljivka z odgovorom »*Pomembnost varnosti osebnih podatkov na splošno*« in znaša 0,19.

9.2 *Regresijska analiza vpliva varnosti osebnih podatkov na sprejemljivost biometrije*

Z regresijsko analizo smo ugotavljali moč povezave med spremenljivkami: »*Sprejemljivost uporabe biometrije*« in dejavnikom »*Varnost osebnih podatkov*« s ciljem odgovora na hipotezo 1, ki se glasi: »*Varnost osebnih podatkov ne vpliva znatno na oceno sprejemljivosti uporabe sistemov množičnega nadzora (identifikacije) v varnostnih sistemih*«. V tem delu raziskave smo upoštevali biometrične identifikacijske sisteme. Zanimalo pa nas je podrobneje, ali ima dejavnik »*Varnost osebnih podatkov*« vpliv na »*Sprejemljivost biometrije v vsakdanjem življenju*« in, če ima ta isti dejavnik vpliv v primeru, ko gre za uporabo biometrije v protiterorističnih aktivnostih, torej na »*Sprejemljivost uporabe biometrije pri protiterorističnem delovanju*«.

Iz izvedene statistike (tabela 67) lahko sklepamo, da »*Varnost osebnih podatkov*« (t=1,555; α=0,05; p_α=0,120) značilno NE vpliva na oceno »*Sprejemljivosti uporabe biometrije*« v primeru protiterorističnih aktivnosti. Koeficient naklona v regresijskem modelu pokaže, da je »*Sprejemljivost biometričnih sistemov*« *= 2,824+0,121* »Varost osebnih podatkov*« enak 0,121 vendar ni statistično značilno različen od 0 (p=0,120).

Tabela 67: Vpliv varnosti osebnih podatkov na sprejemljivost biometrije

	koeficient[a]	Nestandardizirani koeficienti		Standardizirani koeficienti		
model		B	Stand. napaka	beta	t	Stat. znač.
1	(Konstanta)	2,824	,373		7,567	,000
	Varnost osebnih podatkov	,121	,078	,070	1,555	,120

a. Odvisna spremenjivka: spremenljivke za sprejemljivost biometričnih sistemov za primer protiterorističnih aktivnosti

R^2=0,05

Na »*Varnost osebnih podatkov*« pa vpliva »*Sprejemljivost uporabe biometrije v vsakdanjem življenju*« (t =2,733; α=0,015; p_α=0,006) (tabela 68). V tem

primeru je koeficient naklona v modelu »*Sprejemljivost biometričnih sistemov*« = *2,76+0,206** »*Varost osebnih podatkov*« enak 0,206 in je statistično značilno različen od 0 (p=0,006).

Tabela 68: Vpliv varnosti osebnih podatkov na sprejemljivost biometrije

Koeficient[a]		Nestandardizirani koeficienti		Standardizirani koeficienti		
Model		B	Stand. napaka	beta	t	Stat. znač.
1	(Konstanta)	2,796	,363		7,709	,000
	Varnost osebnih podatkov	,206	,075	,122	2,733	,006

a. Odvisna spremenljivka: spremenljivke za sprejemljivost biometričnih sistemov v vsakdanjem življenju

R^2=0,015

9.3 *T-test učinkovitosti identifikacijskih sistemov*

S korelacijsko analizo in t-testom smo ugotavljali povezavo spremenljivk identifikacijskih sistemov (biometrični sistemi in kartični sistemi) z učinkovitostjo, s ciljem odgovoriti na 3 hipotezo, ki se glasi: *Biometrični sistemi za množični nadzor v procesih identifikacije so učinkovitejši kot sedaj poznani alternativni (kartični sistemi) sistemi*.

V tabeli 69 sta predstavljeni 2 spremenljivki in sicer »*Klasični kartični sistemi*« ter »*Biometrični sistemi*« pri čemer merimo njuno povezanost. Večji vpliv na učinkovitost identifikacijskih sistemov, ima spremenljivka »*Biometrični sistemi*« (64,1 %), manj vpliva med statistično pomembnimi spremenljivkami pa ima spremenljivka »*Klasični kartični sistemi*« (35,9 %).

Tabela 69: Učinkovitost identifikacijskih sistemov (kartični sistemi)

Korelacijska tabela			Klasični (kartični) sistemi					
			1 Slaba učinkovitost	2	3	4	5 Odlična učinkovitost	Skupaj
Primerjava sistemov	Klasični (kartični)	Št. anket.	6	5	46	66	37	160
		% v klasični (kartični) sistemi	27,3%	10,4%	28,9%	43,7%	56,1%	35,9%
	Biometrične tehnologije	Št. anket.	16	43	113	85	29	286
		% v klasični (kartični) sistemi	72,7%	89,6%	71,1%	56,3%	43,9%	64,1%
skupaj		Št. anket.	22	48	159	151	66	446
		% v klasični (kartični) sistemi	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

V tabeli 70 sta predstavljeni 2 spremenljivki, od katerih je tokrat spremenljivka »*Biometrični sistemi*« odvisna spremenljivka.

Tabela 70: Učinkovitost identifikacijskih sistemov (biometrični sistemi)

Korelacijska tabela			Biometrični sistemi					
			1 Slaba učinkovitost	2	3	4	5 Odlična učinkovitost	Skupaj
Primerjava sistemov	Klasični (kartični) sistemi	Št. anket.	3	6	40	34	26	109
		% v biometrični sistemi	100,0%	54,5%	59,7%	28,8%	18,7%	32,2%
	Biometrične tehnologije	Št. anket.	0	5	27	84	113	229
		% v biometrični sistemi	,0%	45,5%	40,3%	71,2%	81,3%	67,8%
Skupaj		Št. anket.	3	11	67	118	139	338
		% v biometrični sistemi	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Večji vpliv na učinkovitost identifikacijskih sistemov, ima spremenljivka »*Biometrični sistemi*« (67,8 %), manj vpliva med statistično pomembnimi spremenljivkami pa ima spremenljivka »*Klasični kartični sistemi*« (32,2 %).

V tabeli 71 prikazujemo opisne statistike odvisnih spremenljivk, ki jih bomo uporabili v t-testu.

Tabela 71: Opisne statistike za odvisne spremenljivke

		Povpr.	N	Stand. odklon	Stand. napaka povpr.
Par 1	Biometrični sistemi	4,09	326	,900	,050
	Klasični (kartični) sistemi	3,34	326	1,054	,058

Določimo ničelno hipotezo:
H_0: Povprečna ocena učinkovitosti biometričnega sistema je enaka povprečni oceni učinkovitosti kartičnega sistema.

Tabela 72 nam prikazuje statistično značilnost za biometrični sistem (p=0,00), ki je nižja od stopnje rizika p=0,05 kar nam pove, da so podatki statistično značilni (nizka verjetnost slučajne razlike v variancah vzorcev).

Tabela 72: t-test za odvisne spremenljivke

		Parne razlike							
					95% interval zaupanja odklonov				
		Povpr.	Stand. odklon	Stand. napaka povpr.	Spod.	Zgor.	t	df	Stat. znač. (2-stranski)
Par 1	Biometrični sistemi - Klasični (kartični) sistemi	,755	1,348	,075	,608	,901	10,109	325	,000

Ker je stopnja statistične značilnosti (signifikanca) manjša od 0,05, lahko ničelno hipotezo zavrnemo in sprejmemo osnovno raziskovalno hipotezo.

9.4 *Analiza variance ANOVA po spremenljivkah*

Z analizo variance smo v nadaljevanju poskušali ugotoviti ali se povprečna sprejemljivost biometričnih sistemov razlikuje med anketiranci glede na starostne in izobrazbene skupine. Pred začetkom statističnih analiz bomo predstavili opisne statistike vseh spremenljivk. Poleg aritmetične sredine smo preverili tudi mere variabilnosti, t.j. varianco in standardni odklon.

Tabela 73 prikazuje opisne statistike za spremenljivko »*starost*«, ki jo bomo uporabili v analizi variance.

Tabela 73: Opisne statistike za spremenljivko »starost«

						95% interval zaupanja za povpr.			
		N	Povpr.	Stand. odklon	Stand. napaka	Spod. meja	Zgor. meja	Min.	Maks.
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	14-19	19	3,58	1,305	,299	2,95	4,21	1	5
	20-29	104	3,47	1,114	,109	3,25	3,69	1	5
	30-39	115	3,47	1,209	,113	3,25	3,69	1	5
	40-49	132	3,42	1,192	,104	3,22	3,63	1	5
	50-59	130	3,29	1,103	,097	3,10	3,48	1	5
	Skupaj	500	3,42	1,160	,052	3,31	3,52	1	5
Za preverjanje identitete pri plačilu s kreditno kartico.	14-19	19	3,00	1,202	,276	2,42	3,58	1	5
	20-29	104	3,21	1,138	,112	2,99	3,43	1	5
	30-39	115	3,62	1,128	,105	3,41	3,83	1	5
	40-49	132	3,64	1,092	,095	3,46	3,83	1	5
	50-59	130	3,39	1,254	,110	3,17	3,61	1	5
	Skupaj	500	3,46	1,169	,052	3,36	3,56	1	5
Pri dvigovanju denarja na bankomatu.	14-19	19	3,42	1,216	,279	2,83	4,01	1	5
	20-29	104	3,09	1,208	,118	2,85	3,32	1	5
	30-39	115	3,52	1,180	,110	3,30	3,74	1	5
	40-49	132	3,57	1,173	,102	3,37	3,77	1	5
	50-59	130	3,43	1,276	,112	3,21	3,65	1	5
	Skupaj	500	3,42	1,219	,055	3,31	3,52	1	5
Pri dostopanju	14-19	19	3,42	1,346	,309	2,77	4,07	1	5

do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	20-29	104	3,67	1,101	,108	3,46	3,89	1	5
	30-39	115	3,78	1,176	,110	3,57	4,00	1	5
	40-49	132	3,80	1,149	,100	3,61	4,00	1	5
	50-59	130	3,64	1,276	,112	3,42	3,86	1	5
	Skupaj	500	3,71	1,186	,053	3,61	3,82	1	5
Pri preverjanju preteklosti posameznika.	14-19	19	2,74	1,327	,304	2,10	3,38	1	5
	20-29	104	3,10	1,250	,123	2,85	3,34	1	5
	30-39	115	3,31	1,195	,111	3,09	3,53	1	5
	40-49	132	3,33	1,305	,114	3,10	3,55	1	5
	50-59	130	3,21	1,256	,110	2,99	3,43	1	5
	Skupaj	500	3,22	1,259	,056	3,11	3,33	1	5
Pri kontroli potnih listov.	14-19	19	4,00	1,000	,229	3,52	4,48	1	5
	20-29	104	3,93	,895	,088	3,76	4,11	1	5
	30-39	115	4,01	,950	,089	3,83	4,18	1	5
	40-49	132	3,92	,917	,080	3,76	4,07	1	5
	50-59	130	3,91	1,000	,088	3,73	4,08	1	5
	Skupaj	500	3,94	,943	,042	3,86	4,02	1	5
V potnih listih.	14-19	19	4,00	,943	,216	3,55	4,45	1	5
	20-29	104	4,17	,918	,090	3,99	4,35	1	5
	30-39	115	4,10	,946	,088	3,92	4,27	1	5
	40-49	132	4,20	,863	,075	4,06	4,35	1	5
	50-59	130	4,25	,781	,068	4,12	4,39	1	5
	Skupaj	500	4,18	,876	,039	4,10	4,25	1	5
Na letališčih pri prijavi na let.	14-19	19	3,89	,994	,228	3,42	4,37	1	5
	20-29	104	3,96	1,088	,107	3,75	4,17	1	5
	30-39	115	4,15	1,002	,093	3,96	4,33	1	5
	40-49	132	4,17	,884	,077	4,01	4,32	1	5
	50-59	130	4,30	,754	,066	4,17	4,43	1	5
	Skupaj	500	4,14	,936	,042	4,06	4,23	1	5
Ob vstopu v državne stavbe.	14-19	19	3,53	1,124	,258	2,98	4,07	1	5
	20-29	104	3,74	1,070	,105	3,53	3,95	1	5
	30-39	115	3,95	1,033	,096	3,76	4,14	1	5
	40-49	132	3,98	,973	,085	3,82	4,15	1	5
	50-59	130	4,02	,915	,080	3,86	4,17	1	5

	Skupaj	500	3,92	1,003	,045	3,83	4,00	1	5
Na vozniškem dovoljenju.	14-19	19	3,26	,991	,227	2,79	3,74	1	5
	20-29	104	3,33	1,178	,115	3,10	3,56	1	5
	30-39	115	3,43	1,229	,115	3,20	3,65	1	5
	40-49	132	3,42	1,064	,093	3,24	3,61	1	5
	50-59	130	3,49	1,094	,096	3,30	3,68	1	5
	Skupaj	500	3,42	1,130	,051	3,32	3,52	1	5
Pri izposoji avtomobila (rent a car).	14-19	19	3,00	1,247	,286	2,40	3,60	1	5
	20-29	104	3,13	1,285	,126	2,88	3,38	1	5
	30-39	115	3,33	1,212	,113	3,11	3,55	1	5
	40-49	132	3,22	1,086	,095	3,03	3,41	1	5
	50-59	130	3,37	1,208	,106	3,16	3,58	1	5
	Skupaj	500	3,26	1,196	,053	3,15	3,36	1	5
Pri vpisu v šolo.	14-19	19	2,74	1,195	,274	2,16	3,31	1	5
	20-29	104	2,60	1,195	,117	2,36	2,83	1	5
	30-39	115	2,73	1,320	,123	2,49	2,97	1	5
	40-49	132	2,69	1,236	,108	2,48	2,90	1	5
	50-59	130	2,60	1,217	,107	2,39	2,81	1	5
	Skupaj	500	2,66	1,238	,055	2,55	2,77	1	5

Tabela 74 prikazuje rezultate Levenovega testa, za sprejem ali zavrnitev ničelne hipoteze H_0 o enakosti varianc med starostnimi skupinami in je predpogoj, da lahko analizo variance izvedemo. Določimo ničelno hipotezo:
H_0: Starostne skupine se med seboj ne razlikujejo statistično značilno.

Tabela 74: Test homogenosti varianc za spremenljivko »starost«

	Levenova statistika	df1	df2	Stat. znač.
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	,768	4	495	,546
Za preverjanje identitete pri plačilu s kreditno kartico.	1,558	4	495	,184
Pri dvigovanju denarja na bankomatu.	,627	4	495	,643

Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	1,413	4	495	,229
Pri preverjanju preteklosti posameznika.	,642	4	495	,633
Pri kontroli potnih listov.	,457	4	495	,768
V potnih listih.	,625	4	495	,645
Na letališčih pri prijavi na let.	1,483	4	495	,206
Ob vstopu v državne stavbe.	1,656	4	495	,159
Na vozniškem dovoljenju.	1,523	4	495	,194
Pri izposoji avtomobila (rent a car).	1,177	4	495	,320
Pri vpisu v šolo.	,223	4	495	,925

Ugotavljamo, da se variance med skupinami ne razlikujejo statistično značilno (Levenov test: p>0,05), zato je analiza variance primerna.

Tabela 75 prikazuje, da je p-vrednost pri spremenljivkah »*Za preverjanje identitete pri plačilu s kreditno kartico*« in »*Pri dvigovanju denarja na bankomatu*«, manjša od 0,05 (p=0,009 in p=0,034) kar pomeni, da so razlike med skupinami anketirancev glede na izobrazbo statistično značilne pri 5% tveganju.

Tabela 75: ANOVA za starost

		Vsota kvadr.	df	Povpr. kvadr	F	Stat. znač.
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	Med skupinami	3,149	4	,787	,583	,675
	Znotraj skupin	668,323	495	1,350		
	Skupaj	671,472	499			
Za preverjanje identitete pri plačilu s kreditno kartico.	**Med skupinami**	**18,349**	**4**	**4,587**	**3,421**	**,009**
	Znotraj skupin	**663,769**	**495**	**1,341**		
	Skupaj	**682,118**	**499**			
Pri dvigovanju denarja na bankomatu.	**Med skupinami**	**15,660**	**4**	**3,915**	**2,670**	**,032**
	Znotraj skupin	**725,812**	**495**	**1,466**		

	Skupaj	**741,472**	**499**			
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	Med skupinami	4,134	4	1,034	,733	,570
	Znotraj skupin	697,968	495	1,410		
	Skupaj	702,102	499			
Pri preverjanju preteklosti posameznika.	Med skupinami	8,520	4	2,130	1,349	,251
	Znotraj skupin	781,838	495	1,579		
	Skupaj	790,358	499			
Pri vpisu v šolo.	Med skupinami	1,687	4	,422	,274	,895
	Znotraj skupin	762,831	495	1,541		
	Skupaj	764,518	499			
Pri kontroli potnih listov.	Med skupinami	,822	4	,206	,230	,922
	Znotraj skupin	442,496	495	,894		
	Skupaj	443,318	499			
V potnih listih.	Med skupinami	2,225	4	,556	,723	,577
	Znotraj skupin	380,933	495	,770		
	Skupaj	383,158	499			
Ob vstopu v državne stavbe.	Med skupinami	8,119	4	2,030	2,032	,089
	Znotraj skupin	494,353	495	,999		
	Skupaj	502,472	499			
Na letališčih pri prijavi na let.	Med skupinami	7,876	4	1,969	2,268	,061
	Znotraj skupin	429,756	495	,868		
	Skupaj	437,632	499			
Na vozniškem dovoljenju.	Med skupinami	2,047	4	,512	,399	,810
	Znotraj skupin	635,425	495	1,284		
	Skupaj	637,472	499			
Pri izposoji avtomobila (rent a car).	Med skupinami	5,253	4	1,313	,918	,453
	Znotraj skupin	708,465	495	1,431		
	Skupaj	713,718	499			

V našem primeru nastanejo značilne razlike (izračunane vrednosti pod 0,05), zaradi dejavnika »starost« pri dveh spremenljivkah in sicer: »*Za preverjanje*

identitete pri plačilu s kreditno kartico« in »*Pri dvigovanju denarja na bankomatu*«, pri ostalih desetih spremenljivkah ni statistično značilne razlike.

Ker nas zanima, katere skupine anketirancev glede na starost se med seboj bistveno razlikujejo, smo opravili še dodatno analizo, ki se imenuje post-hoc analiza. V njej primerjamo povprečje vsake skupine s povprečjema preostalih skupin. Da bi lahko za ti dve spremenljivki nadalje ugotovili, za katere starostne skupine je značilno, da se sprejemljivost dviga z dviganjem starostne stopnje, opravimo še Bonferroni post-hoc test (tabela 76).

Tabela 76: Bonferroni post-hoc test starostne stopnje

						95% interval zaupanja	
Odvisna spremenljivka	(I) Star	(J) Star	Razlike v povpr. (I-J)	Stand. napaka	Stat. znač.	Spod. meja	Zgor. meja
Za preverjanje identitete pri plačilu s kreditno kartico.	14-19	20-29	-,212	,289	1,000	-1,03	,60
		30-39	-,617	,287	,318	-1,43	,19
		40-49	-,644	,284	,239	-1,45	,16
		50-59	-,392	,284	1,000	-1,19	,41
	20-29	14-19	,212	,289	1,000	-,60	1,03
		30-39	-,406	,157	,099	-,85	,04
		40-49	**-,432***	**,152**	**,046**	**-,86**	**,00**
		50-59	-,181	,152	1,000	-,61	,25
	30-39	14-19	,617	,287	,318	-,19	1,43
		20-29	,406	,157	,099	-,04	,85
		40-49	-,027	,148	1,000	-,44	,39
		50-59	,225	,148	1,000	-,19	,64
	40-49	14-19	,644	,284	,239	-,16	1,45
		20-29	**,432***	**,152**	**,046**	**,00**	**,86**
		30-39	,027	,148	1,000	-,39	,44
		50-59	,252	,143	,793	-,15	,66
	50-59	14-19	,392	,284	1,000	-,41	1,19
		20-29	,181	,152	1,000	-,25	,61
		30-39	-,225	,148	1,000	-,64	,19
		40-49	-,252	,143	,793	-,66	,15

Pri dvigovanju denarja na bankomatu.	14-19	20-29	,335	,302	1,000	-,52	1,19
		30-39	-,101	,300	1,000	-,95	,74
		40-49	-,147	,297	1,000	-,98	,69
		50-59	-,010	,297	1,000	-,85	,83
	20-29	14-19	-,335	,302	1,000	-1,19	,52
		30-39	-,435	,164	,082	-,90	,03
		40-49	**-,482***	**,159**	**,025**	**-,93**	**-,03**
		50-59	-,344	,159	,312	-,79	,10
	30-39	14-19	,101	,300	1,000	-,74	,95
		20-29	,435	,164	,082	-,03	,90
		40-49	-,046	,154	1,000	-,48	,39
		50-59	,091	,155	1,000	-,35	,53
	40-49	14-19	,147	,297	1,000	-,69	,98
		20-29	**,482***	**,159**	**,025**	**,03**	**,93**
		30-39	,046	,154	1,000	-,39	,48
		50-59	,137	,150	1,000	-,28	,56
	50-59	14-19	,010	,297	1,000	-,83	,85
		20-29	,344	,159	,312	-,10	,79
		30-39	-,091	,155	1,000	-,53	,35
		40-49	-,137	,150	1,000	-,56	,28

* Razlike povprečij so statistično značilne pri stopnji značilnosti 0,05.

Iz izpisa rezultatov te analize, ki smo jo naredili s Bonferroni metodo, je razvidno, da značilne razlike pri obeh spremenljivkah Sprejemljivosti biometrične tehnologije (*Za preverjanje identitete pri plačilu s kreditno kartico*« in »*Pri dvigovanju denarja na bankomatu*«) obstajajo samo med starostno skupino 20-29 let in starostno skupino 40-49, pri primerjavah ostalih starostnih skupin, pa statistično pomembnih razlik ne najdemo.

Tabela 77 prikazuje opisne statistike za spremenljivko »*izobrazba*«, ki jo bomo uporabili v analizi variance.

Tabela 77: Opisne statistike za spremenljivko »izobrazba«

						95% interval zaupanja za povpr.			
		N	Povpr.	Stand. odklon	Stand. napaka	Spod. meja	Zgor. meja	Min.	Maks.
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	Nedokončana ali dokončana osnovna šola.	44	3,48	1,131	,170	3,13	3,82	1	5
	Dveletna ali triletna poklicna srednja šola.	102	3,65	1,105	,109	3,43	3,86	1	5
	Štiriletna ali petletna srednja šola.	211	3,33	1,147	,079	3,17	3,48	1	5
	Visokošolski ali univerzitetni študij.	131	3,33	1,212	,106	3,12	3,54	1	5
	Specializacija, magisterij, doktorat.	12	3,75	1,215	,351	2,98	4,52	1	5
	Skupaj	500	3,42	1,160	,052	3,31	3,52	1	5
Za preverjanje identitete pri plačilu s kreditno kartico.	Nedokončana ali dokončana osnovna šola.	44	3,45	1,190	,179	3,09	3,82	1	5
	Dveletna ali triletna poklicna srednja šola.	102	3,64	1,201	,119	3,40	3,87	1	5
	Štiriletna ali petletna srednja šola.	211	3,37	1,161	,080	3,21	3,53	1	5
	Visokošolski ali univerzitetni študij.	131	3,42	1,170	,102	3,22	3,62	1	5

	Specializacija, magisterij, doktorat.	12	3,92	,793	,229	3,41	4,42	2	5
	Skupaj	500	3,46	1,169	,052	3,36	3,56	1	5
Pri dvigovanju denarja na bankomatu.	Nedokončana ali dokončana osnovna šola.	44	3,52	1,191	,180	3,16	3,88	1	5
	Dveletna ali triletna poklicna srednja šola.	102	3,53	1,272	,126	3,28	3,78	1	5
	Štiriletna ali petletna srednja šola.	211	3,32	1,219	,084	3,16	3,49	1	5
	Visokošolski ali univerzitetni študij.	131	3,41	1,214	,106	3,20	3,62	1	5
	Specializacija, magisterij, doktorat.	12	3,75	,866	,250	3,20	4,30	2	5
	Skupaj	500	3,42	1,219	,055	3,31	3,52	1	5
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	Nedokončana ali dokončana osnovna šola.	44	3,82	1,105	,167	3,48	4,15	1	5
	Dveletna ali triletna poklicna srednja šola.	102	3,80	1,144	,113	3,58	4,03	1	5
	Štiriletna ali petletna srednja šola.	211	3,69	1,237	,085	3,52	3,86	1	5
	Visokošolski ali univerzitetni študij.	131	3,61	1,180	,103	3,41	3,81	1	5
	Specializacija, magisterij, doktorat.	12	4,17	,937	,271	3,57	4,76	2	5

	Skupaj	500	3,71	1,186	,053	3,61	3,82	1	5
Pri preverjanju preteklosti posameznika.	Nedokončana ali dokončana osnovna šola.	44	3,07	1,336	,201	2,66	3,47	1	5
	Dveletna ali triletna poklicna srednja šola.	102	3,34	1,286	,127	3,09	3,60	1	5
	Štiriletna ali petletna srednja šola.	211	3,21	1,252	,086	3,04	3,38	1	5
	Visokošolski ali univerzitetni študij.	131	3,17	1,229	,107	2,96	3,38	1	5
	Specializacija, magisterij, doktorat.	12	3,50	1,243	,359	2,71	4,29	1	5
	Skupaj	500	3,22	1,259	,056	3,11	3,33	1	5
Pri kontroli potnih listov.	Nedokončana ali dokončana osnovna šola.	44	3,75	,991	,149	3,45	4,05	1	5
	Dveletna ali triletna poklicna srednja šola.	102	4,06	,910	,090	3,88	4,24	1	5
	Štiriletna ali petletna srednja šola.	211	3,97	,997	,069	3,83	4,10	1	5
	Visokošolski ali univerzitetni študij.	131	3,85	,869	,076	3,70	4,01	1	5
	Specializacija, magisterij, doktorat.	12	4,17	,718	,207	3,71	4,62	3	5
	Skupaj	500	3,94	,943	,042	3,86	4,02	1	5

V potnih listih.	Nedokončana ali dokončana osnovna šola.	44	4,07	,900	,136	3,79	4,34	1	5
	Dveletna ali triletna poklicna srednja šola.	102	4,27	,858	,085	4,11	4,44	1	5
	Štiriletna ali petletna srednja šola.	211	4,25	,860	,059	4,13	4,36	1	5
	Visokošolski ali univerzitetni študij.	131	4,05	,871	,076	3,90	4,20	1	5
	Specializacija, magisterij, doktorat.	12	3,92	1,165	,336	3,18	4,66	1	5
	Skupaj	500	4,18	,876	,039	4,10	4,25	1	5
Na letališčih pri prijavi na let.	Nedokončana ali dokončana osnovna šola.	44	4,09	1,053	,159	3,77	4,41	1	5
	Dveletna ali triletna poklicna srednja šola.	102	4,34	,862	,085	4,17	4,51	1	5
	Štiriletna ali petletna srednja šola.	211	4,18	,912	,063	4,05	4,30	1	5
	Visokošolski ali univerzitetni študij.	131	3,95	,935	,082	3,79	4,12	1	5
	Specializacija, magisterij, doktorat.	12	4,17	1,267	,366	3,36	4,97	1	5
	Skupaj	500	4,14	,936	,042	4,06	4,23	1	5
Ob vstopu v državne stavbe.	Nedokončana ali dokončana osnovna šola.	44	3,84	1,098	,166	3,51	4,17	1	5

	Dveletna ali triletna poklicna srednja šola.	102	4,14	,912	,090	3,96	4,32	1	5
	Štiriletna ali petletna srednja šola.	211	3,90	,973	,067	3,77	4,03	1	5
	Visokošolski ali univerzitetni študij.	131	3,80	1,041	,091	3,62	3,98	1	5
	Specializacija, magisterij, doktorat.	12	3,83	1,337	,386	2,98	4,68	1	5
	Skupaj	500	3,92	1,003	,045	3,83	4,00	1	5
Na vozniškem dovoljenju.	Nedokončana ali dokončana osnovna šola.	44	3,34	,987	,149	3,04	3,64	1	5
	Dveletna ali triletna poklicna srednja šola.	102	3,65	1,059	,105	3,44	3,86	1	5
	Štiriletna ali petletna srednja šola.	211	3,42	1,120	,077	3,27	3,57	1	5
	Visokošolski ali univerzitetni študij.	131	3,24	1,216	,106	3,03	3,45	1	5
	Specializacija, magisterij, doktorat.	12	3,50	1,243	,359	2,71	4,29	1	5
	Skupaj	500	3,42	1,130	,051	3,32	3,52	1	5
Pri izposoji avtomobila (rent a car).	Nedokončana ali dokončana osnovna šola.	44	3,50	1,151	,174	3,15	3,85	1	5

	Dveletna ali triletna poklicna srednja šola.	102	3,44	1,122	,111	3,22	3,66	1	5
	Štiriletna ali petletna srednja šola.	211	3,26	1,232	,085	3,09	3,43	1	5
	Visokošolski ali univerzitetni študij.	131	3,03	1,183	,103	2,83	3,23	1	5
	Specializacija, magisterij, doktorat.	12	3,25	1,215	,351	2,48	4,02	1	5
	Skupaj	500	3,26	1,196	,053	3,15	3,36	1	5
Pri vpisu v šolo.	Nedokončana ali dokončana osnovna šola.	44	2,48	1,191	,180	2,12	2,84	1	5
	Dveletna ali triletna poklicna srednja šola.	102	2,81	1,295	,128	2,56	3,07	1	5
	Štiriletna ali petletna srednja šola.	211	2,66	1,241	,085	2,49	2,83	1	5
	Visokošolski ali univerzitetni študij.	131	2,58	1,209	,106	2,37	2,79	1	5
	Specializacija, magisterij, doktorat.	12	2,83	1,193	,345	2,08	3,59	1	5
	Skupaj	500	2,66	1,238	,055	2,55	2,77	1	5

Tabela 78 prikazuje rezultate Levenovega testa, za sprejem ali zavrnitev ničelne hipoteze H_0 in je predpogoj, da lahko analizo variance izvedemo. Določimo ničelno hipotezo:

H_0: Skupine se po izobrazbi med seboj ne razlikujejo statistično značilno.

Tabela 78: Test homogenosti varianc za spremenljivko izobrazba

	Levenova statistika	df1	df2	Stat. znač.
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	,809	4	495	,519
Za preverjanje identitete pri plačilu s kreditno kartico.	1,980	4	495	,096
Pri dvigovanju denarja na bankomatu.	1,141	4	495	,336
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	1,208	4	495	,306
Pri preverjanju preteklosti posameznika.	,282	4	495	,890
Pri kontroli potnih listov.	,413	4	495	,799
V potnih listih.	,692	4	495	,598
Na letališčih pri prijavi na let.	1,452	4	495	,216
Ob vstopu v državne stavbe.	1,548	4	495	,187
Na vozniškem dovoljenju.	1,509	4	495	,198
Pri izposoji avtomobila (rent a car).	,822	4	495	,512
Pri vpisu v šolo.	,353	4	495	,842

Ugotavljamo, da se variance med skupinami ne razlikujejo statistično značilno (Levenov test: p>0,05), zato je analiza variance primerna.

V naslednji tabeli 79 ugotovimo, da je p-vrednost pri spremenljivki »*Na letališčih pri prijavi na let*«, manjša od 0,05 (p=0,034), torej so razlike med skupinami anketirancev glede na izobrazbo statistično značilne pri 5% tveganju.

Tabela 79: ANOVA za izobrazbo

		Vsota kvadr.	df	Povpr. kvadr.	F	Stat. znač.
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj.	Med skupinami	9,629	4	2,407	1,800	,127
	Znotraj skupin	661,843	495	1,337		
	Skupaj	671,472	499			
Za preverjanje identitete pri plačilu s kreditno kartico.	Med skupinami	7,640	4	1,910	1,402	,232
	Znotraj skupin	674,478	495	1,363		
	Skupaj	682,118	499			
Pri dvigovanju denarja na bankomatu.	Med skupinami	5,007	4	1,252	,841	,499
	Znotraj skupin	736,465	495	1,488		
	Skupaj	741,472	499			
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	Med skupinami	5,311	4	1,328	,943	,439
	Znotraj skupin	696,791	495	1,408		
	Skupaj	702,102	499			
Pri preverjanju preteklosti posameznika.	Med skupinami	3,864	4	,966	,608	,657
	Znotraj skupin	786,494	495	1,589		
	Skupaj	790,358	499			
Pri vpisu v šolo.	Med skupinami	5,074	4	1,268	,827	,509
	Znotraj skupin	759,444	495	1,534		
	Skupaj	764,518	499			
Pri kontroli potnih listov.	Med skupinami	4,742	4	1,186	1,338	,255
	Znotraj skupin	438,576	495	,886		
	Skupaj	443,318	499			
V potnih listih.	Med skupinami	5,321	4	1,330	1,743	,139
	Znotraj skupin	377,837	495	,763		
	Skupaj	383,158	499			
Ob vstopu v državne stavbe.	Med skupinami	7,091	4	1,773	1,771	,133
	Znotraj skupin	495,381	495	1,001		
	Skupaj	502,472	499			
Na letališčih pri	**Med skupinami**	**9,102**	**4**	**2,275**	**2,628**	**,034**

prijavi na let.	**Znotraj skupin**	**428,530**	**495**	**,866**		
	Skupaj	**437,632**	**499**			
Na vozniškem dovoljenju.	Med skupinami	9,649	4	2,412	1,902	,109
	Znotraj skupin	627,823	495	1,268		
	Skupaj	637,472	499			
Pri izposoji avtomobila (rent a car).	Med skupinami	12,780	4	3,195	2,256	,062
	Znotraj skupin	700,938	495	1,416		
	Skupaj	713,718	499			

Da bi lahko za to značilno spremenljivko nadalje ugotovili, za katere stopnje izobrazbe je značilno, da se sprejemljivost niža z višanjem stopnje izobrazbe, opravimo še Bonferroni post-hoc test (tabela 80).

Tabela 80: Bonferroni post-hoc test za izobrazbo

Odvisna spremenljivka	(I) [šola]	(J) [šola]	Razlike povpr. (I-J)	Stand. napaka	Stat. znač.	95% interval zaupanja Spod. meja	Zgor. meja
Na letališčih pri prijavi na let.	Nedokončana ali dokončana osnovna šola.	Dveletna ali triletna poklicna srednja šola.	-,252	,168	1,000	-,73	,22
		Štiriletna ali petletna srednja šola.	-,084	,154	1,000	-,52	,35
		Visokošolski ali univerzitetni študij.	,137	,162	1,000	-,32	,59
		Specializacija, magisterij, doktorat.	-,076	,303	1,000	-,93	,78
	Dveletna ali triletna poklicna srednja šola.	Nedokončana ali dokončana osnovna šola.	,252	,168	1,000	-,22	,73
		Štiriletna ali petletna srednja šola.	,168	,112	1,000	-,15	,48

	Visokošolski ali univerzitetni študij.	**,389***	**,123**	**,016**	**,04**	**,74**
	Specializacija, magisterij, doktorat.	,176	,284	1,000	-,62	,98
Štiriletna ali petletna srednja šola.	Nedokončana ali dokončana osnovna šola.	,084	,154	1,000	-,35	,52
	Dveletna ali triletna poklicna srednja šola.	-,168	,112	1,000	-,48	,15
	Visokošolski ali univerzitetni študij.	,221	,103	,331	-,07	,51
	Specializacija, magisterij, doktorat.	,009	,276	1,000	-,77	,79
Visokošolski ali univerzitetni študij.	Nedokončana ali dokončana osnovna šola.	-,137	,162	1,000	-,59	,32
	Dveletna ali triletna poklicna srednja šola.	**-,389***	**,123**	**,016**	**-,74**	**-,04**
	Štiriletna ali petletna srednja šola.	-,221	,103	,331	-,51	,07
	Specializacija, magisterij, doktorat.	-,212	,281	1,000	-1,00	,58
Specializacija, magisterij, doktorat.	Nedokončana ali dokončana osnovna šola.	,076	,303	1,000	-,78	,93
	Dveletna ali triletna poklicna srednja šola.	-,176	,284	1,000	-,98	,62

	Štiriletna ali petletna srednja šola.	-,009	,276	1,000	-,79	,77
	Visokošolski ali univerzitetni študij.	,212	,281	1,000	-,58	1,00

* Razlike povprečij so statistično značilne pri stopnji značilnosti 0,05.

S testom ugotavljamo, da za drugi del druge hipoteze nastajajo značilne razlike v oceni sprejemljivosti uporabe biometričnih metod le pri enem podvprašanju, pa še to se povprečni oceni statistično značilno razlikujejo le med dvema izobrazbenima skupinama. Razlika (-0,389*) je v v oceni sprejemljivosti med visokošolsko (univerzitetno izobrazbo) in dveletno (triletno poklicno izobrazbo (p=0,016). Torej je ocena sprejemljivosti biometričnih metod statistično značilno nižja pri anketirancih z visokošolsko izobrazbo (univerzitetno izobrazbo) kot pri anketirancih z dvoletno ali (triletno poklicno srednjo šolo) samo »*Na letališčih pri prijavi na let*«.

9.5 *Preveritev hipotez*

H1: Varnost osebnih podatkov ne vpliva znatno na oceno sprejemljivosti uporabe sistemov množičnega nadzora (identifikacije) v varnostnih sistemih.

Za ugotavljanje statistične pomembnosti smo opravili regresijo in sicer med spremenljivko »*Varnost osebnih podatkov*« in med spremenljivkami »*Sprejemljivost nadzornih tehnologij*«. V delu kjer raziskujemo uporabo biometrične tehnologije, za primere vsakdanjih opravil ima dejavnik »*Varnost osebnih podatkov*« statistično pomemben vpliva na »*Sprejemljivost nadzornih tehnologij*«. Anketiranci v Sloveniji so se s tem opredelili tudi do vprašanja: »*Koliko svobode za koliko varnosti?*«, ki je predmet mnogih znanstvenih raziskav. Terorizem je, kot lahko sklepamo iz raziskave, vendarle pojav pri katerem je za vzdrževanje in povečevanje varnosti, dovoljen povečan poseg v temeljne človekove svoboščine v smislu osebnih podatkov.

Hipotezo 1 bi lahko potrdili samo v primeru, ko gre za vpliv varnosti osebnih podatkov na sprejemljivost biometrije, v namene

protiterorističnega delovanja. Zaradi kriterija raziskave, ki preučuje vpliv varnosti osebnih podatkov na sprejemljivost biometrije v vsakdanjem življenju pa hipotezo 1 ZAVRNEMO.

H2: Sprejemljivost nadzornih tehnologij se viša z višanjem starostne stopnje in niža z višanjem izobrazbene stopnje anketirancev.

Bonferroni test, na podlagi ANOVA statistike nam pokaže, da je statistično značilna razlika prvega dela hipoteze »*Sprejemljivost nadzornih tehnologij se viša z višanjem starostne stopnje*« nastala pri dveh spremenljivkah »*Za preverjanje identitete pri plačilu s kreditno kartico*« (sig. ali p:0,009) in »*Pri dvigovanju denarja na bankomatu*« (sig. ali p:0,032), *v* obeh primerih med starostno stopnjo 20-29 let in starostno stopnjo 40-49 (sig. ali p:0,046) in (sig. ali p:0,025). Pri primerjavah ostalih desetih spremenljivk in starostnih intervalov, pa statistično pomembnih razlik ne najdemo.

Za drugi del hipoteze nam Bonferroni test, po predhodno opravljeni ANOVA statistiki pokaže, da je statistično značilna razlika drugega dela hipoteze »*Sprejemljivost nadzornih tehnologij se niža z višanjem izobrazbene stopnje anketirancev*« nastala pri spremenljivki »*Na letališčih pri prijavi na let*« (sig. ali p:0,034) med stopnjami izobrazb: dveletna ali triletna poklicna srednja šola ter visokošolski ali univerzitetni študij (sig. ali p:0,016).

Na podlagi navedenih ugotovitev, hipotezo 2 ZAVRNEMO saj se značilne razlike pojavijo samo pri dveh spremenljivkah (podvprašanjih) za starostno stopnjo in pri eni spremenljivki za stopnjo izobrazbe.

H3: Biometrični sistemi za množični nadzor v procesih identifikacije so učinkovitejši kot sedaj poznani alternativni (kartični) sistemi.

Tretjo hipotezo potrjujemo glede na interpretacijo učinkovitosti po HBSI modelu, kar predpostavlja parametre uporabnosti, ergonomske parametre ter parametre učljivosti identifikacijskega sistema. Glede na statistične ugotovitve, lahko hipotezo 3 v celoti potrdimo, saj smo na osnovi parnega t-testa zavrnili ničelno hipotezo.

Na podlagi navedenih ugotovitev, hipotezo 3 SPREJMEMO.

Na osnovi korelacijske analize pa smo pojasnili večji vpliv biometrije na učinkovitost identifikacijskih sistemov:

1. *kartični sistemi*/biometrični sistemi (35,9 %/64,1 %) in
2. kartični sistemi/*biometrični sistemi* (32,2 %/67,7 %).

10 RAZVOJ ODLOČITVENEGA MODELA SPREJEMLJIVOSTI BIOMETRIJE

V izvedeni raziskavi smo s statističnim preskušanjem treh neodvisnih hipotez poskušali ugotoviti kakšna je sprejemljivost in učinkovitost uporabe identifikacijskih postopkov (biometričnih identifikacijskih metod) s stališča uporabnika. Posebej smo ugotavljali ali se v primerih protiterorističnega delovanja sprejemljivost nadzornih (biometričnih) tehnologij poveča. S tem namenom, smo preverjali kako ljudje sprejemajo biometrične tehnologije v vsakdanjem življenju in kako v primerih, ko je percepcija terorizma izrazitejša.

Z namenom umestitve raziskave v svetovni raziskovalni okvir, poglejmo primerljive raziskave in raziskovalne modele, ki obravnavajo dejavnike sprejemljivosti identifikacijskih tehnologij in varnosti osebnih podatkov. Še posebej bomo izpostavili terorizem kot pomemben dejavnik sprejemljivosti identifikacijskih tehnologij.

Sprejemljivost biometričnih sistemov, je bil kot dejavnik v preteklosti manj obravnavan, ampak postaja vedno bolj pomemben dejavnik za ljudi, ki uporabljajo te sisteme, pri postopkih biometrične identifikacije (Richards, 1997). Sprva, je bilo teh sistemov manj in na razpolago le za namene najvišje varnostne zahteve, kar je v preteklosti posledično doprineslo k manjšemu zanimanju za obravnavo dejavnika sprejemljivosti.

Za sprejemljivost biometrije s stališča uporabnika, je raziskovalna skupina (Community Research and Development Information Service [CORDIS], 2003) v projektu Biovizija, opredelil pomembne dejavnike, ki privedejo do odločitve o sprejetju biometrične tehnologije:

1. *Potreba po večji varnosti*. Uporabniki imajo dejansko potrebo po večji varnosti in verjamejo, da je s pomočjo biometričnih podatkov možno povečati varnost.

2. *Primernost za uporabo*. Biometrični sistem je bolj primeren za uporabo kot prejšnji / alternativni sistemi.
3. *Zaupanje do izvajalca biometričnih ukrepov-operaterja*. Zaupanje do tistih, ki obdelujejo biometrične podatke, da jih varno hranijo in jih ne uporabljajo za noben nepooblaščen namen.

Tradicionalno se za odločitev glede sprejemljivosti informacijskih sistemov uporabljajo instrumenti, kot so: model sprejemljivosti tehnologije (Technology Acceptance Model - TAM) in univerzalna teorija za sprejemljivost in uporabnost tehnologije (Unified Theory of Acceptance and Use of Technology - UTAUT) v kontekstih, ki lahko uporabniku koristijo za določitev in preverbo dejavnikov glede sprejemljivosti. Odločitev o sprejemu je med drugimi odvisna tudi od dejavnikov, ki vplivajo na lažjo uporabo in uporabnost (Schmidt, Das, Kumar in Bekkering, 2008). Biometrične naprave ne ponujajo dosti koristi za uporabnika, v smislu dostopa do drugih biometričnih podatkov v nekem drugem sistemu, so bolj primerne za uporabo tradicionalnih gesel kot takih.

Hovsto (2008) je v vezi s problematiko sprejemljivosti biometrije, v svoji raziskavi izpostavil dejavnike, ki so vezani predvsem na takšno ali drugačno hendikepiranost uporabnika. Izhajal je predvsem iz nalog razvijalca ob snovanju in razvoju sistema ter nalog upravljavca biometričnega sistema, ki morata za sprejemljivost in nemoteno uporabo, med drugimi upoštevati tudi naslednje izredne primere:

- možnost merilne odsotnosti fizičnih delov telesa, ki so potrebni za delovanje biometričnih sistemov (npr. manjka kazalec v primeru sistema za nadzor dostopa kjer so predpisanih prsti),
- odsotnost vedenjske značilnosti, potrebne za pravilno delovanje biometričnega sistema (npr. človek z motnjami v govoru v primeru identifikacije na osnovi glasa),

- fizična nezmožnost dela telesa, potrebnega za pravilno delovanje biometričnega sistema (npr. oseba z artritisom v primeru, da je zahtevana uporaba geometrije roke pri identifikaciji ob vstopu na letalo),
- nezmožnost dosledne predstavitve zahtevanih biometričnih značilnosti na dovolj predvidljiv način v posebnih pogojih identifikacije (npr. težave zaradi nenadzorovanega gibanja zrkla povzročajo nezmožnost primerjave z vzorcem iz baze vzorcev),
- nezmožnost dostopa ali težave s fizičnim dostopom do terminala z biometričnim senzorjem (npr. oseba na invalidskem vozičku ni dovolj visoka za dostop do senzorja ali uporabo terminala na določeni višini),
- nezmožnost identifikacije bodisi, zaradi nepismenosti, nerazumevanja navodil, ali nezmožnost pomnenja pravilnih postopkov, da bi lahko biometrični sistem uspešno deloval.
- psihološke sposobnosti posameznika lahko preprečujejo, da bi biometrični sistem deloval pravilno (npr. osebe z izjemno kompulzivno-obsesivno motnjo ne želijo uporabljati senzorja ali tipkovnice na osnovi fizičnega kontakta) in še mnoge druge.

Na osnovi teh izrednih primerov za katere je možno, da nastanejo v procesu identifikacije, je Hovsto izpostavil dejavnike, ki vplivajo na sprejemljivost biometričnih sistemov in omogočajo registracijo ljudi na osnovi podatkov, ki imajo takšne in drugačne fizične ali psihološke nezmožnosti. Dejavniki sprejemljivosti glede na zmožnost in sposobnost uporabe biometričnih sistemov so tako:

- prilagodljivost v uporabi,
- enostavnost in intuitivnost za uporabo,
- preprostost razumevanja z ustreznimi pozivnimi dodatki,
- ustrezno podpisana,
- strpnost do napak,
- uporabnost ob nizkem fizičnem naporu in

- velikost in enostavnost prostora za pristop in uporabo.

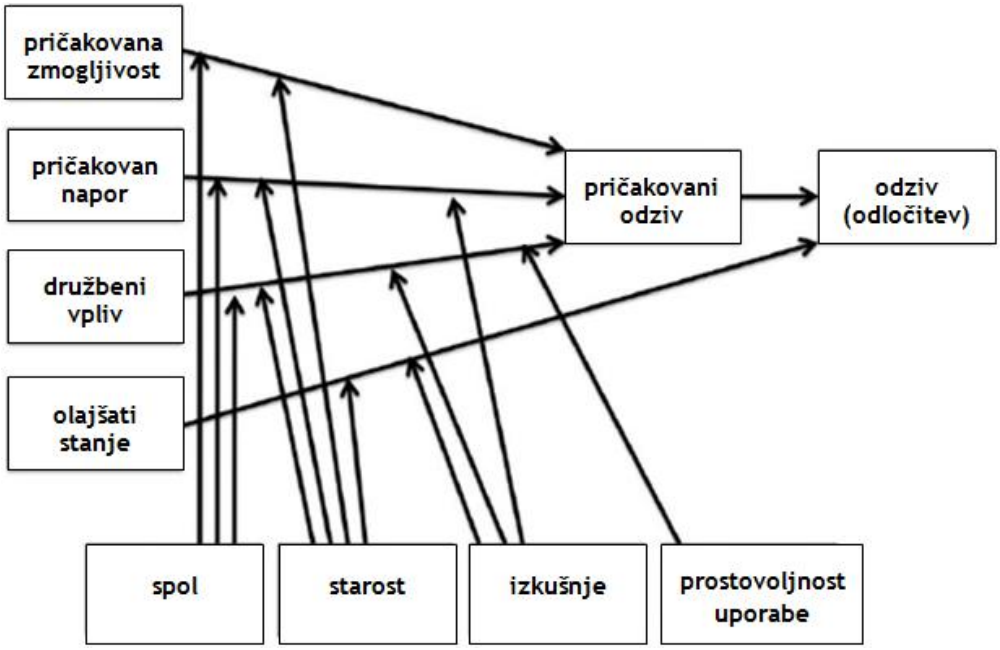
Sprejemljivost biometrije obravnava tudi prilagojen UTAUT model (AL-Harby, Qahwaji in Kamala, 2009) za raziskavo dejavnikov, ki določajo sprejetje sistema z aspekta učinkovitosti biometrije v e-poslovanju in je v pomoč odločevalcem, za boljše razumevanje dejavnikov, ki vplivajo na sprejemljivost uporabnika. Avtorji obravnavajo tudi modificiran UTAUT model sprejemljivosti biometrije s stališča zanesljivosti (AL-Harby, Qahwaji in Kamala, 2010).

Model UTAUT predlaga štiri direktno determinirane konstrukte, ki delujejo kot glavni dejavniki sprejetja biometrične tehnologije do stopnje, ko posameznik verjame, da z uporabo sistema (Venkatesh, Morris, Davis in Davis, 2003):

1. doseže pričakovano uspešnost, ali mu pomaga doseči povečanje delovne uspešnosti,
2. doseže želeni učinek (stopnjo spretnosti) povezan z uporabo sistema z določenim naporom v določenem času,
3. doseže pričakovani socialni (družbeni) vpliv v smislu stopnje, do katere posameznik zaznava, da je pomembno, da se identificira z uporabo tega sistema v družbi. Socialni vpliv je subjektivna (družbena) norma in se nanaša na določeno ne-sistemsko védenje o sistemu, ki je v uporabi za določen specifičen namen in povečamo učinek, saj so prisotni olajševalni pogoji v smislu že (do neke stopnje) predhodno obstoječe organizacijske in tehnične infrastrukture in
4. si s to novo tehnologijo olajša obstoječe delo na osnovi novih boljših in enostavnejših postopkov in tehnologije.

Spol, starost, izkušnje in prostovoljnosti uporabe so predstavljeni kot posredni dejavniki, ki vplivajo na štiri ključne konstrukte (Al-Gahtani, Hubona in Wang, 2007; Venkatesh et al., 2003). Teorija je bila razvita s pomočjo pregleda in konsolidacije osmih modelov, ki so jih avtorji raziskovali v preteklosti za obrazložitev odločitvenih modelov sprejemljivosti tehnologij in sicer, teorija utemeljenega ukrepanja (Fishbein in Ajzen, 1975), tehnologija sprejema

modela (Davis, 1986; Davis, 1989), motivacijski model, teorija načrtovanega vedenja (Ajzen,1985; Ajzen, 1991), kombinirana teorija načrtovanega vedenja/tehnologija sprejema modela, model uporabe računalnika ter teorija difuzije inovacije (Rogers, 1962) in socialne kognitivne teorije (Bandura, 2001). Slika 10 prikazuje UTAUT model.



Slika 10: UTAUT odločitveni model sprejemljivosti biometrije (Venkatesh et al., 2003)

Številne študije so bile opravljene z namenom preučiti odnos samo-učinkovitosti (motivacijo) v zvezi z uporabo informacijske tehnologije (Al-Gahtani et al., 2007; Al-Somalije in drugi, 2008; Bandura, 1977a; Hernández-Ortega, Jiménez-Martínez in De Hoyos, 2008; Wang, Lin in Tang, 2003). Na podlagi pregleda literature (teoretičnega in empiričnega dela), je mogoče sklepati, da ima »močnejša oseba« s prepričanjem glede višje samo-učinkovitosti, večjo verjetnost za dokončanje zahtevanih nalog.

Enoten pogled avtorjev na sprejemljivost informacijske tehnologije za uporabnika je izpostavil kot zelo pomemben dejavnik, samo-učinkovitost (tabela 81). Samo-učinkovitost je definirana kot samostojnost uporabnika in pomeni zaupanje v njegove lastne sposobnosti, za opravljanje nalog na

računalniških aplikacijah oziroma domenah (Monsuwe , Perea, Dellaert in Ruyter, 2004).

Model sprejemljivosti biometrije s tehničnega vidika na osnovi stohastičnega Markovskega modela, pa obravnava Brumnik (2011). V tem delu, model sprejemljivosti temelji na statističnih ocenah časov do odpovedi sistema (Mean Time To Failure - MTTF), časov do popravila (Mean Time To Repair - MTTR), časov med odpovedmi sistema (Mean Time Between Failure - MTBF) ter ocenah učinkovitosti in zanesljivosti (Brumnik in Balantič, 2008) na osnovi katerih, potem sprejmemo oceno glede (ne)ustreznosti biometričnega sistema.

Tabela 81: Pregled raziskav in modelov, ki obravnavajo različne dejavnike sprejemljivosti biometrije

raziskava	model	dejavniki	rezultati/inovativnost
CORDIS (2003)	model obravnave (BVN: BIOVIZION)	- potreba po večji varnosti - zaupanje do izvajalca biometričnih ukrepov-operaterja - primernost za uporabo	
Hovsto (2008)	model obravnave hendikepa	- prilagodljivost v uporabi - enostavnost in intuitivnost za uporabo - preprostost razumevanja z ustreznimi pozivnimi dodatki - ustrezno podpisana, - strpnost do napak - uporabnost ob nizkem fizičnem naporu - velikost in enostavnost prostora za pristop in uporabo	Študija obravnava dejavnike sprejemljivosti s tališča hendikepiranega uporabnika. Izpostavlja vrsto nepredvidenih momentov, s katerimi mora računati tako razvijalec biometrične opreme kot tudi operater, ki z njo izvaja identifikacijski postopek.
Venkatesh et al. (2003)	UTAUT	- pričakovana zmogljivost - pričakovan napor - družbeni vpliv - starost - izobrazba - spol - prostovoljnost uporabe - predhodne izkušnje	Model vsebuje osem konsolidiranih teorij, ki so se ukvarjale z psihološkimi, sociološkimi in družboslovnimi aspekti odločitve sprejemljivosti novih modelov sprejemljivosti biometrične tehnologije s stališča uporabnika.

Brumnik (2011)	Markovski (stohastični)	- MTTF - MTBB - MTTR - zanesljivost - učinkovitost	Stohastični model je razvit na osnovi aplikativne raziskave biometričnega sistema, omogoča napovedovanje zanesljivosti in učinkovitosti obravnavanega sistema. Na osnovi teh ocen se uporabnik lahko odloči o (ne)sprejemljivosti. Model je preverjen z Weibullovo statistično teorijo in aplikativnim testom.
naša raziskava	$UTAUT_{(TE)}$	- efekt grožnje, - učinkovitost (HBSI) - starost, - izobrazba, - predhodne izkušnje (poznavanje IT in varnostne tehnologije)	Novi modificirani $UTAUT_{(TE)}$ model je nadgradnja UTAUT modela (univerzalnega modela sprejemljivosti tehnologije), ki vključuje dejavnik »efekt grožnje«. Model omogoča natančnejši vpogled v kriterije in psihologijo odločevalca (uporabnika), ko se odloča o sprejemljivosti biometričnega sistema.

10.1 *Novi $UTAUT_{(TE)}$ model sprejemljivosti biometrije*

Iz primerjave modelov lahko ugotovimo, različne obravnave sprejemljivosti biometrije, glede na različne dejavnike. Poleg testiranja hipotez v naši raziskavi, je bilo pomembno tudi vprašanje: Ali »*efekt grožnje (ang. threat effect)*« vpliva na sprejemljivost biometričnega sistema? V skladu z UTAUT modelom nas je zanimalo tudi: »Ali ima ta dejavnik direktni vpliv (je glavna determinanta) na sprejemljivost ali pa je to samo odvisna spremenljivka?« torej, v kakšni meri vpliva na sprejemljivost. Efekt grožnje smo v raziskavi preverjali s teroristično nevarnostjo, preko katere smo želeli izvedeti, ali je le ta zadosten razlog, da se ljudje odpovedo delu osebnih svoboščin pri preverjanju osebnih podatkov v meri, ki ga zahteva biometrični postopek (odvzem osebnih lastnosti za preverbo identitete in njihova obdelava). Ugotovili smo, da ima »efekt grožnje« direkten vpliv na sprejemljivost sistema in v primeru ogroženosti (glede na percepcijo terorizma), pristanejo na biometrično tehnologijo, kljub njenemu slabšemu poznavanju in ne glede na njihove prejšnje izkušnje z njo. Lahko celo trdimo, da je »efekt grožnje«

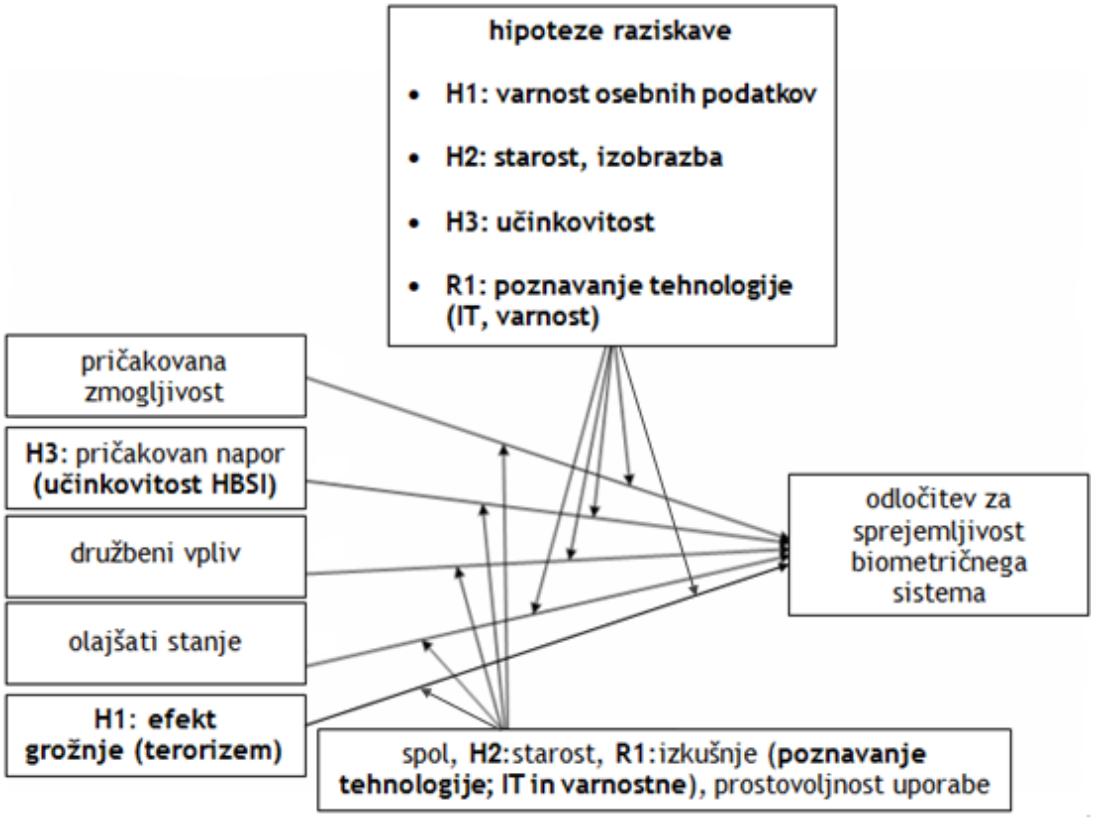
dejavnik zaradi katerega, dejavniki, ki so sicer po UTAUT modelu neodvisni (glavni), pod določenimi pogoji lahko postanejo odvisni.

Nadalje smo v naši raziskavi preverjali tudi pomembnost učinkovitosti identifikacijskega sistema, pri čemer smo ugotovili, da direktno vpliva na sprejemljivost biometrične tehnologije, s čimer potrjujemo UTAUT model avtorjev (Venkateshu et al., 2003).

Dejavnika starost in izobrazba imata sicer posreden vpliv na sprejemljivost biometrije, vendar nista glavna dejavnika. Tudi predhodne izkušnje z biometričnimi identifikacijskimi sistemi ne vplivajo znatno na njihovo sprejemljivost, kadar gre za primere protiterorističnega delovanja.

Glede na ugotovljena dejstva smo UTAUT model modificirali z dejavniki, pridobljenimi v raziskavi. Rezultat zgoraj naštetih ugotovitev je tako novi model $UTAUT_{(TE)}$ (Unified Theory of Acceptance and Use of Technology with Threat Effect), ki med drugim upošteva tudi zelo močan dejavnik »efekt grožnje«.

Rezultat je nov, za biometrijo prirejen model (slika 11), s petimi glavnimi determinantami dejavnikov sprejemljivosti. Odločitveni model je enostaven glede uporabe dejavnikov, mrežno strukturiran ter vsebuje bistvena pričakovanja in odzive, ki so pomembni za odločitve glede sprejemljivosti biometrije.



Slika 11: Odločitveni model sprejemljivosti za biometrijo - modificirani $UTAUT_{(TE)}$ model

V nalogi smo razvili modificiran model odločanja sprejemljivosti, ki poleg že znanih dejavnikov (iz raziskav drugih avtorjev) upošteva tudi dejavnik »efekt grožnje«. Ob pregledu relevantne literature, ki obravnava modele odločanja, menedžment sprejemljivosti, psihologijo odločanja ter dejavnike, ki vplivajo na odločanje za sprejemljivost biometričnih sistemov ugotavljamo, da je bil ta dejavnik v ta namen in v tej obliki, uporabljen prvič. Praktično uporabnost raziskave in razvitega modela lahko vidimo v primerih, ko mora odločevalec (uporabnik, operater, investitor, varnostni inženir idr.) določiti neko varnostno politiko. Ob tem mora odločevalec upoštevati informacije o varnostnih tveganjih v okviru nekega končnega časovnega intervala. Ta časovni načrt se imenuje varnostna ocena tveganja, katerega dolžina ima bistven vpliv na sprejemljivost biometrične tehnologije. Rezultate tega modela lahko uporabimo v potrditev metodološkega postopka za uspešno klasificiranje biometrije v procesu odločanja. »Efekt grožnje« je bil v disertaciji prikazan skozi prizmo terorizma, ki v veliki meri za ljudi pomeni že

skrajni strah, še posebej po terorističnih napadih v ZDA. Ta »efekt grožnje« bi bilo za natančnejšo interpretacijo modela sprejemljivosti biometrične tehnologije, smiselno razdelati na več »močnostnih-jakostnih« stopenj. Terorizem je prav tako mogoče definirati z mnogimi oblikami. Za natančnejši vpogled v sprejemljivost biometrije v momentu protiterorističnega delovanja, bi bilo potrebno podrobneje opredeliti terorizem z dejavniki.

Pomembno je spoznanje, da lahko boljšo uporabnost rezultatov sprejemljivosti biometrije, dosežemo s simulacijo identifikacijskih postopkov, ki pa so nadalje odvisni od trajanja simulacije. Za boljše rezultate modeliranja sprejemljivosti, bi morali izvesti vsaj še vključitev naslednjih dejavnikov:

1. Dejavnik, ki bi vključeval pravni aspekt sprejemljivosti v vezi z varstvom podatkov, preglednosti in zasebnosti.
2. Dejavnik, ki bi vključeval zdravstvene vidike uporabe biometrične tehnologije in njegove neposredne in posredne zdravstvene posledice (npr. IR skeniranje šarenice, termični vpliv biometrije na oči, bakteriološka tveganja itd.). Skrbi povezane s tveganjem za zdravje lahko predstavljajo močno oviro v postopku odločanja glede sprejemljivosti tehnologije.
3. Dejavnik, ki bi vključeval vidik gospodarnosti, v skladu s splošno obravnavanim vprašanjem »optimalne biometrije«. Najmočnejša identifikacijska tehnologija ni nujno vedno tudi najbolj optimalna.
4. Dejavnik, ki bi vključeval vidike religije.

Potrebno je storiti vse, da se z uporabo biometričnih metod izkoristi njene prednostne lastnosti in omeji ali odpravi slabosti oz. pomanjkljivosti tudi v zvezi z vprašanjem ogrožanja zasebnosti.

10.2 *Izvirni prispevek k znanosti*

Doktorska disertacija temelji na znanstvenoraziskovalnem delu na področju terorizma, IKT in zasebnosti v smislu sprejemljivosti biometrije. Raziskovalno delo dosega večplasten pozitivni učinek metodologije organiziranja varnostnih

procesov ob upoštevanju človekovih pravic, ki ga v osnovi lahko nakažemo v praktičnem in teoretičnem prispevku k znanosti.

1. Biometrični sistem za ugotavljanje in/ali potrjevanje identitete oseb bomo obravnavali v luči osnovne človekove pravice do zasebnosti in kot orodje za boj proti terorizmu oziroma eni izmed najsodobnejših pojavnih oblik terorizma, t.j. kibernetskemu terorizmu. Raziskava bo pripomogla k boljšemu razumevanju človekovega zavedanja, percepcije glede nevarnosti terorizma ter podala oceno stopnje pripravljenosti odrekanja zasebnosti, v korist varnosti.
2. Z raziskavo smo potrdili domneve o biometriji kot preprostem in učinkovitem (HBSI) načinu prepoznavanja identitete oseb v širši javni uporabi (Kukula in Proctor, 2009), kakor tudi orodju za boj proti terorizmu. Izvedli in predstavili smo raziskavo parametrov sprejemljivosti, učinkovitosti in zasebnosti ter v okviru tega pripravili kvantitativno statistično oceno. Opisana metodologija določanja parametrov za biometrično tehnologijo je v povezavi s terorizmom bila uporabljena prvič ter tako pomeni neposreden doprinos k znanosti.
3. V znanstveni literaturi lahko zasledimo množico raziskav, ki se ločeno ukvarjajo z učinkovitostjo najrazličnejših postopkov identifikacije, zasebnostjo in terorizmom. Pričakovani rezultat naše raziskave je optimirani empirični model raziskovanja zasebnosti, s stališča varovanja osebnih podatkov in z implikacijo sprejemljivosti biometrične tehnologije zaradi pojava terorizma, ki upošteva zgoraj navedene faktorje, dejavnike in njim pripadajoče spremenljivke. Na osnovi izsledkov raziskave smo konstruirali nov model sprejemljivosti biometrične tehnologije, ki vključuje dejavnike s statistično značilnim vplivom.

11 RAZPRAVA

Vedno večja uporaba biometričnih tehnologij in zastopanost te tehnologije na tržišču, je privedla tudi do številnih polemik glede zasebnosti. Ameriška raziskava (za področje Pittsburgh) obravnava družbeno sprejemljivost biometrije, glede na poznavanje in uporabo interneta. Podatki so bili zbrani na vzorcu 241 anketirancev in obdelani z regresijsko in korelacijsko analizo ter uporabo hi-kvadrat preizkusa. Ugotovljeno je bilo, da je razmerje med seznanjenostjo anketirancev (ki so imeli dostop do interneta) z novo identifikacijsko tehnologijo in njihovim znanjem glede biometričnih podatkov, statistično pomembno. Udeleženci, ki pogosto uporabljajo internet, so bolj zadovoljni z inovativno tehnologijo in jo tudi v večji meri sprejemajo (Smith, 2008).

Raziskava avtorjev Mordini in Petrini (2007) obravnava socialne in etične vidike in dejavnike biometričnih podatkov, predvsem pa osvetli zgodovinski model obravnave teh dejavnikov, ki zadeva nastanek in razvoj biometrične tehnologije. Avtorja se sklicujeta na različne dejavnike, katere je potrebno poznati, za razumevanje etičnih in družbenih posledic pri uporabi identifikacijske tehnologije. Raziskava vsebuje tudi kratek pregled vsebine glavnih institucionalnih dokumentov, tako na mednarodni kot domači ravni v različnih državah. Analize teh poročil, prinašajo v ospredje glavne izzive, ki bi jih morala družba obravnavati, v bližnji prihodnosti in na dolgi rok, kot posledico zelo hitrega širjenja uporabe biometrične tehnologije.

Pristop k modeliranju zaupanja (Blaze, Feigenbaum in Lacy, 1996) je opredeljen z upravljanjem zaupanja, kot zelo pomembnim elementom sprejemljivosti omrežnih storitev. Vidik problematike upravljanja zaupanja vključuje: oblikovanje politike varnosti, varnostne poverilnice, preverjanje, izpolnjevanje ustrezne politike in zaupanje tretjim osebam. Obstoječi tehnični sistemi, ki podpirajo varnost omrežnih aplikacij (npr. X.509, PGP, Kerberos itd.) rešujejo samo ozke segmente celotnega spektra problematike upravljanja zaupanja in to pogosto na način, ki je primeren le za nek posamičen primer. Predstavljen model je celovit pristop k upravljanju

zaupanja, ki temelji na preprostem jeziku določanja ukrepov zaupanja in odnosa do zaupanja. Opisuje tudi prototip izvajanja novega sistema upravljanja zaupanja, ki temelji na oblikovanju politike, ki bo olajšala razvoj varnostnih funkcij v različnih omrežnih storitvah.

Za zagotavljanje varnosti osebnih podatkov, kot osnovnega pogoja za sprejemljivost biometričnih podatkov se izvaja šifriranje (kriptiranje) podatkov. Te metode se nanašajo na pripravo in transformacijo podatkov v takšno obliko, da podatka ni mogoče razumeti brez neke dodatne informacije. Vladne agencije, zasebniki, civilne iniciative v računalniški industriji delajo na razvoju metod šifriranja podatkov, da bi zagotovili pravice do varnosti osebnih podatkov posameznika v družbi (Freeman, 1997).

Biometrija pridobiva veliko na uporabnosti zaradi možnosti natančne in zanesljive identifikacije ter avtentikacije. Veliko tehničnih raziskav je bilo opravljenih, z namenom ocene uspešnosti biometričnih sistemov, s poudarkom na napačnih sprejemih (FAR) in napačnih zavrnitvah (FRR). Veliko manj raziskav pa je bilo opravljenih s stališča uporabnosti, varnosti in sprejemljivosti biometričnih sistemov. Številni dejavniki vplivajo na porast uporabe biometričnih naprav. Senzorji so vse manjši, cenejši, bolj zanesljivi in tudi bolj ergonomsko zasnovani. Tudi biometrični algoritmi so vedno boljši in mnogi sistemi vključujejo funkcije za usposabljanje uporabnikov in izmenjavo izkušenj med uporabo. Poleg tega se biometrične naprave vključujejo v varnostne sisteme, kot je nadzor dostopa, šifriranje storitev itd. Vendar natančnost mnogih biometričnih sistemov, še vedno ni dovolj visoka, za nekatere aplikacije (npr. zelo velika zbirka podatkov). Prav tako je pogosta negativna relacija med natančnostjo biometričnega sistema in udobjem za uporabo. Najbolj natančni sistemi (npr. DNK, šarenica itd), so največkrat tudi najbolj nerodni za uporabo. Biometrični naprave imajo tudi pogosto težave z zajemom podatkov uporabnikov s posebnimi fizikalnimi lastnostmi, kot so zbledeli prstni odtisi, kar lahko pripelje do visoke stopnje neuspele registracije. Raziskave so pokazale, da so uporabniki še vedno previdni glede sprejemljivosti biometričnih tehnologij, saj koristi niso vedno očitne na drugi

strani pa so možnosti za zlorabo zasebnosti, velike. Kljub temu, je raziskava kanadskih državljanov v l. 2004 ugotovila, da 80% anketirancev meni, da se bo uporaba biometričnih sistemov zelo povečala v naslednjih 10 letih. Glede splošno razširjene uporabe biometričnih podatkov v varnostnih sistemih se razvijalci te tehnologije soočajo s številnimi temeljnih izzivi kot npr. biometrična lastnost ni skrivnost, tako da vedno obstaja tveganje, da se jo kopira ali ponaredi. Upravljanje in zagotavljanje zasebnosti pri osebnem nadzoru pri uporabi biometričnih sistemov bo tudi v prihodnosti zelo pomembno vplivalo na dejavnik sprejemanja te tehnologije (Patrick, 2004).

Raziskave temeljnega odnosa uporabnika do tehnologije (sprejemljivosti), se loteva Coventry (2005). S stališča potrošnika, je za sprejemljivost zelo pomembno, da je tehnologija:

- družbeno-socialno sprejemljiva,
- ustrezna za dano okolje,
- izpolnjenje zaznano potrebo,
- v osnovi razumljiva,
- uporabna in
- ne posega v zasebnost.

Izpolnjevanje teh pogojev bo zelo vplivalo na njihovo obnašanje do te tehnologije. Poleg tega, se sprejemljivost za uporabnika biometričnih sistemov spreminja glede na vrsto biometričnih podatkov, ki se uporabljajo in tudi glede na namen zaradi katerega se uporabljajo. Bistveno je zato prepoznati in razumeti specifične uporabnikove pogoje sprejemljivosti, ne pa splošne situacije. Negativni dejavniki, ki vplivajo na sprejemljivost uporabnikov vključujejo strah pred novostmi tehnologije, da je ne bodo mogli uporabiti in varstvo zasebnosti. Obstaja tudi splošno pomanjkanje javnega razumevanja, kako biometrija sploh deluje. To razumevanje razlike se pogosto izraža v smislu suma, nezaupanja, ali slepega sprejemanja. Kljub temu se je stopnja sprejemanja potrošnikov povečala v zadnjih nekaj letih:

Študija iz l. 2002 je pokazala, da je za 78 % ameriške javnosti, preverjanje biometričnih podatkov na bankomatih sprejemljivo (Westin, 2002). Pred nekaj leti, je bila zaznana potreba po dodajanju biometričnih podatkov na identifikacijske kartice (plačilne, zdravstvene itd.) za zmanjšanje zlorab. Medtem, ko tudi teroristične grožnje predstavljajo vedno večje pomisleke glede varnosti, so biometrični podatki večkrat izpostavljeni kot rešitev, tudi za takšna varnostna vprašanja. Zdi se, da je strah pred temi tveganji, pot do strinjanja in sprejemljivosti javnosti, tudi brez ustreznega razumevanja ali izkušenj s to tehnologijo. V raziskavi, ki je bila opravljena s strani Silicon.com, kar 75 % bralcev verjame, da je biometrija bolj varen postopek identifikacije od tradicionalnih radio frekvenčnih identifikacijskih metod (RFID), kartic, osebnih identifikacijskih kombinacij številk (PIN) itd. (Hallett, 2004). Po drugi strani pa mnogi uporabniki težko verjamejo, da lahko takšna »futuristična« tehnologija sploh dobro dela. Mnogi mislijo, da obstaja resnična možnost, da bodo zavrnjeni in ne bodo pridobili dostopa ali pa, da je takšna tehnologija lahko tudi celo zastrašujoča (Coventry, 2005). Ljudje ne marajo zavrnitve (je neprijetno) še posebej, če se to zgodi v javnosti. Poskusi uporabe biometričnih podatkov so pokazali, da lahko vplivajo na višjo raven čustev ob zavrnitvi. Kadar ima uporabnik že izoblikovan nek negativen odnos do tehnologije, bo ob vseh negativnih interakcijah, ta tehnologija služila le še za potrditev njegovega zavračanja. Uporabne študije so pokazale, da dejanske izkušnje z biometrično napravo pogojujejo izboljšanje sprejetja tehnologije (Thalheim, Krissler in Ziegler, 2002) vendar, če sistem kaže slabo uporabnost lahko dejanske izkušnje pogojujejo nesprejetje tehnologije. Iz tega lahko sklepamo, da so učinkovitost registracije uporabnika, usposabljanja za uporabo in jasna navodila ob uporabi sistema, ključni za uporabnost s tem pa tudi za sprejemljivost uporabnika. Nekateri uporabniki so v vezi s tehnologijo, izrazili zaskrbljenost glede higiene, zaradi dotika pri biometrični identifikaciji na osnovi prstnih odtisov in tveganje za zdravje, ob bolj naprednih tehnologijah, kot so identifikacija na osnovi šarenice ali mrežnice (IR skeniranje). Takšna stigmatizacija biometrije je še toliko bolj izrazita v primerih, ko je obvezna (nadzor meja za migrante, v vojski, identifikacija na področjih vojaškega delovanja itd.) (Woodward et al., 2001). Pogled nekaterih

pa celo predpostavlja bojazen, da bodo ubiti in bodo kriminalci ukradli njihove oči ali prste, kot je bilo to prikazano in ovekovečeno s filmi, kot so Mission Impossible in Minority Report itd.

Vendar mora biti na tej točki jasno, da nepravilna interpretacija podatkov in informacij, ter njihovo nestrokovno in kritično širjenje v medijih, lahko povzroči resne posledice zlasti na področju gospodarstva (razvoj in proizvodnja biometričnih tehnik), kot tudi pri uporabi biometrije, na splošno. Uporabniki, ki so že na splošno neradi v sistemu identifikacije, lahko v vezi z uporabo biometrije sprožajo govorice, da lahko biometrični proces vpliva na zdravje ali lahko krši zasebnost. Seveda v vezi s tem obstajajo mnoge raziskave kot ugovor na te pomisleke. Pri uporabi biometrije na splošno ne obstaja več tveganja za zdravje, kot je tveganje pri uporabi kljuke, v primeru, ko se dotaknemo drugih ljudi, pri ravnanju z denarjem ali rokovanjem. Veliko biometričnih naprav sicer uporablja infrardečo svetlobo za osvetlitev delov telesa, ki se uporabljajo za preverjanje pristnosti. Eden od motivov za uporabo te svetlobe, je dejstvo, da krvne žile absorbirajo infrardečo svetlobo hitreje kot okoliško tkivo, vendar tudi s tega stališča, glede na opravljene raziskave, poškodbe niso možne. Po mnenju nekaterih posameznikov, je telo izpostavljeno sevanju, ki ga absorbira in v vezi s tem lahko obstajajo nekateri škodljivi učinki na telesna tkiva. Kljub temu, da sedaj ni dokazanih negativnih učinkov za zdravje pri uporabi biometrije, so se proizvajalci biometrične tehnologije obrnili na nekatere poklicne uprave za zdravje (npr.: Occupational Safety and Health Administration - OSHA), z zahtevo ocene tveganj v vezi s to tematiko.

Rezultat naše raziskave je bila podana percepcija terorizma v Sloveniji, iz katere sledi neposredna primerjava z drugimi EU državami, kjer so doživeli teroristične napade in Kanado, ki velja za eno izmed držav, kjer terorizem sploh ne doživljajo kot grožnjo, ki bi imela vpliv na njihovo življenje.

12 SMERNICE IN IZHODIŠČA ZA NADALJNJE RAZISKOVANJE

Večplastni in večdimenzionalni varnostni izzivi, tveganja in grožnje v regiji, Evropi in svetu povzročajo številne negotovosti pri zagotavljanju nacionalne in mednarodne varnosti. Za pravočasno načrtovanje in izvajanje ukrepov za ohranjanje in krepitev tako nacionalne kot tudi mednarodne varnosti, je potrebno vzpostaviti učinkovit sistem zgodnjega odkrivanja in opozarjanja na potencialna tveganja in grožnje. Biometrija je vsekakor eden izmed elementov zgodnjega odkrivanja tveganj, predvsem v smislu nadzora ljudi, ki imajo za seboj kriminalna dejanja ali imamo informacije, da jih planirajo. V skladu z navedenim morajo biti vzpostavljeni tudi organizacijski, kadrovski in materialni temelji za sodelovanje in izmenjavo obveščevalnih in varnostnih podatkov na nacionalni ravni, v okviru dvostranskega sodelovanja ter v okviru zavezništev.

Ugotovili smo torej, da je biometrija eden izmed ukrepov s katerimi lahko izboljšamo varnost na vseh nivojih. V tehničnem smislu pa nas seveda tudi zanima, ali je biometrija varnejša od tiste s klasičnimi karticami ali PIN kodo? Seveda, z nekaterimi razumnimi ukrepi je mogoče povečati varnost, toda če povprečni uporabnik naleti na kakšnega hekerja ali motivirano kriminalno združbo, najbrž nima veliko možnosti da se zoperstavi, kraji identitete. Lahko zaščitimo računalnike s požarnimi zidovi, s protivirusnimi programi, lahko pošiljamo sporočila, kodirana s šifrirnimi programi, kot je program PGP, lahko anonimno brskamo po spletu s programom »Tor«, toda nikoli ni izključena možnost, da bo kakšen poznavalec, kibernetski kriminalec ali tajna služba s sofisticirano opremo našla varnostno luknjo ali dekodirala sporočila. Sodobne obveščevalne službe in policija uporabljajo učinkovitejše in še bolj sofisticirane načine nadzora, kot smo jih navedli v disertaciji. Ob tem pa je potrebno izpostaviti, da je pravna in zakonodajna podlaga v večini držav še na trhlih in nedorečenih temeljih (Dobovšek, 2007).

Zloraba podatkov, s krajo identitete je še vedno neizogibno tveganje sodobne informacijske družbe. Študije ugotavljajo, da goljufije na področju kraje

identitete oškodujejo evropske države za 15-20 bilijonov EUR letno (European Biometric Portal [EBP], 2007). Za mnoge zainteresirane strani, ki sodelujejo v boju proti goljufijam, uporaba biometrije pomeni eno izmed najbolj obetavnih poti za drastično zmanjševanje goljufij z naslova identifikacije (Department of The Treasury [DOT], 2005). V Veliki Britaniji, so goljufije identitete, obravnavane kot ena od najhitreje rastočih kaznivih dejanj. Ob prvih študijah opravljenih v l. 2002, so stroški teh goljufij ocenjeni na 1,3 milijarde funtov letno. Tudi najnovejše raziskave podkrepijo zgornje ocene in te stroške ocenjujejo na 1,7 milijard funtov letno. Položaj pa se ne razlikuje tudi v drugih državah članicah EU (IWS, 2001). Prav tako Nordijske države izpostavljajo potrebo po globalni sistemski prenovi zaradi kriminala povezanega s krajo identitete. Zvezna komisija (Federal Trade Commission – FTC) ocenjuje, da izgube ZDA zaradi kraje identitete znašajo 47,6 bilijonov dolarjev, za l. 2004 (DOT, 2005).

Libicki, eden prvih avtorjev, ki se je ukvarjal s področjem informacijskega bojevanja, meni, da informacijsko bojevanje, kot posebna oblika vodenja vojne, ne obstaja. Obstaja pa sedem oblik informacijskega bojevanja, v katerih informacija nastopi kot sredstvo, cilj in orožje:

- bojevanje na poveljniško-nadzornem področju (Command-and-Control Warfare - C2W),
- bojevanje, ki temelji na obveščevalni dejavnosti (Intelligence-based Warfare),
- elektronsko bojevanje (Electronic warfare),
- psihološko bojevanje (Psyhological warfare),
- hekersko bojevanje (»Hacker« warfare),
- ekonomsko informacijsko bojevanje (ang. Economic Information warfare) in
- kibernetsko bojevanje (Cyber warfare) (Libicki, 1995).

Arquilla in Ronfeldt vidita bojevanje v prihodnosti kot informacijsko bojevanje in govorita o t.i. kibernetskem »Cyberwar« in omrežnem bojevanju »Netwar«. Kibernetsko bojevanje se nanaša na vojaško sfero, kjer je govora predvsem o konfliktih visoke intenzivnosti (High Intensity Conflict - HIC) in konfliktih

srednje intenzivnosti (Middle-Range Conflict). Omrežno bojevanje pa obsega socialno, politično, vojaško in ekonomsko obliko konflikta, kjer govorimo predvsem o konfliktih nizke intenzivnosti (LIC), operacijah drugačnih od vojne (Operations Other Than War) in drugih, predvsem nevojaških, oblikah konflikta ter kriminala (Arquilla in Ronfeldt, 1996).

V zadnjih dveh desetletjih smo lahko priča precejšnemu preobratu v razmišljanju in tudi življenju, ki ga zaznamuje čedalje večja liberizacija gospodarstva in mobilnost kapitala ter ljudi. Za čim manj ovirano mobilnost rabimo identifikacijske sisteme, ki omogočajo zanesljivo identifikacijo kadarkoli in kjerkoli. Bistven dejavnik je biometrična identifikacijsko komunikacijska tehnologija, ki s svojim razvojem pripomore, da uporaba fizičnih identifikatorjev ni več nujna za potrditev naše istovetnosti (Brumnik, 2011). Seveda nove biometrične identifikacijske tehnologije prinašajo nove organizacijske paradigme in vplivajo na sociološke spremembe. Dosedanje raziskave celičnih avtomatov (Šemrov, Kotnik in Miklavčič, 1996) lahko uporabimo kot modele za kompleksne biokibernetske sisteme in za modeliranje kemičnih reakcij pri vgrajevanju identifikacijskih elementov v človeško telo. To bi lahko veliko doprineslo k razvoju bionskih čipov (United States Space Command [USSC], 2002).

Globalizacija je torej družbeni pojav, ki ima širše politične, socialne, tehnološke in varnostne razsežnosti. Da bi lahko zadostili pogojem sprejemljivosti biometrije moramo upoštevati stroge varnostne standarde z minimalnim vplivom na človekovo avtonomijo.

12.1 *Prihodnost in smernice za nadaljnje delo pri modeliranju sprejemljivosti biometričnih sistemov*

Pričakovati je, da bo biometrična tehnologija kljub pomislekom nekaterih inštitucij (urad za varstvo osebnih podatkov) in posameznikov, dosegla velik razmah tudi v našem vsakodnevnem življenju. Razvoj biometrične tehnologije sproža mnogo etičnih vprašanj, ki zadevajo zasebnost in sprejemljivost

nadzornih tehnologij (Nadel, 2006). Uporaba biometrije lahko povzroča tehnične probleme in sproža moralna vprašanja (Gates, 2004), ki se jih je potrebno zavedati že ob samem razvoju tehnologije in kasneje ob sami uporabi, še posebej s strani operaterjev. Celotna družba je postala vedno bolj odvisna od informacijskih sistemov in zaradi tega tudi bolj ranljiva. Med novimi družbenimi problemi, povezanimi z avtomatizacijo identifikacije, so najbolj pereči: računalniški kriminal, varnost računalniških sistemov, kraja programske opreme, varstvo intelektualne lastnine, računalniški virusi, nezanesljivost programske opreme in škoda, ki jo napaka v njej lahko povzroči, podatkovne zbirke in varstvo zasebnosti ter druge družbene posledice ekspertnih sistemov (Brumnik, 2011).

Problem tveganja današnje sodobne družbe je vsekakor terorizem. Biometrija je primer tehnologije, s katero se danes vse bolj skuša uveljavljati družbeni nadzor. Poskrbeti pa je potrebno, da se družbeni nadzor ne izvaja zgolj na podlagi nekih hipotetičnih tveganj. Zato je tu problem, kako se odločati pod pogoji velike negotovosti, še toliko bolj očiten.

Sodeč po napovedih bo v novem tisočletju področje identifikacije doseglo nesluten razvoj. Dober kazalec zrelosti tehnologije so investicije in vložki v panogo. Leta 2002 je ameriška vlada vložila v biometrično industrijo 16,63 milijona dolarjev. Pričakovani dohodek te industrije v letu 2014 je 9000 milijonov dolarjev (International Biometric Group, 2008).

Glede na zahteve zakona o varstvu podatkov (ZVOP-1) je ključna pridobitev dovoljenja pri informacijskem pooblaščencu RS (IP-RS, 2010), pri čemer je treba utemeljiti, zakaj je uvedba biometričnih ukrepov v vašem primeru nujna za enega ali več taksativno naštetih namenov: opravljanje dejavnosti, varnost ljudi ali premoženja, varovanje tajnih podatkov ali varovanje poslovne skrivnosti.

Biometrične metode postajajo zelo popularna alternativa tradicionalnim pristopom k identifikaciji. Uporaba biometričnih metod poenostavlja identifikacijo in povečuje zanesljivost, saj so elementi identifikacije (prstni odtis) neprenosljivi in preprečujejo zlorabo ter nepooblaščeno uporabo. Prednosti biometrije so jasne, saj ni potrebna uporaba kartice ali drugih identifikacijskih elementov. Z avtomatizacijo identifikacije bosta omogočena združevanje in primerjava trenutnih podatkov s podatki iz integralnega informacijskega sistema ali drugih aplikacij. Vse to pa zagotavlja večjo preglednost ter boljše načrtovanje in izkoristek procesov identifikacije (Brumnik, 2011).

Nadaljnje raziskave sprejemljivosti identifikacijskih sistemov lahko usmerimo v proučevanje vpliva modeliranja sprejemljivosti glede na različne stopnje »efekta grožnje«, ki jih lahko povežemo tudi s finančnimi rezultati.

13 ZAKLJUČEK

Boj proti terorizmu je dolgotrajno, zahtevno in kompleksno delo, ki se zelo razlikuje od vrste in izvora terorističnega delovanja. Nujno potrebno je upoštevati pravne vidike (upoštevanje človekovih pravic, vladavine prava in mednarodne dogovore ter sporazume), obenem pa posvetiti veliko mero pozornosti izvoru terorizma (razlogu) in pogojem, ki omogočajo njegov obstoj in širjenje ter jih odpraviti. Večkrat namreč pridemo do perečega razhajanja med osnovnimi človekovimi pravicami in varnostjo (zasebnosti, osebnih podatkov itd.), kar smo v našem delu tudi obravnavali. Ključ za odpravo omenjene problematike je spoštovanje človekovih pravic, ki je skupaj s spoštovanjem pravnih norm močno orožje proti terorizmu. Upoštevanje obeh skupaj je osnovni pogoj v boju proti terorizmu. To je rezultat spoznanj ob dolgoletnih in tragičnih izkušnjah s terorizmom v svetovnem prostoru.

Kot zaključek pa še izhodišče možnosti, da lahko, smemo in moramo v zvezi s terorizmom pričakovati od kazenskih procesov z vidika: mednarodne izročitve osumljencev terorističnih dejanj (še posebej je problematika pereča, kadar gre za izročitev osumljencev državi, za katero je znano, da izvaja mučenje, kršitve absolutne prepovedi mučenja, nehumanega in ponižujočega ravnanja in nedosledno izvaja pravice do poštenega sojenja itd.).

Razvoj transportne infrastrukture in sredstev, predvsem na področju letalstva in cestnega prometa je eden izmed najpomembnejših vzrokov, da je terorizem prerastel meje nacionalnih držav in prevzel mednarodni značaj. To je omogočilo lažjo in hitrejšo prometno povezavo med državami in tudi olajšalo dostop do njih. Razcvet mednarodnega turizma je povzročil, da so množice turistov iz različnih držav postale priljubljena tarča teroristov, ki so tako internacionalizirali svoja dejanja. Mednarodna trgovina se je razširila in poglobila gospodarske in politične odvisnosti manj razvitih držav od bolj razvitih. Nezadovoljstvo z gospodarskimi ali političnimi razmerami je večkrat usmerjeno na države, ki v očeh teroristov predstavljajo glavne krivce za neugodno situacijo v njihovi domovini.

Hiter tehnološki razvoj pa je omogočil razširitev in izboljšanje komunikacijskih sredstev in razvoj računalniškega komuniciranja preko interneta in elektronske pošte. To je močno olajšalo komunikacijo med teroristi, poenostavilo način izmenjave informacij in koordinacijo terorističnih dejanj. Na razmah mednarodnega terorizma pa je med drugim vplivala tudi velika rast prebivalstva, kar je povzročilo prenaseljenost in revščino ter spodbudilo k večjim imigracijam ljudi v druge države. Potencialni teroristi imajo s tem večje možnosti do ogrožanja življenja in prikritega načrtovanja svojih dejavnosti pod zaščito, do nedavnega večinoma dokaj liberalnih, migracijskih zakonov v tujih državah.

13.1 *Prevencija*

Kot smo v raziskavi že omenili, se je potrebno zavedati, da internet ne pozna meja in da je najboljša zaščita, preventiva. Sprotno spremljanje dogajanja v virtualnem svetu ter poznavanje kriminalitete nam pomaga prepoznati dogodke, katerih namen je oškodovanje. V ta namen obstajajo spletne strani, ki nas sprotno opozarjajo na nove pojavne oblike računalniškega kriminala ter nam v primeru škodnega dogodka, dajejo napotke za ravnanje (Internet Crime Complaint Center [IC3], 2011); (National Consumers League [NCL], 1999). Računalniška kriminaliteta v Evropi ni tako mlada disciplina, vendar je z razmahom računalniške tehnologije postala pereč problem 21. stoletja (Podbregar in Slapar, 2006) . V naši študiji je bilo nakazanih kar nekaj tehničnih (situacijska prevencija) in zakonskih ukrepov (kriminalna prevencija) za reševanje problematike računalniškega kriminala in terorizma. Vendar se je potrebno zavedati, da samo ta dva aspekta pri preprečevanju računalniške kriminalitete ne bosta zadostna. Iz raznolikosti pojavnih oblik kriminalitete je mogoče sklepati, da ni mogoče govoriti o univerzalni metodi za preprečevanje kriminalitete (Meško, 2000). Tako tudi ni mogoče uspešno preprečevati računalniške kriminalitete z orodji, ki jih uporabljamo pri drugih pojavnih oblikah kriminala. Huges (1998) govori o kameleonskem konceptu, saj preprečevanje kriminalitete obsega različne ukrepe, metode in pobude, ki jih je mogoče v različnih okoliščinah različno razumeti in izvajati.

Razumevanje storilcev kaznivih dejanj odpira novo poglavje, ki pa dosedaj pri prevenciji računalniškega kriminala ni redno prisotno. Vedno več se sicer govori o zasvojenosti z računalniškimi igrami mladostnikov, vendar je sociološki aspekt računalniške kriminalitete je le redko prisoten. Socialna strategija je nujnost prevencije, tudi pri računalniški kriminaliteti. Problem kriminalitete je namreč v družbi in tudi v teh primerih se je potrebno usmeriti v spreminjanje družbenega okolja in motivacije storilcev.

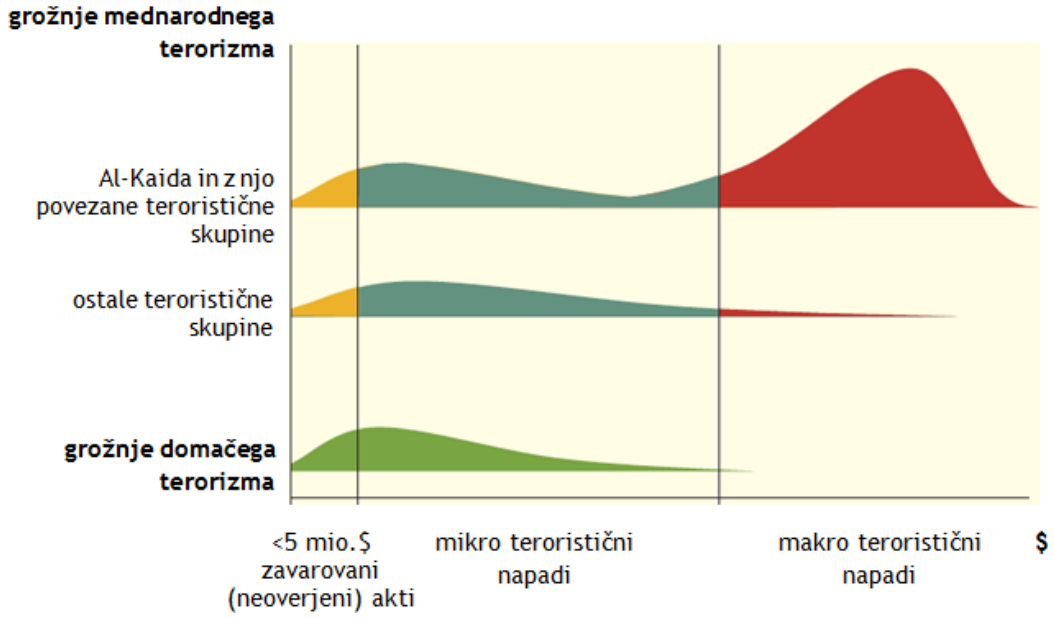
13.2 *Upravljanje terorističnih tveganj*

Grožnja terorističnih napadov predstavljajo in bodo predstavljale veliko tveganje za mnoge discipline, kot so gospodarstvo, zavarovalništvo, ekonomija itd. Teroristični napadi v ZDA l. 2001 so po ocenah povzročili 80-90 bilijonov dolarjev izgube in stroškov (Kunreuther, Michel-Kerjan in Porter, 2003). Katastrofalne posledice terorizma so motivirale več milijard dolarjev naložb v ZDA in drugod v orodja za zaznavanje, analizo in oceno terorističnih groženj, s ciljem izboljšanja varnosti in zaščite. Povečan obseg za povpraševanje po teh orodjih in naložbe, so rezultat skrbnega premisleka za izvajanje, delovanje in vzdrževanje varnosti kakor tudi koristi, ki izhajajo iz zmanjšanja stroškov izpostavljenosti in prihodnjih izgub. V nasprotju z naravnimi ali naključnimi dogodki, kot so poplave, potresi ali izpad infrastrukturnih sistemov je terorizem v osnovi kontradiktoren in predvidljiv pojav, torej se ga da napovedati.

Za obravnavanje in oceno teh tveganj obstajajo mnoga programska orodja, kot so npr.: RMS™ (Terorism Risk Model) s katerimi lahko izdelamo oceno za določeno območje ali teroristično grožnjo. Ta orodja temeljijo na mnenjih strokovnjakov, metodologijah ter raziskavah in predpostavkah ključnih ozadij terorističnih napadov kar zagotavlja podlago za RMS modeliranje. RMS model za ocenjevanje in kvantifikacijo terorističnega tveganja, zagotavlja celovit pogled na nevarnost terorizma v ZDA in v ocenah upošteva tako tuje kot domače teroristične organizacije. RMS podpira več-nivojske analize tveganja, za certificirane in neoverjene dogodke, ki vplivajo na oceno lastnine, možnost prekinitve poslovanja, odškodnine delavcev, ocena človeškega življenja,

osebne nesreče, smrt zaradi nezgode povezane s terorističnim napadom itd. Po vzoru in pogostosti terorističnih napadov Al-Kaide v ZDA v l. 2001 in naprej, to modeliranje terorističnega tveganja vključuje in upošteva tudi možnosti za več sinhronih napadov. Model uporablja najnovejše metode za kvantifikacijo vpliva morebitnih terorističnih napadov tudi v odvisnosti od uporabe konvencionalnega in nekonvencionalnega orožja (v smislu uporabe konvencionalnega orožja s kemičnimi, biološkimi, radiološkimi in jedrskimi (Chemical, Biological, Radiological, and Nuclear - CBRN) itd. in nekonvencionalnega, z informacijskimi, elektronskimi, socialnimi itd. načini napada).

Graf na sliki 12 kaže primer modeliranja tveganj, ki so razporejena in ovrednotena (finančna ocena stroškov in razsežnosti) glede na domače in mednarodne teroristične organizacije.



Slika 12: RMS™ ocena tveganja terorističnih napadov glede na domače in mednarodne teroristične skupine za ZDA

Določanje strategije za izboljšanje varnosti (krizni menedžment) za primere terorističnih aktivnosti, se radikalno razlikuje od običajnih problemov odločanja v varnostno negotovih situacijah. To je posledica prilagajanja različnim taktikam ter obnašanju teroristov in tudi zaradi pomanjkanja

natančnih podatkov, potrebnih za modeliranje in ocenjevanje tveganja določene teroristične aktivnosti. Način za reševanje problematike omejene pomanjkljivosti podatkov, je uporaba strokovnega znanja pri modeliranju.

Ocenjevanje predvidljivih stroškov je samo ena možnost, ki spada v spekter tehnoloških zmogljivosti delovanja teroristov, s ciljem škodovanja neki družbi. Uničevalne posledice lahko teroristi dosežejo ne le z uporabo orožja za množično uničevanje ali s kinetičnimi napadi na ciljno infrastrukturo, ampak tudi z incidenti, ki imajo daljnosežne psihološke posledice neke družbe, kot so samomorilski bombni napadi, poboji in umori voditeljev. To so premišljene in preračunane poteze s ciljem povzročitve dolgotrajne ostre, neznosne bolečine z namenom, da bi ciljano družbo spravili na kolena.

Seveda je določanje dejavnikov in njihovega vpliva pri modeliranju varnostne ocene težaven proces, ki zahteva usposobljene strokovnjake. Tudi, če je pri modeliranju uporabljeno vso razpoložljivo strokovno znanje, so odločitve vedno pogojene z neko stopnjo negotovosti, ki je ne smemo prezreti. Kadar takšne negotove vrednosti dejavnikov uporabljamo za numerično ocenjevanje, lahko končne izračunane vrednosti vsebujejo zelo velike intervale negotovosti. Končni cilj naše raziskave in študije (t.j. $UTAUT_{EF}$ model sprejemljivosti biometrične tehnologije), je v pomoč pri reševanju težav pri investicijskih in varnostno-tehničnih odločitvah. Z uporabo ustrezne stohastične metodologije, ki upošteva statistično negotovost, ki je del nekega terorističnega (varnostnega) problema, lahko model v praksi koristno uporabimo za podporo odločanju, kadar sprejemamo kompleksne odločitve glede identifikacijske tehnologije, na osnovi varnostih ocen tveganja in drugih tehničnih priporočil.

14 LITERATURA IN VIRI

Abelson, H., Lessig, L. (1998). *Digital Identity in Cyberspace*. Pridobljeno 14.9.2011 na http://www.swiss.ai.mit.edu/6095/student-papers/fall98-papers/identity/white-paper.html

Academic and Research Network of Slovenia. (2008). *Varnostna priporočila*. Pridobljeno 7.10.2011 na http://www.arnes.si/pomoc-uporabnikom/varnostna-priporocila.html

Adelman, G. (2010). *Not every Violent act Amounts to Terorrism*. Pridobljeno 17.9 2010 na http://www.familysecuritymatters.org/publications/id.5568/pub_detail.asp

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. V J. Kuhl in J. Beckmann (ur.), *Springer series in social psychology* (str. 11-39). Berlin: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

AL-Harby, F., Qahwaji, R. in Kamala, M. A. (2010*). Users' Acceptance of Secure Biometrics Authentication System: Reliability and Validate of an Extended UTAUT Model, Networked Digital Technologies*. Prague: SpringerLink.

Al-Gahtani, S., Hubona, G. in Wang, J. (2007). Information technology (IT) in Saudi Arabia. Culture and the acceptance and use of IT. *Information & Management, 44,* 681–691.

Al-Somali, S. A., Gholami, R. in Clegg, B. (2009). An investigation into the acceptance of online banking in Saudi Arabia. *Technovation, 29,* 130-141.

Al-Harby, F., Qahwaji, R. in Kamala, M. (2009). *The Role of User Self-Efficacy for the Acceptance of Biometrics Fingerprint Authentication System in E-commerce: The Use of UTAUT Model*. Pridobljeno 18.7.2011 na http://www.scribd.com/doc/23886048/The-Role-of-User-Self-Efficacy-for-the-Acceptance-of-Biometrics-Fingerprint-Authentication-System-in-E-commerce-The-Use-of-UTAUT-Model

Andress, J., Winterfeld, S. in Rogers, R. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Boston: Syngerss/Elsevier.

Anti-Phishing Working Group. (2011). *Crimeware and Phishing*. Pridobljeno 02.07.2011 na http://www.antiphishing.org/crimeware.html

Anžič, M. (2005). *Vloga biometričnih metod pri preprečevanju terorizma*. Pridobljeno 02.10.2011 na http://dk.fdv.uni-lj.si/dela/Anzic-Marko.PDF

Arah, M. (1995). *Evropska unija: vizija političnega združevanja*. Ljubljana: Arah consulting.

Atwan, A. B. (2006). *The secret history of Al-Qaida*. London: Saqi Books.

Axelrod, E. M. (2009). *Violence goes to the internet: Avoiding the snare of the net*. Springfield: Charles C Thomas Publisher.

Bandura, A. (1977a). Self-efficacy: Towards a unifying theory of behavioral change. *Psychological Review, 84,* 191–215.

Bandura, A. (2001). Social cognitive theory: An agentive perspective. *Annual Review of Psychology, 52*(1), 34-45.

Bedi, R. (2005). *Telecom - The Terrorism Risk*. Pridobljeno 4.11.2010 na http://www.pvtr.org/pdf/Financial%20Response/Telecom%20-%20The%20Terrorism%20Risk.pdf

Belič, I. (2001). Informacijski terorizem. *Varstvoslovje,* 3(4), 262–268.

Benyon, J. (1997). The developing system of police cooperation in the European Union. V W.F. McDonald (ur.), *Crime and law enforcement in the global village* (str.103-122). Cincinnati Anderson Publishing Co.

Biegelman M.T. (2009). *Identity Theft Handbook: Detection, Prevention, and Security*. New York: John Wiley and Sons.

Biometric Evaluation Methodology Working Group. (2002). *Biometric Evaluation Methodology*. Pridobljeno 4.10.2010 na http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf

Blane, J. V. (2003). *Cybercrime and cyberterrorism: Current issues*. New York: Nova Science Publishers.

Blaze, M., Feigenbaum, J. in Lacy, J. (1996). *Decentralized Trust Management*. Pridobljeno 12.9.2011 na http://www.crypto.com/papers/policymaker.pdf

Bucci, S. P. (2009). *The confluence of cyber crime and terrorism*. Pridobljeno 23.4.2011 na http://www.insideronline.org/.cfm?id=10340

Blekxtoon, R. (2004). *The European Arrest Warrant, in ICLN (International Criminal Law Network, The Hague) and EULEC (European Institute for Freedom, Security and Justice, Brussels), joint co-operation, European Co-operation Against Terrorism*. Nijmegen: Wolf Legal Publishers.

Boyd, M. J. (2009). *Navy Contributions to Identity Management: Biometric Consortium Conference – 2009* . Pridobljeno 17.3.2011 na Dhttp://forum.prisonplanet.com/index.php?topic=187829.0

Boyle, E. J. (2002). An Ethical Decision Making Process for Computing Professionals. *Ethics and Information Technology, 4,* 267-277.

Bratuša, T. (2007). *Napad na slovenijo*. Pridobljeno 7.11.2010 na http://www.mojmikro.si/preziveti/varnost/napad_na_slovenijo

Brown, M. (1994). *S-Tools for Windows*. Pridobljeno 27.10.2010 na http://www.spychecker.com/program/stools.html

Brumnik, R. in Balantič, Z. (2008). Reliability and efficacy of identification systems and supply chain management. *Strojniški vestnik*, *54*(11), 783-795.

Brumnik, R. in Podbregar, I. (2011). How terrorists use the internet. V G. Meško, A. Sotlar in J.Winterdyk (ur.), *Policing in Central and Eastern Europe - social control of unconventional deviance: Conference proceedings* (str. 158-174). Ljubljana: Faculty of Criminal Justice and Security.

Brumnik, R. (2011). *Učinkovitost in zanesljivost biometričnega sistema pri osebni identifikaciji*. Doktorska disertacija, Kranj: Univerza v Mariboru, Fakulteta za organizacijske vede.

BS7799. (1995). *Code of practice for Information Security Management. CEPS (Centre for European Policy Study). The European Arrest Warrant, A Good Testing Ground for Mutual Recognition in the Enlarged EU*. Pridobljeno 7.11.2010 na http://www.ceps.be/Article.php?article_id=295

Bunyan, T. (2005). Unaccountable Europe: Unknown to most of its citizens, behind the closed doors of Brussels the European Union is making serious inroads on their privacy. *Index on Censorship, 3*. 52-53.

Bulmer, M. (2003). *Franciss Galton; Pioneer of Heredity and Biometry*. Oxford: John Hopikins University Press.

Casale, D. (2008). EU Institutional and Legal Counter Terorrism Framework. *Defence Against Terrorism Review, 1* (1). Pridobljeno 17.10.2010 na http://www.coedat.nato.int/publications/datr/04.Davide%20CASALE.pdf

Carmines, E. G. in Zeller, R. A. (1979). *Reliability and validity assessment*. Londres: Sage.

Casella, R. (2003). The false allure of security technologies. *Social Justice*, *30*(3), 82-93.

Cassese, A. (2001). Terrorism is also Disrupting Some Crucial Legal Categories of International Law. *American Journal of International Law, 95,* 993.

Cassidy, W. L. (1977). *Planned Political Assassinations: An Introductory Overview*. Gaithersburg: Md Publishing.

Center for Defense Information. (2007). *Terrorist Networks*. Pridobljeno 24.08.2011 na http://www.cdi.org/program/issue/index.cfm?ProgramID=39&issueid=56

Cisco. (2011). Email Attacks: This Time is Personal. Pridobljeno 29.08.2011 na http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

Chen, H. Reid, E. in Sinai, J. (2008). *Terrorism informatics: Knowledge management and data mining for homeland security*. New York: Springer.

Clarke, R. (2006*). Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Pridobljeno 07.09.2011 na http://www.rogerclarke.com/DV/Intro.html

Coker, C. (2004). *The future of war: The re-enchantment of war in the twenty-first century*. Oxford: Wiley-Blackwell publishing.

Colarik, A. M. (2006). *Cyber terrorism: Political and economic implications*. London: Idea Group Publishing.

Coleman, K. (2003). *Cyber Terrorism*. Pridobljeno 23.10.2011 na http://www.directionsmag.com/article.php?article_id=432

Cordesman, A. H. (2002).*The lessons of Afghanistan: War fighting, intelligence, and force transformation*. Washington: CSIS Press.

Community Research and Development Information Service. (2003). *BioVision: Roadmap for Biometrics In Europe to 2010*. Pridobljeno 7.9.2011 na http://oai.cwi.nl/oai/asset/4057/04057D.pdf

Council of the European Union. (1999). *Article 35 and 37 of the Presidency Conclusions to the Tampere*. Pridobljeno 17.11.2010 na http://www.europarl.europa.eu/summits/tam_en.htm

Council of the European Union. (2002a). *Framework Decisions on Combating Terrorism*. Pridobljeno 18.11.2010 na http://www.eur-lex.europa.eu/pri/en/oj/dat/2002/l_164/l_16420020622en00030007.pdf

Council of the European Union. (2002b). *Framework Decision on the European arrest warrant and the surrender procedures between Member States*. Pridobljeno 17.11.2010 na http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/ l_190/l_19020020718en00010018.pdf

Council of the European Union. (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*. Pridobljeno 27.11.2010 na http://conventions.coe.int/Treaty/en/Treaties/html/189.htm

Council of the European Union. (2004). *Declaration on Combating Terrorism, Brussels*. Pridobljeno 4.11.2010 na http://ue.eu.int/uedocs/cmsUpload/DECL-25.3.pdf

Council of the European Union. (2005). *Draft Conclusions of the Representatives of the Government of the Member States on common minimum security standards for Members States' national identity cards*, 14351/2005. Pridobljeno 27.4.2011 na http://www.statewatch.org/news/2005/nov/eu-biometric-ID-Cards-Conclusions. pdf

Cooperative Association for Internet Data Analysis. (2011). *Research security*. Pridobljeno 17.9.2011 na http://www.caida.org/research/security/#Publications

Coventry, L. (2005). *Usable Biometrics: Securitiy and usability*. London: Human Centred system group.

Crotty, W. J., Kirkham, J. F. in Levy, S. G. (1970). *Assassination and Political Violence*. New York: Harper and Row.

Cryptome. (2011). *Nadzorovana omrežja: NSA*. Pridobljeno 04.06.2011 na http://cryptome.org/nsa-ip-update9.htm; http://cryptome.org/info/

Čaleta, D. (2011*). Ocena uspešnosti procesov zoperstavljanja terorizmu v mednarodnem okolju 10 let po terorističnih napadih na ZDA*. Pridobljeno 5.8.2011 na http://www.ics-institut.com/images/stories/PPT/aleta.pdf

Černič-Letnar, J. (2011). *Varstvo človekovih pravic v boju zoper terorizem*. Pridobljeno 17.9.2011 na http://www.icsinstitut.com/images/stories/PPT/erni.pdf

Dalgaard-Nielsen, A. in Hamilton, D. S. (2006). *Transatlantic homeland security: Protecting society in the age of catastrophic terrorism*. London: Routledge.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Doctoral dissertation, Sloan: School of Management, Massachusetts: Institute of Technology.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Den Boer, M. (2003). The EU Counterterrorism Wave: Window of Opportunity or Profound Policy Transformation?. V M. Van Leuween (ur.), *Confronting Terrorism. European Experiences, Threat Perceptions and Policies* (str. 189). Haag: Kluver Law international.

Denning, D. (1999). *Information warfare and security*. Berkeley, Sidney, Bonn: Addison-Wesley.

Denning, D. (2001). "Activism, Hactivism, and Cyberterrorism. The internet is a Tool of Influencing Foreing policy. *The Computer Security Jouranl, 16*(3), 15-35.

Denning, P. J. (2005). *Is Computer Science Science?*. Pridobljeno 4.10.2011 na http://cs.gmu.edu/cne/pjd/PUBS/CACMcols/cacmApr05.pdf

Department of The Treasury. (2005). *The Use of Technology to Combat Id entity Theft*. Pridobljeno 13.5.2011 na http://www.cbanet.org/files/FileDownloads/BiometricsStudy.pdf

Devost, M. G., Houghton, B. K. in Pollard, N. A. (2006). *Information Terrorism: Can You Trust Your Toaster? Sun Tzu Art of War in Information Warfare Research Competition*. Washington: Institute for National Strategies Studies.

Direktiva 95/46/EC. (1995). *Protection of individuals with regard to the processing of personal data and on the free movement of such data*. Pridobljeno 27.5.2011 na http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46

Direktiva 58/ES. (2002). *Direktiva o zasebnosti in elektronskih komunikacijah*. Pridobljeno 15.1.2011 na http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SL:NOT

Dobovšek, B. (2007). Kibernetska kriminaliteta bodočnosti. *Varnostni forum ISSN 1581 9221*, str. 14-16.

Dorizzi, B. (2006). New trend in biometrics. V S. S Calvante, R. F. Colare in P. C. Barbosa (ur.), *Telecommunication: Advanced and Trends in Transmission, Networking and Applications* (str. 173-183). Pridobljeno 16.10.2010 na http://www.gtel.ufc.br/~charles/PDF/book_telecommunications.pdf

Dvoršak, A. (2003). *Detektiv*: *Taktika in metodika poizvedovanja & primeri*. http://www.detektiv.si/files/NoveDatoteke/DETEKTIV%20-%20taktika,%20metodika,%20primeri.pdf

Electronic Privacy Information Center. (2004). Privacy and Human Rights Report. Pridobljeno 14.3.2011 na https://www.privacyinternational.org/article/privacy-and-human-rights-2004

Electronic Frontier Foundation. (2011). *What is a Tor Relay?*. Pridobljeno 12.2.2010 na https://www.eff.org/torchallenge/what-is-tor/

Emigh, A. (2005). *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*. Pridobljeno 20.4.2011 na http://www.antiphishing.org/Phishing-dhs-report.pdf

Emigh, A. (2006). "*The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond*". Pridobljeno 20.9.2010 na http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf

Estevez, M. L. M., Pavolka, D. in Nižňansky, J. (2006). *European response to Terrorism:The Caese of Spain and Slovakia*. Pridobljeno 25.11. 2010 na http://www.mod.gov.sk/data/files/518.pdf

European Biometric Portal. (2007). *Biometrics in Europe*. Pridobljeno 27.10.2010 na http://www.scribd.com/doc/11770142/Bio-Metrics-in-Europe-Trend-Report

Euractiv. (2004). »*Biometric Era*« *raises fears over privacy, 15 August*. Pridobljeno 27.11.2010 na http://www.euractiv.com/en/justice/biometric-era-raises-fears-privacy/article-111988

Euractiv. (2005). *Biometrics & Democracy*. Pridobljeno 17.11.2010 na http://www.euractiv.com/en/justice/biometrics-democracy-archived/article-139471

Euractiv. (2005*). European Arrest Warrant ruled unconstitutional in Germany, 19 July 2005*. Pridobljeno 27.5.2011 na http://www.euractiv.com/en/security/european-arrest-warrant-ruled-unconstitutional-germany/article-142674.

European Commission. (2003). *Proposal for a Council regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas and amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals, COM (2003) 558 Final, 24. Brussels*. Pridobljeno 25.3.2010 na http://www.statewatch.org/news/2003/sep/combiometrics.pdf

European Union Committee. (2006). *House of Lords, 30th Report of the 2005-2006 Session, European Arrest Warrant -Recent Developments, pp. 10-12*. Pridobljeno 27.5.2011 na http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/156/156.pdf

Evropska komisija. (2007). *Konvencija o kibernetskem kriminalu*. Pridobljeno 27.3.2011 na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:SL:HTML

Evropska komisija. (2010). *Sporočilo komisije Evropskemu parlamentu in svetu: Politika za EU za boj proti terorizmu: Glavni dosežki in izzivi prihodnosti*. Pridobljeno 27.4.2011 na http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0386_/com_com(2010)0386_sl.pdf

Financial Action Task Force. (2009). *Money Laundering and Terrorist Financing in the Securities Sector*. Pridobljeno 4.11.2010 na http://www.fatf-gafi.org/dataoecd/32/31/43948586.pdf

Financal Transaction and Reports Analysis Centre of Canada (2011*). Money Loundering and Terorist activity Financing Watch*. Pridobljeno 14.9.2011 na http://www.fintrac-canafe.gc.ca/publications/watch-regard/2011-06-eng.pdf

Fischhoff, B., Gonzalez, R. M., Lerner, J. S. in Small, D. A. (2005). Evolving judgments of terrorrisks: Foresight, hindsight, and emotion. *Journal of Experimental Psychology, 11,* 124–139.

Fishbein, M. in Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, Mass*. Ontario: Addison-Wesley Pub. Co.

Fitzpatrick, T. (2002). Critical theory, information society and surveillance tehnologies, *Information, Communication & Society, 5*(3), 357–378.

Freeman, E. H. (2007). When Technology and Privacy Collide. V M. Krause in H. F Tipton (ur.), Handbook of Information Security Management (str. 213-256). Boca Raton: Aurbach Publication.

Fossati, M. (2005). *Terorizem in teroristi*. Ljubljana: Založba Sophia.

Galley, P. (1996). *Computer terrorism: What are the risks?* Pridobljeno 14.9.2011 na http://www.stealth-iss.com/documents/pdf/compterrorism.pdf

Gamage, P. (2010). *Media, Terrorism and Insurgency in South Asia*. Pridobljeno 25.11.2010 na http://www.upsam.upeace.org/pdf/Curricula/Gamage/Media%20Terrorism%20and%20Insurgency%20in%20South%20Asia.pdf

Gams, M. (2001). Weak Intelligence: Through the principle and paradox of multiple knowledge. New York: Nova Science Publishers.

Gates, K. A. (2004). *Our biometric future: The social construction of an emerging information technology*. New York: New York University Press.

Glaser, A. In Hippel, F. N. (2006). *Thwarting nuclear terrorism*. Pridobljeno 14.3.2011 na http://www.bnl.gov/nns/news/SciAm0206Fishbone.pdf

Glüpker, G. (2009). *Media and Terrorism*. Istanbul: GRIN Verlag.

Goles, T., White, G. B., Beebe, N., Dorantes, C. A. in Hewitt, B. (2006). Moral Intensity and Ethical Decision-Making: A Contextual Extension. *The Data Base for Advances in Information Systems, 37,* 2-3.

Golob, J. (2005). *Vrednotenje kakovosti spletnih predstavitev izbranih Slovenskih in tujih spletnih knjigarn*. Pridobljeno 04.11.2011 na: http://www.cek.ef.uni-lj.si/u_diplome/golob1813.pdf

Gorman, C. (2011). *How Biometrics Helped to Identify the Master Terorrism*. Pridobljeno 04.11.2011 na: http://www.scientificamerican.com/article.cfm?id=how-biometrics-helped-to-identify-master-terrorist

Grabosky, P. in Stohl, M. (2010). *Crime and Terrorism*. London: SAGE Publications.

Gurr, T. R. (1968). Psychological factors in civil violence. *World Politics, 20,* 245-278.

Hallett, T. (2004). *Give Me Some Skin: Biometrics Get Thumbs Up*. Pridobljeno 15.4.2010 na http://www.silicon.com/technology/security/2004/01/06/give-me-some-skin-biometrics-get-thumbs-up-39117626/

Haines, R. in Leonard, L. N. K. (2007). Individual Characteristics and Ethical Decision-Making in an IT Context. *Industrial Management and Data, 107*(1), 5-20.

Henry, J. W. in Pierce, M. A. (1994). Computer Ethics: A Model of Influences on the Individual's Ethical Decision Making. *Computer Personnel, 15 (3),* 21-27.

Hernández-Ortega, B., Jiménez-Martínez, J. in Martín-De Hoyos, M.(2008). B2C e-commerce acceptance: The moderating effect of gender. *Communications of the IBIMA, 6*(16), 104-112.

Hocquet, S., Ramel, J. in Cardot, H. (2005). Fusion of Methods for Keystroke Dynamic Authentication. *4th IEEE Workshop on Automatic Identification Advanced Technologies 5,* 224–229.

Hovsto, A. (2008). *Critical factors of biometrics in eHealth: BioHealth findings.* Pridobljeno 5.11.2010 na http://www.hideproject.org/downloads/HIDE_FG-System_Interoperability-Presentation_Asbjorn_Hovsto_FG1-20080915.pdf

Hu, V., Ferrailo, D. in Kuhn, D. R. (2006). Assesment of *Access Control Systems.* Pridobljeno 17.11.2010 na http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Hutter, R. (2002). *Cyber Terror-eine realistische Gefahr?.* Pridobljeno 16.9.2010 na http://www.aksis.de/Cyber-Terror.pdf

Huges, G.(1998). *Understanding Crime Prevention: Social Control, Risk and Late Modernity.* Buckingam: Open University Press.

Hustinx, P. (2006). *Comments on the Communication of the Commission on interoperability of European databases.* Pridobljeno 12.3.2011 na http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

Identity Theft Protection Resource Center. (2011). *Identitiy Theft and Terrorism.* Pridobljeno 14.8.2011 na http://bestidentityprotection.net/identity-theft-and-terrorism/

Informacijski pooblaščenec Republike Slovenije. (2010). *Prijava biometrijskih ukrepov informacijskemu pooblaščencu.* Pridobljeno 7.11.2011 na http://www.ip-rs.si/fileadmin/user_upload/doc/obrazci

Information Telecommunication Union. (2009). *Technology Watch Reports: Biometrics and Standards.* Pridobljeno 24.10.2011 na www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002MSWE.doc

Information Warfare Site. (2011). *The cost of cyber crime: Full report.* Pridobljeno 15.8.2011 na http://www.iwar.org.uk/ecoespionage/resources/cost-of-cybercrime/index.htm

Institute for Safety Security and Crisis Management. (2008). *Terrorism and the Media.* Pridobljeno 12.5.2011 na

http://www.transnationalterrorism.eu/tekst/publications/WP4%20Del%206.pdf

International Biometric Group. (2008). *Biometrics Market and Industry Report 2009-2014*. Pridobljeno 7.11.2010 na http://www.biometricgroup.com/reports/public/market_report.php

International Biometric Group. (2009). *Biometric Revenues by Technology. Biometrics Market and Industry Report 2009-2014*. Pridobljeno 12.5.2010 na http://www.biometricgroup.com/reports/public/market_report.php

Internet Crime Compliant Center. (2006). *Internet Fraud Crime Report*. Pridobljeno 23.11.2010 na http://www.ic3.gov/media/annualreport/2006_ic3report.pdf

Internet Crime Complaint Center. (2011). *Data, Tools, and Resources for Enforcement Professionals*. Pridobljeno 24.9.2011 na http://www.ic3.gov/default.aspx

Isserof, A. (2006). *Zionism and Israel - Encyclopedic Distionary (Hezbollah, Hizballah, Hizbullah, Hizbu Allah, Hezbullah Definition)*. Pridobljeno 20. 10. 2011 na http://www.zionism-israel.com/dic/Hezbollah.htm.

Jain, A. K., Ross, A. in Prabhakar, S. (2004). *An Introduction to Biometric Recognition*. Pridobljeno 17.11.2010 na http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf

Jain, A. K. (2010). *Avtomatic Face Recognition: State of the Art*. Pridobljeno 17.3.2011 na http://biometrics.cse.msu.edu/Presentations/AnilJain_FaceRecognition_KU10.pdf

Jain, A. K., Bolle, R. in Pankanti, S. (2002). *Biometrics: Personal Identification in Networked Society*. Norwell: Kluwer Academic Publishers.

Janczewski, L. in Colarik, A. M. (2005). *Managerial guide for handling cyber-terrorism and information warfare*. Hershey PA: Idea Group Publishing.

Jereb, E. in Šmitek, B. (2006). Applying multimedia instruction in e-learning. *Innovations in educations and teaching international*, 2006, 43(1), 15-27.

Johnson, N. F. (1995). *Steganography*: *Technical Report*. Pridobljeno 22.4.2011 na http://www.jjtc.com/pub/tr_95_11_nfj/sec202.html

Johnson, N. F. in Jajodia, S. (1998). *Explooring Steganography; Seeing the Unseen*. Pridobljeno 7.11.2010 na http://www.jjtc.com/pub/r2026.pdf

Johnson, N. F (2011). *Steganography ans Digital Watermarking in Tool Table*. Pridobljeno 22.4.2010 na http://www.jjtc.com/Steganography/tools.html

Joint Research Centre. (2005). *Biometrics at the Frontiers: Assessing the Impact on Society, Technical Report Series*. Pridobljeno 12.1.2011 na http://ftp.jrc.es/EURdoc/eur21585en.pdf

Kahn, D. (1967). *The Codebreakers*. New York: Macmillan.

Kaos.theory. (2011). Anonym.os live CD. Pridobljeno 04.09.2011 na: http://sourceforge.net/projects/anonym-os/files/

Kapczyński, A. (2006). *Relationship between IT Security and users' needs*. Pridobljeno 7.3.2011 na http://www.proceedings2006.imcsit.org/pliks/166.pdf

Kazenski zakonik RS. (2008). *Uradni list RS št. 55/2008*, str. 5865. Pridobljeno 27.4.2011 na http://www.uradni-list.si/1/objava.jsp?urlurid=20082296

Kaye, B. H. (1995). Science and the detective: Selected reading in forensic science. New York: VCH.

Kendry, A. (2007). Denar kot vir zla- ekonomija mednarodnega terorizma. Nato Review. Pridobljeno 4.11.2011 na http://www.nato.int/docu/review/2007/issue2/slovene/analysis2.html

Kimmage, D. *(2008). The Al-Qaeda media nexus.The virtual network behind the global message*. Pridobljeno 17.10.2010 na http://docs.rferl.org/en-US/AQ_Media_Nexus.pdf

Kirkpatrick, M. (2001). *How New Technologies (Biometrics) Can Be Used To Prevent Terrorism*. Pridobljeno 12.11.2011 na: http://www.fbi.gov/congress/congress01/kp111401.htm

Knil, E. (2010). Quantum computing. *Nature, 463(28)*. Pridobljeno 17.3.2011 na http://www.nist.gov/cgi-bin//get_pdf.cgi?pub_id=902941

Kobeja, B. (2002). *Napotki za pisanje seminarske in diplomske naloge*. Koper: Visoka šola za management.

Kodelja, M. in Banovič, Z. (2008). Zakrivanje spletnih sledi. *Moj mikro*. Pridobljeno 17.3.2011 http://www.mojmikro.si/preziveti/varnost/zakrivanje_spletnih_sledi

Komarinski, P (2005). *Automated fingerprint identification systems (AFIS)*. Burlington: Academic Press.

Korošec, D. (2002). Terorizem kot izziv za (materialno) kazensko pravo. V M. Pavčnik (ur.), *Zbornik znanstvenih razprav, let. LXII, 97-128* (str. 97-128). Ljubljana; Pravna fakulteta.

Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Znanstvena knjižnica.

Kovačič, M. (2007). Intervju. *Mladina*. Pridobljeno 12.10.2011 na http://www.mladina.si/dnevnik/13-07-2007-intervju/

Krasavin, S. (2004). *What is Cyberterrorism?*. Pridobljeno 3.11.2010 na http://www.crime-research.org/analytics/Krasavin/

Krause, M. in Tipton, H. F. (2004). *Handbook of Information Security Management*. Boca Raton: CRC Press LLC.

Kučič, L. (8.4.2002). Intervju z Jurijem Kebetom: Prestopniška domišljija ne pozna računalniških meja. *Delo,* str. 7.

Kukula, E. in Proctor, R. (2009). Human-Biometric Sensor Interaction: Impact of Training on Biometric System and User Performance. V M. Smith in G. Salvendy (ur.), *Human Interface and the Management of Information* (str. 168–177). Heidelberg: Springer Berlin.

Kumar-Singh, N. (2009). *Transnational Cyber Crime and Terrorism*. New Delhi: Publications Pvt. Ltd.

Kunreuther, H., Michel-Kerjan, E. in Porter, B. (2003). *Assessing, managing and financing extreme events: Dealing with terrorism: Working Paper 10179*. Cambridge: National Bureau of Economic Research.

Lah, P. (2003). *PGP (Pretty Good Privacy)*. Pridobljeno 4.11.2010 na http://www.si-ca.si/kripto/kr-pgp.htm

Lemyre, L., Turner, M. C., Lee, J. C. in Krewski, D. (2006). *Public Perception of Terrorism Threats and Related Information Sources in Canada: Implications for the management of terrorism risks. Journal of Risk Research, 9*(7). Pridobljeno 7.11.2010 na http://www.gapsante.uottawa.ca/English/Articles/34_Lemyre,Turneretal.Public%20Perception%20of%20Terrorism_2006.pdf

Lemyre, L., Clement, M. in Gibson, S. (2004). Summary report on the focus groups held with members of the public on the psychosocial aspects of CBRN terrorism. University of Ottawa in partnership with Health Canada and the Canadian Food Inspection Agency. *Journal of risk research, 9*(7), 23-67.

Lerner, J., Gonzalez, R., Small, D. in Fischhoff, B. (2003). Effects of fear and anger on perceived risks of terrorism: A national field experiment. *Psychological Science, 14,* 144–150.

Likar, M. (2005). *Biološka vojna*. Ljubljana: Ministrstvo za obrambo RS, Uprava RS za zaščito in reševanje, Ljubljana.

Liu, S. in Silverman, M. (2001). *A practical guide to Biometric Security Technology*. Pridobljeno 4.11.2010 na http://www.lfca.net/Reference%20Documents/A%20Practical%20Guide%20To%20Biometric%20Security%20Technology.pdf

Loch, K. D. in Conger, S. (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM, 39*(7), 74-83.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

Maier, F. G in Karageorghis, V. (1984). *Paphos: History and archaeology*. Nicosia: Laventis Fundation.

Malcolm, J. (2004). *Virtual threat, real terror. Cyber terorrism in 21st century. Testimony of the United States Senate Comittee on the Judiciary*. Pridobljeno 25.5.2011 na http://www.gpo.gov/fdsys/pkg/CHRG-108shrg94639/pdf/CHRG-108shrg94639.pdf

Malik, J. (2011). *Cyber crime and terrorism*. New Delhi: Swastik Publications.

Maver, D. (2004). *Kriminalistika: Uvod, taktika in tehnika*. Ljubljana: Uradni list Republike Slovenije.

Maynes Charles, W. (2004). All Political Violence is Not Terrorism. V L. K. Legendorf (ur.), *Terorrism Opposing Viewpoints* (str. 213-255). San Diego: Greenhaven Press.

Mcknight, D. H. in Chervany, N. L. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce, 6*(2), 35-59.

Meško, G. (2000). Pogledi na preprečevanje kriminalitete v pozno modernih družbah. *Teorija in praksa, 37*(4), 716-727.

Meško, G. in Dobovšek, B. (2007). Merjenje organizirane kriminalitete - omejitve in izzivi. V I. Prezelj (ur.), *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*. Ljubljana: Ministrstvo za obrambo (str. 103-124). Direktorat za obrambne zadeve.

Milkovič, J. in Justin M. (2004). Kibernetske subkulture. Ljubljana: Fakulteta za družbene vede.

Ministrstvo za notranje zadeve. (2008). *Varni na internetu*. Pridobljeno 4.11.2011 na https://docs.google.com/viewer?url=http://www.policija.si/images/stories/Publikacije/PDF/varniNaInternetu.pdf

Ministrstvo za zunanje zadeve. (2011). *Boj proti terorizmu*. Pridobljeno 4.3.2011 na http://www.mzz.gov.si/si/zunanja_politika/mednarodna_varnost/boj_proti_terorizmu/

Ministrstvo za zaunanje zadeve. (1966). *Najpomemnejši mednarodnopravni dokument s področja človekovih pravic*. Pridobljeno 24.4.2011 na http://www.mzz.gov.si/si/zunanja_politika/clovekove_pravice/najpomemnejsi_mednarodnopravni_dokumenti_s_podrocja_clovekovih_pravic/Miholič , A. (2004). *Logistične značilnosti sodobnih terorističnih skupin*. Diplomsko delo, Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.

Monsuwe, T. P., Perea, T., Dellaert, B. G. in Ruyter, K. D. (2004). What drives consumers to shop online? A literature review. *International Journal of Service Industry Management, 15*(1), 102–121.

Mordini E. in Petrini C. (2007). Ethical and social implications of biometric identification technology. *Ann Ist Super Sanita, 43*(1). Pridobljeno 25.5.2011 http://www.iss.it/binary/publ/cont/STAMPA%20ANN_07_02%20Mordini.1180428288.pdf

Moteff, J., Copeland, C. in Fischer, J.(2003). CRS *Report for Congress. Critical Infrastructures: What makes an Infrastructure Critical?*. Pridobljeno 7.11.2010 na http://www.fas.org/irp/crs/RL31556.pdf

Mraović, M. (2003). *Biometrične metode v sistemu pristopne kontrole*. Ljubljana: Fakulteta za elektrotehniko.

Muller, E. R., Spaaij, R. F. J. in Ruitenberg, A. G. W. (2003). *Trends in Terorrisem*. Alphen aan de Rijn: Kluwer.

Murrill, R. (2011). *The Question Of Cyber Terrorism*. Pridobljeno 4.9.2011 na http://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/

Müller- Wille, B. (2004). *For our eyes only? Shaping an intelligence community within EU. Occacional paper No.50*. Paris: Institute for security Study.

Nadel, L. (2006). On the Future of Biometrics–Research, Applications, and Social Challenges. V A. Fitzgibbon, C. J. Taaylor in Y. Lacun (ur.), *Computer Vision and Pattern Recognition. IEEE Computer Society conference* (str. 131-145). New York: Computer Society.

National Comission of Terorrist Attack. (2004). *9-11 Commission Report*. Pridobljeno 7.11.2010 na http://www.911commission.gov/report/911Report.pdf

National Consumers League. (1998). *Online Incident Report*. Pridobljeno 25.5.2011 na http://www.fraud.org/info/contactnfic.htm

National Science and Technology Council. (2006). *Federal Plan for Cyber Security and Information Assurance Research and Development*. Pridobljeno 7.10.2010 na http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

National Science and Technology Council. (2006). *Biometrics*. Pridobljeno 23.11.2010 na http://www.biometrics.gov/Documents/glossary.pdf

Nedog, J. (2002). Samomorilski napadi. *Obramba, 34*(3), str. 55-57.

Network Mapper. (2010). *SecLists.Org: Security Mailing List Archive*. Pridobljeno 15.3.2011 na http://seclists.org/

Olman, G. (2010). *Asymmetrical Warfare: Challenges and Strategies for Countering Botnets*. Pridobljeno 04.03.2011 na http://www.damballa.com/downloads/r_pubs/ICIW_2010.pdf

Pahor, M. (2010). *Introduction to PASW (SPSS) workshop*. Ljubljana: Ekonomska fakulteta.

Patrick, A. S. (2004). Usability and acceptability of biometric security systems. NATO woorkshoop and Enhancing Informating System, Security through Biometrics. Ottawa: Institute for Information Technology.

Podbregar, I., Ivanuša, T. in Lipičnik, M. (2007). Razsežnosti gospodarskega vohunstva v 21. Stoletju-primer gospodarskega vohunstva s pomočjo trojanskega konja. V B. Lobnikar (ur.), *Zbornik povzetkov: 8 slovenski dnevi varstvoslovja: Varnost v sodobni družbi groženj in tveganj* (str.6). Ljubljana: Fakulteta za varnostne vede.

Podbregar, I. in Ivanuša, T. (2009). Avian influenza (AI) : the threat of pandemic is real if not inevitable: Who will protect the security/armed forces in case of such pandemic?. *International journal of emergency management*, *6*(2), 152-161.

Podbregar, I. in Ivanuša, T. (2010). Javni viri in analitika v obveščevalni dejavnosti. *Krim. kriminol.*, *61*(2), 191-198.

Podbregar, I., Pleteršek, M. in Ivanuša, T. (2010). *Preprečevanje pranja denarja in financiranja terorizma pri trgovanju s plemenitimi kovinami in dragimi kamni*. Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Podbregar, I. (2010). Obveščevalno-varnostna dejavnost in boj proti terorizmu. V G. R. Newman, R. V. Clarke, I. Podbregar in A. Sotlar (ur.). *Policijska dejavnost proti terorizmu: učbenik za vodilno osebje na policijskih postajah* (str.134-150). Ljubljana : Fakulteta za varnostne vede.

Pollitt, M. M. (1997). *Cyberterrorism - Fact or Fancy?*. Pridobljeno 15.10.2010 na http://www.cs.geor ge t own.edu/~denning/ infosec/pollitt.html

Poulsen, K. (2003). Slammer worm crashed Ohio nuke plant network. *Securtiy Focus*. Pridobljeno 04.11.2011 na http://www.securityfocus.com/news/6767

Prabhakar, S., Pankanti, S. in Jain, K. A. (2003). *Biometric Recognition: Security and Privacy Concerns*. Pridobljeno 23.11.2010 na http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf

Prezelj, I. (2006). Teroristično ogrožanje nacionalne in mednarodne varnosti. *Varstvoslovje*, *8*(1), 18-30.

Quigley, M. (2008). *Encyclopedia of information ethics and security*. Herhey: IGI Global.

Rapoport, D. C. (2001). *Inside terrorist organizations*. London: Routledge.

Rauchs G. in Koenig D. J. (2001). Europol. V D. J. Koenig in D. K. (ur.), *International police cooperation* (str. 43-62). New York: Lexington Books.

Raymond, E. S. (2001). *How to Become A Hacker*. Pridobljeno 10.05.2011 na http://www.catb.org/%7Eesr/faqs/hacker-howto.html#style

Reddy, R. (2006). Robotics and Intelligent Systems in Support of Society. *Intelligent Systems*, *21*(3), 24–31.

Resolucija Evropskega parlamenta o boju proti terorizmu P6TA(2007)0612. (2007). *Uradni list Evropske Unije*. Pridobljeno 27.3.2011 na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:323E:0349:0355:SL:PDF

Richard, D. (1997). *Biometric indentification: Acess Control Issues*. Pridobljeno 12.6.2011 na http://www.cccure.org/Documents/HISM/033-037.html#Heading3

Rogers, E. M. (1962). *Diffusion of Innovations*. New York: The Free Press.

Rubin, G. J., Brewin, C. R., Greenberg, N., Simpson, J. in Wessely, S. (2005). Psychological and behavioural reactions to the bombings in London on 7 July 2005: Cross sectional survey of a representative sample of Londoners. *British Medical Journal, 331,* 606.

Ryder, N. (2011). *Financial Crime in the 21st Century: Law and Policy*. Northampton: Edward Elgar Publishing.

Sanders, T. (2005). Rise of rent-a-cop: Private security in Canada. *Canadian Journal of Criminology and Criminal Justice*, *47*(1), 175-190.

Satzger, H. in Pohl, T. (2006). The German Constitutional Court and the European Arrest Warrant: Critical Signal from Karlsruhe. *Journal of International Criminal Justice, 4*(4), 686-701.

Saul, B. (2003). International Terrorism as a European Crime: The Policy Rationale for Criminalization. *European Journal of Crime, Criminal Law and Criminal Justice, 11,* 323.

Schiller, J. (2010). *Cyber Attacks & Protection*. Charleston: CreateSpace.

Schmidt, P. A. in Yongman, J. A. (2005). *Political terrorism*. London: Transaction Publisher.

Schmidt, H. (2004). *Testimony before the Judiciary Committee on Cyber Terorrism U.S. Senate*. Pridobljeno 7.11.2010 na http://kyl.senate.gov/legis_center/subdocs/022404_schmidt.pdf

Schmidt, M., Das, D., Kumar,V. in Bekkering, E. (2008). *A proposed study and analysis of user perceptions of biometric acceptance*. Pridobljeno 27.11.2010 na http://www.decisionsciences.org/Proceedings/DSI2008/docs/396-2784.pdf

Schmitz, W. (2003). *Analysis and Assessment for Critical Infrastructure Protection, Work Package 6, Deliverable D6.4, Version 1*. Brusel: Information Society Technology Programme.

Schuster, M. A., Stein, B. C., Jaycox, L. H., Collins, R. L., Marshall, G. N., Elliott, M. N., Zhou, A. J., Kanouse, D. E., Morrison, J. L. in Berry, S. H. (2001). A national survey of stress reactions after the September 11, 2001, terrorist attacks. *New England Journal of Medicine, 345,* 1507–1512.

Shahar, Y. (1997). *Information warfare. International Policy Institute for Counter-Terrorism*. Pridobljeno 3.11.2010 na http://www.iwar.org.uk/cyberterror/resources/CIT.htm

Shaw, M. (2003). *International Law, fifth edition*. Cambridge: University Press.

Shaw, T. R. (2003). The Moral Intensity of Privacy: An Empirical Study of Webmaster's Attitudes. *Journal of Business Ethics, 46,* 301-318.

Siegel, L. J. (2010). *Criminology: Theories, patterens and typologies*. Belmont: Cengage Learning.

Skoudis, E. in Zeltser, L. (2003). *Malware: Fighting Malicious Code*. New Jersey: Prentice Hall PTR.

Slovic, P. (2002). Terrorism as a hazard: A new species of trouble. *Risk Analysis, 22,* 425–426.

Smith, A. D. (2008). Biometrics-based service marketing issues: Exploring acceptability and risk factors of iris scans associated with registered travel programmes. *International Journal of Electronic Healthc, 4*(1), 43-66.

Sotlar, A. (2010). Nekaj razmišljanj o (policijskem) zaznavanju teroristične grožnje v Sloveniji. V G. R. Newman, R. V. Clarke, I. Podbregar in A. Sotlar (ur.). *Policijska dejavnost proti terorizmu: učbenik za vodilno osebje na policijskih postajah* (str.134-150). Ljubljana : Fakulteta za varnostne vede.

Suler, J. (1996). *The Psychology of Cyberspace*. Pridobljeno 15.10.2010 na http://www.rider.edu/~suler/psycyber/psycyber.html

Sulivan, B. (2004). *9/11 report light on ID theft issues; Scant mention raises civil liberties concern*. Pridobljeno 15.3.2011 na http://www.msnbc.msn.com/id/5594385/ns/us_news-security/t/report-light-id-theft-issues/

Svete, U. (2005). *Informacijske razsežnosti sodobnega terorizma — teoretična vprašanja in praktični vidiki*. Pridobljeno 18.3.2011 na http://www.sos112.si/slo/tdocs/ujma/2007/124.pdf

Statistični urad Republike Slovenije. (2011). *Slovenija v številkah*. Pridobljeno 22.11.2011 na http://www.stat.si/doc/pub/slo_stevilke_11.pdf

Šemrov, D., Kotnik, T. in Miklavčič, D. (1996). Modeliranje bioloških in kemijskih sistemov s celičnimi avtomati. *Elektrotehniški Vestnik*, *63*(4/5). Pridobljeno 3.10.2010 na http://lbk.fe.uni-lj.si/pdfs/ev1996ds.pdf

Terrorism Act. (2000). *Prevention and suprression of terorrism*. Pridobljeno 27.3.2011 na http://www.homeoffice.gov.uk/publications/counter-terrorism/terrorism-act-remedial-order/terrorism-act-remedial-order?view=Binary

Thalheim, L., Krissler, J. in Ziegler, P. M. (2002). *Bodycheck: Biometric Access Protection: Devices and Their Programs Put to the Test*. Pridobljeno 12.4.2011 na http://www.heise.de/ct/english/02/11/114/

The American Heritage Dictionary of the English Language, Fourth Edition. (2000). Boston: Houghton Mifflin Company.

Thomas, T. (2003). *Al Qaeda and the Internet: The Danger of Cyberplanning, Parameters*. Pridobljeno 5.11.2010 na http://carlistewww.army.mil/usawc/Parameters/03spring/

Tičar, B. (2010). Ureditev preprečevanja terorizma v pravnem redu Republike Slovenije. V G. R. Newman, R. V. Clarke, I. Podbregar in A. Sotlar (ur.).

Policijska dejavnost proti terorizmu: učbenik za vodilno osebje na policijskih postajah (str.15-25). Ljubljana : Fakulteta za varnostne vede.

Tillema, H. K. (2010). A Brief Theory of Terrorism and Technology. V T. K. Ghosh, M. A. Prelas, D. S. Wisvanath in S. K. Loyalka (ur.), *Science and technology of terrorism and counterterrorism* (str. 1-13). New York: Marcel Dekker.

Toš, N. (1988). *Metode družboslovnega raziskovanja*. Ljubljana: Državna založba Slovenije.

Trast International. (2010). *Identifikacijski sistemi*. Pridobljeno 7.11.2010 na http://www.trast-int.si/IDS.html

Trapečar, M. in Robek, A. (2003). Sodobne biometrične metode pri verifikaciji identitet posameznikov ter njihova uporabnost v letalskem prometnem sistemu, *Varstvoslovje, 5*(1), 49–56.

Treaty an European Union TEU. (1992). Maastricht. *Official Journal, 191.* Pridobljeno 28.8.2010 na http://eur-lex.europa.eu/en/treaties/dat/11992M/htm/11992M.html#0001000001

Troosters, R. (2004). *The European Union Framework Decision of 13th June 2002 on Combating Terrorism, in ICLN (International Criminal Law Network, The Hague) and EULEC (European Institute for Freedom, Security and Justice, Brussels), joint Co-operation, European Co-operation Against Terrorism*. Nijmegen: Wolf Legal Publishers.

Uludag, U. in Jain, A. K. (2003). Hiding in biometric data. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 25*(11), 1494-1498).

United States Space Command. (2002). *Biochip Implant: Hi-Tech/Top Secret Project*. Pridobljeno 12.05.2011 na http://www.bibliotecapleyades.net/ciencia/secret_projects/implants.htm

United States Congress Office of Technology Assesment. (1991). *The FBI Fingerprint Identification Automation Program: Issues and Options.* Pridobljeno 5.9.2011 na http://www.fas.org/ota/reports/9141.pdf

United Nations. (2006). *Resolution adopted by the General Assembly*. Pridobljeno 17.4.2011 na http://www.unodc.org/pdf/terrorism/Index/60-288en.pdf

United Nations Office on Drugs and Crime. (2011). *Action against Terorrism: Ressolution*. Pridobljeno 27.3.2011 na https://www.unodc.org/tldb/en/action_sc_ga.html

Uredba Sveta (ES) št. 2252. (2004). *Uradni list RS št. 385*, str. 1–6.

Vacca, J. R. (2003). *Identity theft*. New York: Prentice Hall.

Vacca, J. R. (2007). *Practical Internet security*. New York: Springer.

Venkatesh, V., Morris, M., Davis, G. in Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Villiers, M. (2006). Distributed Denial of Service: Law, Technology & Policy. *World Jurist Law/Technology Journal, 39* (3). Pridobljeno 23.10.2010 na http://www.austlii.edu.au/au/journals/UNSWLRS/2007/3.html

Wang, Y., Wang, Y., Lin, H. in Tang, T. (2003). Determinants of user acceptance of internet banking: An empirical study. *International Journal of Service Industry Management, 14*(5), 501-519.

Weinberg, L., Pedahzur, A. in Perliger, A. (2003). Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists. *Deviant Behavior*, *24*(4) 405-423.

Westin, A. (2002). Biometrics in the Main Stream: What Does the U.S. Public Think, *Privacy and American Business Newsletter*, *9,* 8.

Wilkinson, P. (2005). International Terrorism: The Changing Threat and the EU's Response. *Institute for Security Studies Chaillot Paper, 84,* 29-31.

Woodward, J. D., Horn C., Gatune, J. in Thomas, A. (2003a). *Biometrics: A Look at Facial Recognition, Rand Documented Briefing prepared for the Virginia State Crime Commission*. Arlington: RAND Public safety and Justice.

Woodward, J. D., Orlans, N. M. in Higgins, P. T. (2003b). *Biometrics*. New York: McGraw–Hill.

Walsh, R. (2010). Cyberterrorism Trends Analysis. *Perspectives on Global Issues, 5*(1). Pridobljeno 15.12.2010 na http://www.perspectivesonglobalissues.com/archives/current/

Weimann, G. (2005). *Cyberterrorismus ist einegroße, schwarze Wolke am Horizont*. Pridobljeno 27.11.2010 na

http://www.sicherheitheute.de/index.php?cccpage=readtechnik&set_z_artikel=200

Willson, C. (2005). *CRS Report for Congress. Computer Attack and Cyberterorrisem. Vulnerabilities and Policy Issues for Congress.* Pridobljeno 7.11.2010 na http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf

Willson, C. (2008). CRS Report for Congress. *Bontnets, Cybercrime, and Cyberterorrism: Vulnerabilities and Policy Issues for Congress.* Pridobljeno 7.11.2010 na http://www.fas.org/sgp/crs/terror/RL32114.pdf

Woodward, J. D., Webb, K. W., Newton, E. M., Bradley, M in Rubenson, D. (2001). *Army biometric applications: Identifying and addressing sociocultural concerns.* Pridobljeno 14.11.2010 na http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1237.pdf

Zachary, A. (2003). *Funding Terrorism in Southeast Asia: The Financial Network of Al Qaeda and Jemaah Islamiyah.* Pridobljeno 7.11.2010 na www.nbr.org/publications/analysis/pdf/vol14no5.pdf

Zakon o varstvu osebnih podatkov. (2007). *Uradni list RS, št. 94/2007,* str. 12707. Pridobljeno 27.5.2011 na http://www.uradni-list.si/1/objava.jsp?urlid=200486&stevilka=3836

PRILOGE

Vprašalnik

Opomba: spodnje besedilo je izvoženo iz spletne različice vprašalnika, ki je bil ob izvedbi ustrezno oblikovan in sprogramiran (preskoki, ipd.) – dostopen je bil na http://fluidsurveys.si/s/identifikacija/ – zaprt z geslom: biometrija. Dodane opombe in razlage v tem dokumentu so označene s krepkim in ležečim tekstom.

Anketa o identifikacijskih tehnologijah

Spoštovani!
Pred vami je anketa o identifikacijskih tehnologijah. Anketa je anonimna. Prosimo, da jo izpolnite v celoti. Izpolnjevanje ankete traja približno 10 minut. Pri vsakem vprašanju označite eno ali več možnosti, v skladu z navodili za posamezno vprašanje. »Pravilni« ali »napačni« odgovori ne obstajajo. Zanima nas vaše mnenje. Za Vašo prizadevnost in sodelovanje se Vam iskreno zahvaljujemo.

Sistemi preverjanja dostopa.
Katerega izmed spodaj naštetih načinov preverjanja dostopa najbolj pogosto uporabljate v vsakodnevnem življenju?

- ○ Kartični sistem (npr. registracija s kartico pri vstopu na delovno mesto, vstop v hotelsko sobo)
- ○ Klasični ključi (npr. vsakokratna uporaba ključev za odpiranje vrat)
- ○ Biometrični sistemi (npr. prepoznava prstnega odtisa – položimo prst na čitalec)
- ○ Varnostniki (npr. pregled in registracija pri varnostniku pred vstopom v parlament)
- ○ Drugo, prosimo vpišite: _____

Zanimajo nas vaše izkušnje z identifikacijskimi sistemi (kartični sistemi, biometrični sistemi, varnostniki itd.).

Naštete so različne situacije, pri katerih se uporabljajo tehnologije za identificiranje. Gre za primere, kjer je potrebno potrditi istovetnost uporabnika oz. se legitimirati. Izberite situacije, pri katerih ste se že srečali z identifikacijo. Možnih je več odgovorov.

- ☐ Registracija delovnega časa zaposlenih.
- ☐ Preverjanje identitete zaposlenih pred vstopom v zavarovan arhiv ali kakšno drugo zavarovano delovno območje.
- ☐ Preverjanje identitete pred vstopom na letalo.
- ☐ Preverjanje identitete potnikov pri vstopu v tujo državo.
- ☐ Preverjanje identitete obiskovalcev podjetji, javnih ali vladnih ustanov.
- ☐ Preverjanje identitete obiskovalcev podjetji, javnih ali vladnih ustanov pri vstopu na območje označeno z znakom SAMO ZA ZAPOSLENE.

Postavili vam bomo nekaj vprašanj o biometričnih tehnologijah za identifikacijo in vaših izkušnjah z njimi.

Poznamo različne biometrične tehnologije, ki se uporabljajo v procesih identifikacije. Prosimo, seznanite se z glavnimi tehnologijami, ki se pri nas uporabljajo. Gre za prepoznavo:

- prstnega odtisa (položimo prst na čitalec),
- oblike roke (geometrije členkov in prstov), ki jo izvedemo z odčitalno ploščo,
- podpisa,
- ožilja roke (vzorca žil v roki), ki jo izvedemo tako, da damo roko pod čitalec,
- obraza s pomočjo kamere,
- značilnosti šarenice s pogledom v skener,
- DNK: analiza vzorca krvi, las itd.,
- glasu.

S katerimi izmed naštetih biometričnih sistemov, ki se uporabljajo za identifikacijo, ste seznanjeni?

S pomočjo 5-stopenjske lestvice (1 – sploh nisem seznanjen/a, 5 – zelo dobro seznanjen/a) ocenite vaše poznavanje biometričnih sistemov.O biometričnem sistemu za identifikacijo (sem):

	1 Sploh nisem seznanjen/a	2 Slabo seznanjen/a	3 Srednje	4 Dobro seznanjen/a	5 Zelo dobro seznanjen/a
Prepoznava prstnega odtisa (položimo prst na čitalec).	○	○	○	○	○
Prepoznava oblike roke (geometrija členkov in prstov), ki jo izvedemo z odčitalno ploščo.	○	○	○	○	○
Prepoznava podpisa.	○	○	○	○	○
Prepoznava ožilja roke (vzorca žil v roki), ki jo izvedemo tako, da damo roko pod čitalec.	○	○	○	○	○
Prepoznava obraza s pomočjo kamere.	○	○	○	○	○
Prepoznava šarenice s pogledom v skener.	○	○	○	○	○

Prepoznava DNK: analiza vzorca krvi, las itd.	○	○	○	○	○
Prepoznava glasu.	○	○	○	○	○

Vaše izkušnje z biometričnimi sistemi v procesih identifikacije v preteklosti. Ali ste se že kdaj identificirali (legitimirali) s pomočjo biometrije?

○ Da

○ Ne

Dejali ste, da ste se v preteklosti že legitimirali s pomočjo biometrije. S katerimi izmed biometričnih sistemov ste imeli največ izkušenj v preteklosti?

○ Prepoznava prstnega odtisa (položimo prst na čitalec).

○ Prepoznava oblike roke (členkov in prstov), ki jo izvedemo z odčitalno ploščo.

○ Prepoznava podpisa.

○ Prepoznava ožilja roke (vzorca žil v roki), ki jo izvedemo tako, da damo roko pod čitalec.

○ Prepoznava obraza s pomočjo kamere.

○ Prepoznava značilnosti šarenice s pogledom v skener.

○ Prepoznava DNK: analiza vzorca krvi, las, itd.

○ Prepoznava glasu.

Vprašanje se nanaša na prvo in drugo hipotezo.

Sprejemljivost biometričnih tehnologij

S pomočjo 5-stopenjske lestvice (1 – sploh se ne strinjam, 5 – popolnoma se strinjam) ocenite ali se s posamezno trditvijo strinjate ali ne.

	1	2	3	4	5
	Sploh se ne	Ne strinjam	Neodločen	Strinjam se	Popolnoma se strinjam

	strinjam	se			
Če se uporablja biometrična identifikacija, se mora okrepiti varstvo zasebnosti in pošteno ravnanje s podatki.	○	○	○	○	○
Organizacija, ki zbira biometrične podatke, mora uporabnike jasno obvestiti o potrebnosti in načinu zbiranja in obdelave podatkov.	○	○	○	○	○
Organizacije lahko biometrične podatke zbirajo zgolj na način, ki je bil uporabniku predhodno opisan.	○	○	○	○	○
Skrivno zbiranje biometričnih podatkov ni dovoljeno.	○	○	○	○	○
Biometričnih podatkov se ne sme povezovati z drugimi osebnimi podatki.	○	○	○	○	○
Zgoraj naštete trditve se lahko kršijo, če gre za interese državne varnosti.	○	○	○	○	○

Vprašanje se nanaša na prvo in drugo hipotezo.

Sprejemljivost uporabe biometrije pri identifikaciji (legitimiranju)

S pomočjo 5-stopenjske lestvice (1 – sploh ni sprejemljiva, 5 – zelo sprejemljiva) ocenite, ali se s posamezno trditvijo strinjate ali ne. Se vam zdi sprejemljiva uporaba biometričnih podatkov …

	1 Sploh ni sprejemljiva	2 Ni sprejemljiva	3 Neodločen	4 Sprejemljiva	5 Zelo sprejemljiva
Kot sredstvo za pomoč pri preprečevanju manjših kaznivih dejanj (manjša kraja, prometni	○	○	○	○	○

prekrški itd.).					
Kot sredstvo za pomoč pri preprečevanju težjih kaznivih dejanj (teroristični napadi, posilstva, umori itd.).	○	○	○	○	○
Pri preverjanju identitete kupca orožja v bazi pravnomočno obsojenih kriminalcev.	○	○	○	○	○
Za preverjanje identitete pri plačilu s kreditno kartico.	○	○	○	○	○
Pri dvigovanju denarja na bankomatu.	○	○	○	○	○
Pri dostopanju do zaupnih podatkov, kot so osebni zdravstveni podatki in podatki o financah.	○	○	○	○	○
Pri preverjanju preteklosti posameznika.	○	○	○	○	○

Vprašanje se nanaša na prvo in drugo hipotezo.

Pomislite na koristi, ki jih spodnji primeri prinašajo in zanemarite dejstvo ogrožanja zasebnosti. Se vam zdi sprejemljiva uporaba biometričnih podatkov …

1	2	3	4	5
Sploh ni sprejemljiva	Ni sprejemljiva	Neodločen	Sprejemljiva	Zelo sprejemljiva

Pri vpisu v šolo.	○	○	○	○	○
Pri kontroli potnih listov.	○	○	○	○	○

Vprašanje se nanaša na prvo in drugo hipotezo.

Pomislite na teroristične napade in njihovo preprečevanje. Se vam zdi sprejemljiva uporaba biometričnih podatkov za preverjanje identitete …

	1 Sploh ni sprejemljiva	2 Ni sprejemljiva	3 Neodločen	4 Sprejemljiva	5 Zelo sprejemljiva
V potnih listih.	○	○	○	○	○
Ob vstopu v državne stavbe.	○	○	○	○	○
Na letališčih pri prijavi na let.	○	○	○	○	○
Na vozniškem dovoljenju.	○	○	○	○	○
Pri izposoji avtomobila (rent a car).	○	○	○	○	○

Zaupanje v zbiranje biometričnih podatkov.

S pomočjo 5-stopenjske lestvice (1 – sploh ne zaupam, 5 – zelo zaupam) ocenite, koliko zaupate, da bodo na zgornje načine pridobljeni biometrični podatki res uporabljeni zgolj v protiteroristične namene in ne bo prišlo do njihovih zlorab. Če jih zbirajo:

	1 Sploh ne zaupam		Neodločen		5 Zelo zaupam
Državni organi	○	○	○	○	○
Privatne organizacije	○	○	○	○	○

Vprašanje je bilo oblikovano z namenom ugotoviti, ali imajo ljudje, ki veliko potujejo z letalom, drugačno percepcijo o biometriji kot ljudje, ki redko potujejo z letalom.

Smo že čez polovico ...

Preden nadaljujemo z naslednjim sklopom vprašanj, nas zanima, kako pogosto potujete z letali. Seštejte vse lete, ki ste jih opravili v zadnjem letu, vključno s transferji. S cifro vpišite število letov, ki ste jih opravili v zadnjem letu dni.

Vprašanje je bilo oblikovano z namenom ugotoviti pomembnost varnosti osebnih podatkov na splošno.

Vprašanje se nanaša na prvo hipotezo.

Varnost osebnih podatkov

Na 5-stopenjski lestvici (1 – sploh ni pomembna, 5 – zelo pomembna) ocenite pomembnost varnosti osebnih podatkov.Kako pomembna se vam na splošno zdi varnost osebnih podatkov?

1 Sploh ni pomembna				5 Zelo pomembna
○	○	○	○	○

Vprašanje je bilo oblikovano z namenom nadalje na praktičnih primerih ugotoviti pomembnost varnosti podatkov pri različnih načinih zbiranja.

Zbiranje osebnih podatkov

Na 5-stopenjski lestvici (1 – sploh ni pomembna, 5 – zelo pomembna) ocenite pomembnost varnosti osebnih podatkov. Kako pomembna se vam zdi varnost osebnih podatkov pri zbiranju podatkov ...

	1 Sploh ni pomembna			5 Zelo pomembna
Pri plačilu s plačilnimi karticami trgovcev (Pika, Magna, ipd.).	○	○	○	○

S karticami zvestobe (Mercator, Petrol, Spar, Tuš, ipd.).	○	○	○	○	○
Pri registraciji v spletne trgovine (mimovrste, enaa, eventim ipd.).	○	○	○	○	○
Pri naročanju telekomunikacijskih storitev (mobilna telefonija, stacionarna telefonija, internet).	○	○	○	○	○
S pomočjo zdravstvenih kartic in zdravstvenih kartonov.	○	○	○	○	○

Vprašanje se nanaša na prvo hipotezo.

Varnost osebnih podatkov

S pomočjo 5-stopenjske lestvice (1 – sploh ne podpiram, 5 – popolnoma podpiram) ocenite, ali podpirate posamezno trditev ali ne. Pomislite na koristi, ki jih spodnji primeri prinašajo in zanemarite dejstvo ogrožanja zasebnosti. Ali podpirate uporabo biometričnih podatkov ...

	1 Sploh ne podpiram	2 Ne podpiram	3 Neodločen	4 Podpiram	5 Popolnoma podpiram
Za varovanje zaupnih podatkov, ki jih pri svojem delu zbirajo kriminalisti in policija.	○	○	○	○	○
Pri kriminalističnem delu na mestih zločina, če se podatki zbrani na mestu zločina primerjajo z bazami podatkov pravnomočno obsojenih zločincev.	○	○	○	○	○
Za izdelavo baz s podatki o resnih kriminalcih in zločincih.	○	○	○	○	○
Pri delu prometne policije, če policist ustavi prometnega prekrškarja in hkrati primerja njegove podatke s podatki o obsojencih na	○	○	○	○	○

begu.

Vprašanje je bilo oblikovano z namenom ugotoviti ali anketirani povezujejo preprečevanje terorizma z biometrijo

Biometrični podatki in preprečevanje terorizma

Pomislite na teroristični napad, ki se je v ZDA zgodil 11. septembra 2001. S pomočjo 5-stopenjske lestvice (1 – sploh se ne strinjam, 5 – popolnoma se strinjam) ocenite, ali bi po vašem mnenju lahko s pomočjo mednarodne baze z biometričnimi podatki teroristov pripomogli k zmanjšanju terorističnih napadov?

1 Sploh se ne strinjam				5 Popolnoma se strinjam
○	○	○	○	○

Vprašanje se nanaša na tretjo hipotezo.

Vprašanje je bilo oblikovano z namenom ugotoviti kateri izmed sistemov se zdi anketiranim učinkovitejši.

Ocenite vašo izkušnjo z učinkovitostjo (hitrost identificiranja, reakcijski čas in enostavnost uporabe) klasičnih (kartičnih) in biometričnih sistemov za preverjanje podatkov, ki jih najpogosteje uporabljate. Na 5-stopenjski lestvici (1 – slabo, 5 – odlično) ocenite vašo izkušnjo z učinkovitostjo sistemov ob preverjanju podatkov.

	1 Slaba učinkovitost			5 Odlična učinkovitost	Ne morem oceniti
Biometrični sistemi	○	○	○ ○	○	○
Klasični (kartični) sistemi	○	○	○ ○	○	○

Vprašanje se nanaša na tretjo hipotezo.

Vprašanje je bilo oblikovano z namenom ugotoviti kateri izmed sistemov se zdi anketiranim primernejši.

Primerjava klasičnih sistemov identifikacije (legitimiranja) in biometričnih sistemov.

Prosimo, primerjate vaše vedenje ali izkušnjo identifikacije s klasičnimi (kartičnimi) sistemi (npr. osebna izkaznica, identifikacijska kartica, identifikator itd.) in biometričnimi tehnologijami identifikacije. Kateri sistem se vam zdi primernejši?

- ○ Klasični (kartični) sistemi
- ○ Biometrične tehnologije

Zaupajte nam še nekaj demografskih podatkov.

Podatki bodo obravnavani zaupno.

Letnica rojstva (izberite vašo letnico rojstva)

- ○ 1900
- ○ 1901
- ○ 1902
- ○ 1903
- ○ 1904
- ○ 1905
- ○ 1906
- ○ 1907
- ○ 1908
- ○ 1909

... 90 - število skritih možnosti ...

- ○ 2001
- ○ 2002
- ○ 2003
- ○ 2004
- ○ 2005

- ○ 2006
- ○ 2007
- ○ 2008
- ○ 2009
- ○ 2010

Spol

- ○ Moški
- ○ Ženski

Vprašanje je bilo oblikovano z namenom povezovanja med rezultati in izobrazbo anketiranih.

Zadnja šola, ki ste jo končali redno ali izredno je ...

- ○ Nedokončana ali dokončana osnovna šola.
- ○ Dveletna ali triletna poklicna srednja šola.
- ○ Štiriletna ali petletna srednja šola.
- ○ Visokošolski ali univerzitetni študij.
- ○ Specializacija, magisterij, doktorat.

Vprašanje je bilo oblikovano z namenom povezovanja med rezultati in zaposlitvenim statusom anketiranih.

Aktivnosti organizacije v kateri delam, najbolje opišem kot ...

- ○ Razvoj, proizvodnja ali dobavitelj informacijske tehnologije.
- ○ Razvoj, proizvodnja ali dobavitelj varnostne tehnologije.
- ○ Ostale gospodarske družbe.
- ○ Javni sektor/uprava/šolstvo.

- ○ Ostalo.
- ○ Nisem zaposlen/a.

Vprašanje je bilo oblikovano z namenom povezovanja med rezultati in regijo v kateri živijo anketirani.

V kateri regiji živite?

- ○ Pomurska regija
- ○ Podravska regija
- ○ Koroška regija
- ○ Savinjska regija
- ○ Zasavska regija
- ○ Spodnjeposavska regija
- ○ Jugovzhodna Slovenija
- ○ Osrednjeslovenska regija
- ○ Gorenjska regija
- ○ Notranjsko - kraška regija
- ○ Goriška regija
- ○ Obalno - kraška regija

Vprašanje je bilo oblikovano z namenom povezovanja med rezultati in politično opredelitvijo anketiranih.

Politična opredelitev. V politiki se včasih govori o levici in desnici. Označite, kam bi vi uvrstili sami sebe.

Levica		Sredina		Desnica	Ne želim odgovoriti
○	○	○	○	○	○

Delovni življenjepis

Robert Brumnik roj. 17.06.1971 v Slovenj Gradcu, je l.1991 zaključil srednjo strojno tehnično šolo na Ravnah na Koroškem ter pridobil naziv, strojni tehnik. Študij je nadaljeval na Univerzi v Mariboru, ter zaključil univerzitetni program strojništva, smer konstruiranje in gradnja strojev. Kot študent, je spoznal razvojno-tehnološki proces avtomobilske industrije, v družbi Prevent d.d. ter Johnson Controls d.d. v Slovenj Gradcu, kjer se je l.1998 tudi redno zaposlil kot razvojni tehnolog. V l.1999, je službovanje nadaljeval v družbi Grammer Automotive d.d., kot tehnolog kakovsti in postal odgovoren za izvedbo presoj procesa, v skladu z evropskimi in ameriškimi standardi avtomobilske industrije. V okviru zagotavljanja kvalitete proizvodov v avtomobilski industriji, je spoznal standardizacijo ter postopke preverjanja skladnosti procesov, glade na standarde ISO9001:2000, QS9000, VDA, TS16694. Pridobil je znanja za planiranje procesov ter opravil izpit, za vodilnega presojevalca sistemov kakovosti, po ISO9001:2000. Leta 2000 se je zaposlil v družbi Metra inženiring d.o.o. v Trzinu na mestu vodje kakovosti ter se vključil v razvojno raziskovalno skupino, ki deluje v okviru družbe. Z aktivnim vključevanjem v izvedbo razvojno-raziskovalnih projektov, na temo identifikacijskih sistemov ter pristopne kontrole, je l. 2004 pridobil naziv samostojni razvijalec. V družbi je bil odgovoren za vzpostavitev in vzdrževanje sistema vodenja kakovosti ter za CE certificiranje proizvodov, po evropskih EC regulativah. Aktivno se udeležuje mednarodnih konferenc ter objavlja znanstvene članke, v mednarodnih revijah. Leta 2006 je v okviru reinženiringa podjetja, vodil projekt implementacije integralnega informacijskega sistema ter ga skupaj z sodelujočimi, uspešno zaključil l.2007. Njegova raziskovalna dejavnost, se navezuje na mednarodne razvojno raziskovalne projekte, katerih rezultat so mednarodno registrirani patenti. S prispevki se udeležuje mednarodnih znanstvenih konferenc, s področja informatike in informacijske varnosti.