

**UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE**

Marko Anžič

Mentor: doc. dr. Iztok Prezelj

VLOGA BIOMETRIČNIH METOD PRI PREPREČEVANJU TERORIZMA

Diplomsko delo

Ljubljana, 2005

IZJAVA O AVTORSTVU

KAZALO

SEZNAM KRATIC	V
1. UVOD	1
2. METODOLOŠKO HIPOTETIČNI OKVIR	3
2.1 OPREDELITEV PREDMETA IN CILJEV PREUČEVANJA	3
2.2 HIPOTEZE	4
2.3 METODOLOŠKI PRISTOP	4
3. TEMELJNI POJMI	4
3.1 BIOMETRIJA	5
3.2 BIOMETRIČNE METODE	7
3.3 TERORIZEM	12
3.4 PREPREČEVANJE TERORIZMA	15
4. ZGODOVINA UPORABE BIOMETRIČNIH METOD	17
5. VZROKI UPORABE BIOMETRIČNIH METOD	19
5.1 POVEČANJE VARNOSTI	20
5.2 POVEČANA PRIKLADNOST ZA UPORABNIKE	22
5.3 ZMANJŠANJE STROŠKOV	23
6. NAJPRIMERNEJŠE BIOMETRIČNE METODE ZA PREPREČEVANJE TERORIZMA	25
6.1 OBRAZNA PREPOZNAVA	26
6.1.1 Princip delovanja	26
6.1.2 Splošne značilnosti	29
6.2 PRSTNI ODTISI	31
6.2.1 Princip delovanja	32
6.2.2 Splošne značilnosti	34
6.3 PREPOZNAVA ŠARENICE	35
6.3.1 Princip delovanja	36
6.3.2 splošne značilnosti	36
6.4 MULTIMODALNE BIOMETRIČNE METODE	37
6.4.1 Princip delovanja	38

6.4.2 Splošne značilnosti.....	39
6.5 PRIMERJAVA BIOMETRIČNIH METOD PO DOLOČENIH KARAKTERISTIKAH.....	40
7. PODROČJA UPORABE BIOMETRIČNIH METOD.....	41
7.1 KONTROLA DOSTOPA.....	44
7.2 MEJNA VARNOST.....	47
7.3 NADZOR JAVNIH PROSTOROV	49
7.3.1 Prepoznavna človeške identitete na daljavo (<i>Human ID</i>)	50
7.3.2 XXXV finale ameriškega nogometa (<i>XXXV Super Bowl</i>) januarja 2001 ...	52
7.3.3 CCTV kamere v Veliki Britaniji.....	53
7.4 PREPREČEVANJE KRAJ IN ZLOUP RABE IDENTITETE	54
8. ANALIZA IZBRANIH PRIMEROV	55
8.1 SLOVENIJA	55
8.2 EVROPSKA UNIJA (EU).....	60
8.3 ZDRUŽENE DRŽAVE AMERIKE (ZDA)	63
8.3.1 <i>US-VISIT: Visitor and Immigrant Status Indicator Technology</i>	64
8.3.2 <i>INSPASS: INS Passenger Accelerated Service System</i>	68
8.3.3 <i>TWIC: Transportation Worker Identification Credential (Identifikacijska poverilnica za delavce na področju transporta)</i>	69
9. VPRAŠANJE ZASEBNOSTI PRI UVAJANJU BIOMETRIČNIH METOD.....	70
9.1 BIOMETRIČNE METODE KOT 'PODPORNIK, ZAVEZNIK OZ. PRIJATELJ' ZASEBNOSTI	74
9.2 BIOMETRIČNE METODE KOT 'SOVRAŽNIK OZ. NASPROTNIK' ZASEBNOSTI	74
9.3 VARNOSTNI IN DRUGI UKREPI, KI OMOGOČAJO VARNEJŠO UPORABO BIOMETRIČNIH METOD V RAZMERJU DO ZASEBNOSTI	77
9.4 ZAKON O VARSTVU OSEBNIH PODATKOV (ZVOP-1) V RS IN UPORABA BIOMETRIČNIH METOD	79
10. ZAKLJUČEK IN VERIFIKACIJA HIPOTEZ	82
SEZNAM SLIK, GRAFOV IN TABEL	87
11. SEZNAM VIROV.....	88

SEZNAM KRATIC

AFIS	Automated Fingerprint Identification System (Računalniški sistem za avtomatsko obdelavo prstnih odtisov)
CCTV	Close Circuit Television (Sistem za video nadzor in arhiviranje)
DARPA	The Defense Advanced Research Projects Agency (Centralna raziskovalna in razvojna organizacija ministrstva za obrambo ZDA)
DHS	Department of Homeland Security (Ministrstvo za domovinsko varnost)
EER	Equal Error Rate (Stopnja enake napake)
EU	Evropska unija
FAR	False Acceptance Rate (Delež napačnih odobritev)
FRR	False Rejection Rate (Delež napačnih zavrnitev)
FRVT	Face Recognition Vendor Test (Test ponudnikov obrazne prepoznavne)
Human ID	Human Identification at a Distance (Prepoznavanje človeške identitete na daljavo)
ICAO	International Civil Aviation Organization (Mednarodna organizacija za civilno letalstvo)
INSPASS	INS Passenger Accelerated Service System (Avtomatiziran sistem za hitrejši prehod meje registriranih potnikov)
TWIC	Transportation Worker Identification Credential (Identifikacijska poverilnica za delavce na področju transporta)
US-VISIT	United States Visitor and Immigrant Status Indicator Technology (Vstopno – izstopni program na mejah ZDA)
VWP	Visa Waiver Program (Program v katerega je vključenih 27 držav, ki za vstop v ZDA ne potrebujejo vizuma)
ZDA	Združene države Amerike

1. UVOD

Terorizem! Malokateri pojem ima v današnjem času tako izrazito negativno konotacijo kot prav terorizem, pa naj to velja za javnost ali za najvišje državne voditelje. Ob omembi terorizma spomin nehote uide na nadvse tragične dogodke v New Yorku, Madridu, Beslanu in drugod, če naštejemo le nekaj najodmevnejših v zadnjem obdobju. Predvsem dogodki 11. 9. 2001 so sprožili vrsto sprememb celo v svetovnem merilu. In nehote se dobi občutek, da nič več ne bo tako, kot je bilo. V imenu boja (vojne?) proti terorizmu se vodijo celo (klasične) vojne. Pojavljajo se zapisi o terorizmu kot 'velikem zlu sodobnega časa'. Boj proti terorizmu oz. preprečevanje le-tega pa je postal eden izmed prvih ciljev večine svetovnih voditeljev oz. vlad ter tudi mednarodnih organizacij, združenj idr. Ta cilj se poskuša uresničevati preko zelo različnih metod – od klasičnih, ki jih izvajajo organi pregona in obveščevalne službe ter tudi vojske na represiven način, do drugih manj represivnih, kot je preprečevanje vzrokov za pojav terorizma.

Predvsem v zadnjem času (po 11. 9. 2001) se pogosto omenja tudi biometrija oz. biometrične metode kot sredstvo za preprečevanje terorizma. Prav to je bistvo mojega diplomskega dela. Biometrija in biometrične metode se pogosto pojmujejo kot visoko tehnološke rešitve, ki so bile v preteklosti videne predvsem v znanstvenofantastičnih filmih in jih večina javnosti zelo slabo pozna. Drugače je ob omembi prstnih odtisov, katere večina ljudi pozna in ve kakšen je njihov namen. In ena od biometričnih metod so tudi prstni odtisi, ki jih že več kot stoletje uspešno uporabljajo organi pregona po celem svetu predvsem z namenom ugotovitve storilcev kaznivih dejanj. Obstaja pa še cela vrsta drugih biometričnih metod, ki so že razvite, se razvijajo ali pa so omenjene le kot možni koncept za v prihodnje. Ne glede na biometrično metodo pa je njihovo bistvo v tem, da prepoznajo človeka na podlagi njegovih značilnosti in so tako močno orodje za verifikacijo (ali sem jaz res tisti za katerega se predstavljam?) in identifikacijo (kdo sem jaz?) ljudi.

In kje (sedaj) nastopijo biometrične metode pri preprečevanju terorizma? Gre za večplasten sklop možnosti. Najpogosteje se biometrične metode v sklopu boja proti terorizmu uporabljajo kot način omogočanja oz. preprečevanja dostopa do sredstev, ki bi jih potrebovali teroristi (npr. skladišča orožja), ciljev, ki bi jih želeli poškodovati ali uničiti (npr. jedrske elektrarne) ter držav, v katerih bi želeli delovati. To se dosega

tako, da imajo do naštetega dostop le pooblašчени posamezniki ali le tisti, ki ne predstavljajo varnostnega tveganja. Pri tem imajo biometrične metode pasivno vlogo preprečevanja terorizma. Aktivnejša vloga biometričnih metod pri preprečevanju terorizma pa se izraža pri nadzorni funkciji, s katero se omogoča (oz. naj bi se omogočalo) prepoznavo ljudi (v tem primeru teroristov) na daljavo. Ob tem se v javnosti (tudi strokovni) sproža vrsta pomislekov in nasprotovanj, saj naj bi to vodilo k povečanemu ali celo vseobsegajočemu nadzoru države nad državljani.

Da bi ustrezno opisal način, na katerega biometrične metode (lahko) preprečujejo terorizem ter razjasnil dileme, ki se ob tem pojavljajo, bom v prvem vsebinskem poglavju razdelal temeljne pojme, ki so pri biometriji, biometričnih metodah in s tem povezanimi pojmi precej redko ustrezno in temeljito razdelani, pogosto pa se opredeljujejo enaki pojmi za drugačne realnosti in enake realnosti z drugačnimi pojmi. Drugo poglavje bo namenjeno zgodovinskemu pregledu oz. razvoju biometričnih metod, da se spozna, da biometrične metode niso prisotne 'od včeraj ali danes'. V tretjem poglavju nameravam razdelati vzroke za uvajanje biometričnih metod v uporabo s ciljem preprečevanja terorizma. Torej preprosto in konkretno zakaj se uvajajo biometrične metode? Četrto poglavje bo namenjeno biometričnim metodam, ki so najprimernejše za preprečevanje terorizma, saj niso vse biometrične metode v ta namen enako uporabne. Peto poglavje je namenjeno področjem uporabe biometričnih metod, torej kje se, zaradi v četrtem poglavju omenjenih vzrokov, le-te uporabljajo za preprečevanje terorizma. Šesto poglavje je namenjeno analizi izbranih primerov. Pri tem bom seveda opisal stanje v Sloveniji ter EU, katere enakopraven del smo sedaj in ima na tem področju na nas tudi velik vpliv, ter ZDA, kjer se biometričnim metodam s ciljem preprečevanja terorizma namenja daleč največ poudarka. V zadnjem (vsebinskem) poglavju bom osvetlil vprašanje zasebnosti, ki ga zastavlja uporaba biometričnih metod. Nedvomno gre tu za področje, ki ga bo potrebno ustrezno urediti, da bodo biometrične metode v prihodnosti s strani državljanov sprejete kot legitimna metoda preprečevanja terorizma.

2. METODOLOŠKO HIPOTETIČNI OKVIR

2.1 OPREDELITEV PREDMETA IN CILJEV PREUČEVANJA

Danes je preprečevanje terorizma eden poglavitnih ciljev mnogih držav po celem svetu. K temu so veliko prispevali dogodki enajstega septembra 2001 v ZDA in dogodki, ki so temu napadu sledili. 'Boj (vojna?) proti terorizmu' je tako postal osrednji problem. Ta 'boj' poteka na zelo veliko področjih in z ogromno različnimi sredstvi oz. metodami. Takšno sredstvo, ki je, predvsem po že omenjenem enajstem septembru, ogromno pridobilo na veljavi in širini uporabe, so tudi biometrične metode. Kljub velikemu optimizmu, ko naj bi biometrične metode pomenile celo 'srebrni metek' v preprečevanju terorizma, je bila in je realnost vseeno nekoliko drugačna. Strokovnjaki s tega področja so si praktično edini, da biometrične metode kljub vsemu lahko pomenijo pomemben košček mozaika v preprečevanju terorizma, vsekakor pa te metode niso edina in vsemogočna rešitev pri uresničevanju tega cilja. V nalogi bom poskušal osvetliti čim več zornih kotov povezave med preprečevanjem terorizma in biometričnimi metodami ter odgovoriti, na kakšen način imajo le-te lahko vpliv oz. dodano vrednost pri preprečevanju terorizma.

V nalogi sem si zastavil naslednje cilje:

- opredeliti biometrijo in biometrične metode ter s tem povezane pojme, ki so pomembni za celovito razumevanje tega področja;
- orisati zgodovinski razvoj na področju uporabe biometričnih metod;
- raziskati vzroke uporabe biometričnih metod;
- ugotoviti katere biometrične metode so najprimernejše za preprečevanje terorizma;
- opredeliti področja uporabe biometričnih metod s ciljem preprečevanja terorizma;
- analizirati izbrane primere uporabe biometričnih metod v Sloveniji, Evropski uniji in Združenih državah Amerike ter
- ugotoviti vpliv uvajanja biometričnih metod na zasebnost.

2.2 HIPOTEZE

1. Biometrične metode so bile za preprečevanje terorizma uporabljane že pred 11. 9. 2001.
2. Najprimernejša biometrična metoda za preprečevanje terorizma je obrazna prepoznavna.
3. Poglavitna 'dodana vrednost' biometričnih metod kot oblike preprečevanja terorizma je v njihovi zastraševalni oz. odvrtačevalni vlogi.
4. Pri uvajanju biometričnih metod s ciljem preprečevanja terorizma so najodločnejši akter ZDA, v EU in Sloveniji pa na tem področju še ni (bilo) dovolj storjenega.
5. Uvajanje biometričnih metod pomeni vdor v zasebnost posameznika.

2.3 METODOLOŠKI PRISTOP

V diplomskem delu bom uporabljal več različnih (predvsem neempiričnih) raziskovalnih metod.

Glavni del bo temeljil na analizi in interpretaciji sekundarnih virov. To raziskovalno metodo bom uporabil z namenom pridobitve čim več relevantnih informacij na področjih obravnave s strani kompetentnih avtorjev in bo prisotna skozi celotno delo. Deloma in v omejenem obsegu bom uporabil tudi analizo in interpretacijo primarnih virov, da bi dobil boljši pregled nad nekaterimi področji (npr. pri definiciji terorizma in vprašanju zasebnosti). Omejeno primerjalno metodo bom uporabil tudi pri primerjanju različnih biometričnih metod med seboj in stanju v državah na tem področju. Ponokod, kjer bo le-to potrebno, bom ostale raziskovalne metode dopolnil še s t.i. 'opisno (deskriptivno) metodo' in s tem zaokrožil obravnavano temo v celoto in predstavil tudi ozadja določenih pojavov.

3. TEMELJNI POJMI

Preden se lotim vsebinskih poglavij je potrebno opredeliti še temeljne pojme, ki bodo v mojem primeru biometrija in biometrične metode (znotraj teh dveh temeljnih pojmov bom opredelil še nekatere druge pojme, ki celovito zaokrožajo to področje in

bi bila, po mojem mnenju, brez tega predstavljena problematika necelovito zajeta) ter terorizem in preprečevanje terorizma.

3.1 BIOMETRIJA

Beseda biometrija (biometry) izhaja iz dveh grških besed bios (življenje) in metrikos (meriti) (Prabhakar et al, 2003: 33).

Glede na Slovenski medicinski slovar (2002: 97) je biometrija “/v/eda, ki uporablja merjenje in statistično analizo na vseh področjih biologije”, kot sinonim slovar uporablja izraz “biometrika”.¹

SSKJ (1994, 46) biometrijo preprosto opredeli kot “statistično proučevanje življenjskih pojavov, procesov”.

Medicinska enciklopedija (1980: 127) definira biometrijo tako: “Biometrija je veja biologije, ki uporablja matematične statistične metode za preučevanje bioptičnih pojavov. Z merjenji proučuje fizične in psihične lastnosti posameznika, njihovo spremenljivost zaradi okoliščin in tudi dednih vplivov. Uporablja tudi verjetnostni račun. V genetiki in medicini rabi za določanje splošnih lastnosti in meje med normalnim in patološkim stanjem enote”.

Bolj v kontekstu naloge je slednja opredelitev: “Biometrija je veda o uporabi edinstvenih fizioloških² značilnosti, s katerimi se lahko verificira³ identiteta posameznikov. Nanaša se na uporabo matematično-statističnih analiz bioloških karakteristik. Namen preiskovanja v biometriji, kot tudi drugih tovrstnih identifikacijskih postopkov, je torej najti individualnost znotraj splošnega. Vsak človek ima obraz, roke, prste. Raziskovanje teh splošnih človeških 'lastnosti' pa je pot k medsebojnemu ločevanju oseb” (Trapečar in Robek, 2003: 49).

Torej, če se oprem na zgornjo definicijo in odpravim (po mojem mnenju) nekatere pomanjkljivosti, bi se definicija biometrije, ki jo bom imel v mislih v diplomskem delu glasila: *Biometrija je veda o uporabi edinstvenih fizioloških in/ali edinstvenih vedenjskih značilnosti, s pomočjo katerih se prepoznava identiteta posameznikov. Nanaša se na uporabo matematično-statističnih analiz značilnosti.*

¹ V SSKJ ni najti besede biometrika, je le biometrija in tudi večinoma se uporablja beseda biometrija, čemur bom sledil tudi sam.

² Ter edinstvenih vedenjskih značilnosti (op. M.A.).

³ Ali identificira. V tuji literature se kot skupen izraz za verifikacijo (verification) in identifikacijo (identification) uporablja izraz prepoznavo (recognition).

Če sedaj na kratko analiziram ključne točke delovne definicije, gre najprej za *edinstvene fiziološke in/ali edinstvene vedenjske značilnosti*.

Fiziološke značilnosti temeljijo na meritvah in podatkih iz neposrednega merjenja in podatkih pridobljenih od delov človeškega telesa (How is Biometrics Defined?, 2005). Primeri fizioloških značilnosti, kar velja tudi za vedenjske značilnosti, morajo biti "specifične za vsakega posameznika, s časom nespremenljive oz. stabilne in merljive"⁴ (Fefer, 2004: 151). Primeri fizioloških značilnosti so npr.: prstni odtis, šarenica, mrežnica, obraz, roka idr.

Vedenjske značilnosti temeljijo na merjenju in podatkih pridobljenih iz nekih dejanj in podatkov ter posredno merijo značilnosti človeškega telesa. Ena od karakteristik, ki definirajo vedenjske značilnosti je vključenje časa kot merjenja – merjena vedenjska značilnost ima začetek, sredino in konec⁵ (How is Biometrics Defined?, 2005). Primeri vedenjskih značilnosti so npr.: podpis, glas, hoja, tipkovnični vnos idr.

Kljub navedeni klasifikaciji pa je povsem na mestu ugotovitev Maltonija in sodelavcev (2003: 2), da so verjetno vse biometrične značilnosti kombinacija fizioloških in vedenjskih značilnosti. Npr. pri prstnih odtisih je pomembno tudi to, kako je prst postavljen na čitalnik, pritisk idr. Še bolj značilno je to pri govoru, ki je rezultat fiziološke strukture in okolja, v katerem je oseba odraščala.

Naslednja ključna točka je *prepoznav*,⁶ ki je skupni pojem za identifikacijo in verifikacijo.⁷ Bistvo verifikacije je zajeto v vprašanju "sem tisti za katerega se izdajam (am i whom i claim to be)?" (Chirillo in Blaul, 2003: 3). Bistvo identifikacije pa v vprašanju "kdo sem jaz (who am i)?" (ibidem). V praktičnem primeru verifikacija poteka tako, da se nek posameznik predstavi biometričnemu sistemu z zahtevano

⁴ Tem kriterijem je v praksi zelo težko v celoti zadostiti. Pri tem je problematična predvsem časovna nespremenljivost, saj bi pri doslednem upoštevanju tega kriterija kot neprimerne značilnosti obveljali tudi obraz, dlan idr., da ne govorimo o vedenjskih značilnostih. Problemi pa se pojavijo tudi pri specifičnosti za vsakega posameznika, saj imajo določene značilnosti enojajčni dvojčki praktično enake ter pri merljivosti, kjer se pojavlja problem invalidnosti, bolezni idr. Človek brez roke ali prstov pač ne more ustrezati zahtevam za odvzem prstnega odtisa ipd.

⁵ Za prepoznavo glasu ali hoje je potreben posnetek dolg nekaj sekund in ne zgolj enkratni zajem, ki je potreben za fiziološke značilnosti.

⁶ Prepoznav je nevtralen pojem tako za verifikacijo kot identifikacijo. Kljub temu, da tega ne uporabljajo vsi avtorji, pa se sam strinjam s potrebnostjo skupnega pojma, kot ga pojmujejo in uporabljajo tudi priznani strokovnjaki (glej npr. Maltoni et al, 2003; Jain et al, 2004; Jain, Ross in Prabhakar, 2004 idr.). Pojem bom uporabljal, kadar ne bom želel razlikovati med pojmom oz. kadar to ne bo potrebno.

⁷ Poleg verifikacije in identifikacije Phillips in sodelavci (2003: 6) opredeljujejo še t.i. listo oz. seznam iskanih (watch list) z vprašanjem ali me iščete? (Are you looking for me?) Sam ne vidim razloga, da bi listo iskanih posebej izdvajal, saj gre po mojem mnenju le za obliko identifikacije s pomočjo točno določenih omejenih oz. zmanjšanih podatkovnih baz v katerih so le (najbolj) iskane osebe (npr. baza najbolj iskanih teroristov).

značilnostjo, ta pa jo primerja z že shranjeno šablono.⁸ Če je podobnost dovolj velika⁹ je zahtevek pozitivno razrešen. Verifikacija torej poteka na principu primerjave enega z enim (one to one). V praksi poteka identifikacija takrat, ko se želi ugotoviti identiteta posameznika, katerega šablona je shranjena v podatkovni bazi. Na ta način se zajame posameznikova značilnost¹⁰ in se jo primerja s celotno podatkovno bazo. Identifikacija tako poteka na principu primerjave enega z mnogimi (one to many).

Zadnji ključni del definicije se nanaša na *matematično-statistične analize značilnosti*. Gre predvsem za programsko opremo, ki jo pri biometričnih metodah predstavljajo algoritmi, ki 'obdelujejo' podatke na način primeren za izvedbo same primerjave.

3.2 BIOMETRIČNE METODE

Glede definicije biometričnih metod v tuji, znanstveni in tudi neznanstveni, literaturi ni večjih odstopanj, so le izpeljanke osnovno oblikovane definicije, ki v večini zapisov zavzema sledečo obliko: *Biometrične metode so avtomatizirane metode prepoznave ljudi, temelječe na njihovih fizioloških ali/in vedenjskih značilnosti* (glej npr. Woodward, Orlans in Higgins, 2003: 27; Chirillo in Blaul, 2003: 2; Prabhakar et al, 2003: 33; Jain et al, 2004: 1 idr.).

Glede na to, da sem nekatere temeljne značilnosti, ki so zajete tudi v zgornji definiciji opisal že pri pojmu biometrije, mi ostaja še opis *avtomatiziranih* metod. "Beseda avtomatizirane je nujna za definicijo, ker bi brez nje opisovali tudi celo množico zelo običajnih, toda bistveno manj zanesljivih identifikacijskih tehnik kot npr. fotografija ali črnilni prstni odtis na identifikacijski znački" (Bowman, 2000).

Biometrične metode so avtomatizirane do stopnje, kot je avtomatiziran proces zajema vzorca, vzorčenja, primerjave zajetega vzorca s poprej pridobljenim vzorcem

⁸ Obstajajo tri prevladujoče metode, ki so lahko uporabljene za shranjevanje šablon. To so: lokalna hramba, mrežna hramba, ter hranjenje na prenosnem mediju (npr. pametna kartica) (Woodward, Orlans in Higgins, 2003: 40). Pri verifikaciji je šablona običajno shranjena na prenosnem mediju, pri identifikaciji pa na samem sistemu (lokalna hramba) ali oddaljeni podatkovni bazi (mrežna hramba).

⁹ (Skoraj) vedno gre zgolj za približek in (skoraj) nikoli za popolno ujemanje. Stopnjo oz. odstotek ujemanja, za katerega se zahtevek pozitivno razreši določi tisti, ki s sistemom upravlja in se v angleškem jeziku imenuje threshold. Nastavitev te stopnje odločilno vpliva na napake biometričnega sistema.

¹⁰ Ta zajem lahko poteka na prikrit ali odkrit način.

in algoritemske primerjave, ki omogoči rezultat.¹¹ Posledica tega je, da je odločanje zelo hitro in se večinoma zgodi v realnem času (How is Biometrics Defined?, 2005).

Za boljši pregled nad biometričnimi metodami bom naštel tiste,¹² ki sem jih zasledil v strokovni literaturi.¹³

Vrste biometričnih metod: prepoznavna prstnih odtisov, prepoznavna geometrije roke, prepoznavna odtisa dlani, obrazna prepoznavna, glasovna prepoznavna, prepoznavna šarenice, prepoznavna mrežnice, prepoznavna podpisa, prepoznavna dinamike tipkovničnega vpisa, prepoznavna vzorca žil na notranji strani zapestja, prepoznavna obraznega termograma, prepoznavna znojnih por, prepoznavna stiska roke, prepoznavna telesnega vonja, prepoznavna oblike ušesa, prepoznavna značilne drže oz. hoje, prepoznavna vzorcev možganskega valovanja, prepoznavna odtisov stopal, prepoznavna DNK¹⁴ (Woodward, Orlans in Higgins, 2003: 45-136; Chirillo in Blaul, 2003: 13-251; Trapečar in Robek, 2003: 50).

Število biometričnih elementov in posledično biometričnih metod je omejeno zgolj z našo domišljijo in našo zmožnostjo merjenja teh značilnosti. Jih je toliko, kolikor je telesnih merljivih delov (Woodward, Orlans in Higgins, 2003: 135) in merljivih vedenj.

Za bolj celostno obdelavo področja o katerem pišem je potrebno opredeliti še nekatere druge pojme:

Biometrična tehnologija: *Biometrične tehnologije so avtomatizirane metode preverjanja in ugotavljanja identitete oseb* (Fefer, 2004: 148). Izraz se običajno uporablja, ko se govori o področju biometričnih metod na splošno.

¹¹ Rezultat je običajno zgolj binaren, torej zgolj DA/NE. Redko je lahko rezultat sestavljen iz večjega števila zadetkov, kar pa je posledica nizko določene stopnje ujemanja in se uporablja, kadar se resnično ne želi izpustiti možnega zadetka, pa čeprav to pomeni dodatno preverjanje s strani strokovnjakov in se uporablja predvsem pri prepoznavi prstnih odtisov s strani organov pregona.

¹² Seveda pregled ne more biti popoln, saj je biometričnih metod zelo veliko in se tudi zelo hitro pojavljajo nove. Nekatere od omenjenih so šele v raziskovalnih fazah ali pa še to ne.

¹³ Woodward, Orlans in Higgins (2003: 45-136) razdelijo biometrične metode na zrele oz. prevladujoče, ki so prisotne že nekaj časa in o katerih je bilo narejenih že veliko raziskav, so že prisotne in tudi uporabljane v praksi. Ostale biometrične metode pa avtorji poimenujejo kot ezoterične, ker so še vedno v eksperimentalnih ali razvojnih stopnjah. Sam podobnih delitev ne mislim delati, razlog pa je v hitrosti razvoja na tem področju, ki je zelo hiter. Običajnejše so delitve biometričnih metod glede na fiziološke oz. vedenjske značilnosti.

¹⁴ DNK (deoksi-ribonukleinska kislina) glede na definicijo ne ustreza kot element za biometrično metodo, saj o avtomatizaciji danes ne moremo govoriti pa tudi čas, ki je potreben za analizo DNK je neprimeren "saj so rezultati analiz lahko na voljo že (zgolj z vidika forenzičnih preiskav in ne z vidika biometričnih metod op. M.A.) v 24 – 48 urah" (Drobnič, 2001: 141).

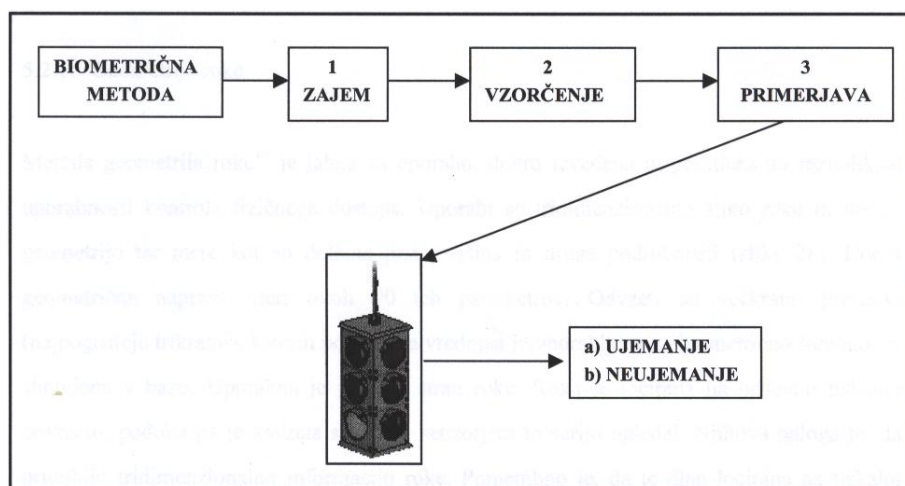
Biometrični sistem: Najustreznejše definicije v enem samem viru nisem našel, zato bom za definiranje tega pojma združil elemente več definicij.

Biometrični sistem je avtomatiziran sistem prepoznave fizičnih in/ali vedenjskih vzorcev, ki deluje na podlagi štiristopenjskega postopka (glej sliko 3.1), ki vsebuje:

- **zajem** vzorca fizičnih in/ali vedenjskih značilnosti,
- **vzorčenje**: izdelana je šablona individualnih značilnosti,
- **primerjava** zajetega vzorca z vzorci v bazi,¹⁵
- **rezultat**, pri katerem sistem potrdi ali ovrže primerjavo (Jain et al, 2004: 2; 1999 Glossary of Biometric Terms, 1999: 2; Trapečar in Robek, 2003: 49).

Večinoma sestavljajo biometrične sisteme naslednji sestavni deli. Potreben je senzor,¹⁶ za zajem biometričnega elementa, *algoritemska programska oprema*, ki poskrbi za vzorčenje, neka *podatkovna baza*, s katero se izvede primerjava in *ostala strojna in programska oprema*, ki omogoča potek omenjenih postopkov in na koncu 'razglasitev' rezultatov. Za delovanje biometričnega sistema pa je potrebno še usposobljeno osebje, da z njim upravlja.

Slika 3.1: Štiristopenjski postopek biometričnega sistema



Vir: Ashbourn, 2000 v Trapečar (2003: 76).

“Štiristopenjski proces je enako uporaben za identifikacijo, verifikacijo in potrditev, vendar je potrebno upoštevati posamezne značilnosti biometričnih tehnik, predvsem s stališča okolja in človeškega faktorja. Samo nevtrarno zajeti biometrični material je

¹⁵ Primerjava poteka na podlagi primerjanja algoritmov.

¹⁶ Mišljeno v širšem smislu, tako da so kot senzorji mišljeni, poleg različnih vrst senzorjev (optičnih, toplotnih, ultrazvočnih idr.), tudi npr. video kamere, skenerji, naprave za snemanje idr.

lahko osnova za spreminjanje z matematičnim algoritmom, ki je bistvo biometričnega sistema in razlog za visoko stopnjo zanesljivosti” (Trapečar in Robek, 2003: 50).

Biometrični element (biometric): *Biometrični element je merljiva fizična ali vedenjska značilnost, ki je uporabljena za prepoznavo posameznika* (1999 Glossary of Biometric Terms, 1999: 2).

Biometrični vzorec (biometric sample): *Biometrični vzorec je 'surov' (neobdelan) podatek, ki predstavlja biometrično značilnost končnega uporabnika, kot je zajet s strani biometričnega sistema* (1999 Glossary of Biometric Terms, 1999: 2). “Za biometrični vzorec, nad katerim se vrši proces identifikacije ali verifikacije, so primerni le deli telesa, katerih karakteristike so specifične za vsakega posameznika, so s časom nespremenljive oz. stabilne in so merljive” (Fefer, 2004: 151).

Biometrični podatek (biometric data): *Biometrični podatek je informacija, ki je 'vzeta' iz biometričnega vzorca in uporabljena ali za kreiranje šablone ali za primerjavo z že prej narejeno šablono* (1999 Glossary of Biometric Terms, 1999: 2).

Šablona (template): *Šablona je podatek, ki predstavlja biometrično meritev posameznika in je tvorjena s pomočjo algoritma ter jo uporablja biometrični sistem za primerjavo z na novo vzetim biometričnim vzorcem* (1999 Glossary of Biometric Terms, 1999: 2; Woodward, Orlans in Higgins, 2003: 262, 263).

Točnost biometričnega sistema je izražena z '*Deležem napačnih odobritev*' (FAR - False Acceptance Rate) ter '*Deležem napačnih zavrnitev*' (FRR – False Rejection Rate) (McDowall, 2000 v Fefer, 2004: 151).

- **FAR¹⁷** (False Acceptance Rate): **Delež napačnih odobritev** je definiran kot delež napačno odobrenih pristopov nepooblaščenih uporabnikov glede na število vseh testiranih pristopov uporabnikov, izražen v odstotkih.
- **FRR¹⁸** (False Rejection Rate): **Delež napačnih zavrnitev** je definiran kot delež napačno zavrnjenih pooblaščenih uporabnikov glede na število vseh

¹⁷ Delež napačnih odobritev (FAR) se včasih v angleški literature pojavlja še kot napaka tipa 2 (type 2 error) ali delež napačnega ujemanja (FMR - false match rate).

testiranih pristopov uporabnikov, izražen v odstotkih (McDowall, 2000 v Fefer, 2003: 151).

Formula za izračun FAR in FRR:

$$(\%) FAR = \frac{FA}{N} \times 100$$

FAR – Delež napačnih odobritev

FA – Število napačnih odobritev

N – Število poskusov

$$(\%) FRR = \frac{FR}{N} \times 100$$

FRR – Delež napačnih zavrnitev

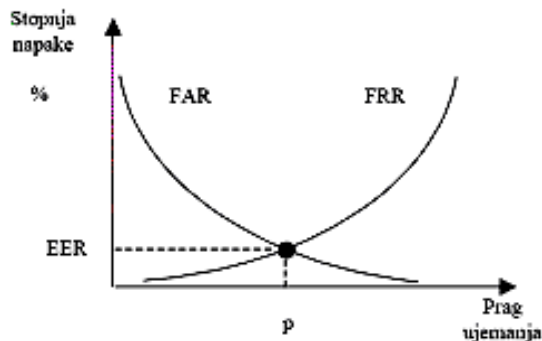
FR – Število napačnih zavrnitev

N – Število poskusov

Vir: Prirejeno po Woodward, Orlans in Higgins (2003: 35).

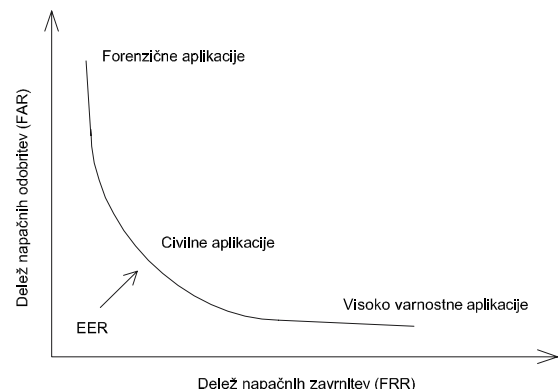
- **EER¹⁹** (Equal Error Rate): **Stopnja enake napake**, pri kateri sta vrednosti FAR (Delež napačnih odobritev) in FRR (Delež napačnih zavrnitev) enaki (glej graf 3.1)²⁰ (Fefer, 2004: 151).

Graf 3.1: Delež napačnih odobritev/zavrnitev



Vir: Fefer (2004: 152).

Graf 3.2: Prikaz izbire stopenj napak glede na aplikacijo biometričnega sistema



Vir: Maltoni et al (2003: 17, 18).

¹⁸ Delež napačnih zavrnitev (FRR) se včasih v angleški literaturi pojavlja še kot napaka tipa 1 (type 1 error) ali delež napačnega neujemanja (FNMR - false non-match rate).

¹⁹ Angleško tudi Crossover Error Rate (CER).

²⁰ Točka EER pomeni uravnoteženje poprej opisanih napak biometričnih sistemov. Vsak biometrični sistem ima svoje karakteristike in za vsakega posebej je potrebno narisati tak graf, da dobimo točko EER. Nadalje je zelo pomembno povedati še, da ta točka ne pomeni nujno najpametnejše izbire, ampak je potrebno to razmerje določiti na podlagi okolja, za katerega se bo določeni biometrični sistem uporabljal.

Točka EER je najprimernejša v večini civilnih aplikacij. Za dostop do zelo varovanih območij je potrebno na minimum zmanjšati FAR, medtem ko forenzične aplikacije uporabljajo zelo nizko stopnjo FRR (Maltoni et al, 2003: 17, 18), glej graf 3.2.

Poleg obeh stopenj napak pa so pomembni še nekateri drugi deleži, ki pomembno vplivajo na samo točnost biometričnega sistema.

- **FER** (Failure to Enroll Rate): **Delež nezmožnosti registracije** je delež uporabnikov, za katere biometrični sistem ni zmožen ustvariti šablone zadovoljive kakovosti (Biometric Glossary and Abbreviations, 2005), kar je lahko posledica poškodbe uporabnika, problemov s kvaliteto zajema ali problemov pri pozicioniranju (Woodward, Orlans in Higgins, 2003: 188).
- **FTA** (Failure to Acquire Rate): **Delež nezmožnosti zajema biometričnega podatka** je delež poskusov biometričnega sistema, v katerih le-ta ne more zajeti 'slike' zadovoljive kakovosti (Biometric Glossary and Abbreviations, 2005). Razlika med FTA in FER je v tem, da FER nastane ob registraciji uporabnika, FTA pa ob ponovnem odvzemu biometričnega podatka npr. za primerjavo vzorcev ob dostopu.

3.3 TERORIZEM

Terorizem vsekakor ni nov pojav. "V resnici je terorizem poznan že iz starodavnih časov, medtem ko je sam pojem stalno v uporabi od 18. st." (Symeonidou-Kastanidou, 2004: 16). "Tujka terorizem je bila v slovenščino prevzeta iz francoščine. Beseda *terreur* pa se je v političnem izrazoslovju uveljavila razmeroma pozno, in sicer s francosko revolucijo, ko je izvirno označevala sistem vladanja z nasiljem in (u)strahovanjem, ki so ga izvajali jakobinci, zato ta čas (od marca 1793 do julija 1794) imenujemo obdobje jakobinskega terorja" (Smolej, 2003: 10, 11).

Zdi se mi primerno, da omenim dejstvo, da mednarodno sprejete definicije terorizma preprosto ni,²¹ čeprav so v preteklosti in še vedno potekajo aktivnosti,²² da bi se omenjeno uresničilo.²³ Ganor (2002: 287) celo meni, da večina znanstvenikov, ki raziskujejo to področje verjame, da objektivne in mednarodno sprejete definicije ne bo nikoli moč sprejeti.

²¹ "IC/elo ameriška vlada uporablja v tej zvezi različne definicije, da ne omenimo drugih" (Rizman, 2004).

²² S to težko nalogo se trenutno ukvarja šesti komite generalne skupščine ZN (General Assembly's Sixth Committee), ki razpravlja o splošni konvenciji o mednarodnem terorizmu (draft Comprehensive Convention on International Terrorism), ki bo vsebovala definicijo terorizma, če bo sprejeta (Counter - Terrorism Committee, 2005).

²³ Sprejetih je 12 mednarodnih konvencij za različne vidike terorizma oz. preprečevanja le-tega.

Razlikujejo se celo mnenja o tem, ali je sploh potrebno sprejeti takšno definicijo. Ganor (2002: 288) v tem pogledu zastopa jasno stališče, ko pravi, da “/o/bjektivna definicija terorizma ni le možna; ampak je tudi nujno potrebna v vsakem resnem poskusu boriti se proti terorizmu”.

Tako smo soočeni z množico definicij tega zelo kompleksnega pojava, ko praktično vsak, ki piše o terorizmu, veliko organizacij, držav, varnostnih organov idr. uporablja svojo definicijo terorizma, ki pač ustreza njihovim ciljem in prepričanjem. “Različne definicije imajo seveda različne etične in politične (tudi praktične) implikacije” (Rizman, 2004). “Veliko definicij, ki jih danes uporabljajo v tem pogledu hinavske države ali pa so jih uporabljale v preteklosti, meri na to, da so naši 'teroristi' v resnici 'borci za svobodo', njihovi 'borci za svobodo' pa v resnici 'teroristi'” (ibidem).²⁴

Da je zmeda na tem področju še večja je krivo tudi dejstvo, da je več različnih terorizmov oz. njegovih podzvrsti. Sorel (2003: 1367) tako *navaja terorizem z revolucionarnimi zahtevami* (npr. Italijanske Rdeče Brigade, Nemška frakcija rdeče Armade idr.), *terorizem z nacionalističnimi ali neodvisnostnimi zahtevami* (IRA, ETA idr.), *fundamentalistični terorizem* (Hamas, Al-Quaeda idr.), *terorizem skrajne desnice* (OAS idr.), *ekološki terorizem*, *kiber terorizem*, pri čemer avtor navaja, da seznam še zdaleč ni vseobsegajoč. Za potrebo diplomskega dela razlikovanje med terorizmi ni potrebno.

Ganor (2002: 288) opredeljuje terorizem kot “namerno uporabo ali grožnjo z uporabo nasilja proti civilistom z namenom pridobiti politične, ideološke ali verske namene”.

Sorel (2003, 371) mednarodni terorizem opredeli kot “nezakonito dejanje (ne glede na storilca ali njegov namen), ki povzroči nemir v javnem redu, kot je definiran s strani mednarodne skupnosti, z uporabo resnega in nediskriminatornega nasilja (v kakršni koli obliki, tako proti ljudem kot tudi proti javni ali zasebni lastnini) s ciljem ustvariti ozračje terorja in ciljem vplivanja na politično delovanje”.

²⁴ Zgodovina in tudi sedanost nam postreže s precej takšnimi primeri. Npr. fašistično pojmovanje 'prvih antifašistov v Evropi' kot teroristov in ustrelitev Bidovca, Marušiča, Miloša in Valenčiča 6.9.1930 v Bazovici (Novice – TIGR, 2005), pojmovanja nacističnih oblasti med II. SV do odporiških gibanj kot teroristov, dojemanja mudžahidov med Rusko okupacijo Afganistana, pojmovanja skrajnih palestinskih gibanj in mnogo drugih podobnih primerov.

V Vzorcih globalnega terorizma 2003 (2004: xii)²⁵ je podana definicija terorizma.²⁶ Definicija se glasi: "Pojem terorizem pomeni naklepno, politično motivirano nasilje proti neborcem s strani podnacionalnih skupin ali tajnih agentov, običajno predviden za vpliv na javnost". Pojem mednarodni terorizem je opredeljen kot: "terorizem, ki vključuje državljane ali teritorij več kot ene države". Pojem teroristične skupine pa kot "skupina, ki izvaja, ali ki ima pomembne podskupine, ki izvajajo mednarodni terorizem".

Definicija ima tri ključne značilnosti, ki razlikujejo terorizem od ostalih oblik nasilja. Prvič, terorizem mora biti politično motiviran (teroristična dejanja imajo namen upravljati ali vplivati na vladne odločitve). Drugič, teroristično nasilje je naperjeno proti neborcem (ljudje, ki niso člani vojske, ali niso aktivno udeleženi v vojaških sovražnostih) in tretjič, da podnacionalne skupine ali tajni agenti zagrešijo teroristična dejanja (Ruby 2002: 10, 11).

Na ravni EU pred 11. 9. 2001 ni bilo storjeno prav veliko v smeri definiranja terorizma. Izjemo predstavlja podpis Evropske konvencije o zatiranju terorizma (European Convention on The Supression of Terrorism) iz leta 1977. Toda ta konvencija ne ponuja celovite definicije terorizma²⁷ (Dumitriu, 2004: 586). Po 11. 9. 2001 pa so se stvari začele precej hitreje odvijati in sprejet je bil okvirni sklep sveta z dne 13. junija 2002 o boju proti terorizmu (Council Framework decision of 13 June 2002 on Combating Terrorism).²⁸ Ta dokument predstavlja "temelj boja Evropske unije proti terorizmu" (Dumitriu, 2004: 590). Za opredelitev terorizma je še zlasti pomemben člen 1, ki ga zato navajam v celoti.

Člen 1: Teroristična kazniva dejanja in temeljne pravice in načela

1. Vsaka država članica sprejme vse potrebne ukrepe, ki zagotavljajo, da se namerna dejanja, na katera se nanašajo spodnje točke (a) do (i) in ki so po nacionalni zakonodaji določena kot kazniva dejanja, ki lahko zaradi svojega značaja ali vsebine hudo škodujejo državi ali mednarodni organizaciji, kadar so storjena z namenom:

– da bi resno zastraševala prebivalstvo ali

²⁵ Patterns of Global Terrorism 2003. Gre za letno publikacijo ameriškega zunanjega ministrstva o globalnem terorizmu.

²⁶ Definicija je sicer vzeta iz Title 22 of the United States Code, Section 2656f(d).

²⁷ Njen cilj je proceduralne narave, torej pregon terorističnih dejanj, s strani držav podpisnic (Dumitriu, 2004: 586).

²⁸ Države članice naj bi v svojo zakonodajo vpeljale sprejeta določila do 31.12.2002 (Article 11). Toda do konca marca 2004 je to storilo zgolj 8 držav (Belgija, Italija, Avstrija, Danska, Finska, Švedska in Velika Britanija (Agence Europe, n°8657, 27 March 2004, p. 6 and 7 v Dumitriu, 2004: 589).

- nezakonito izsiljevala vlado ali mednarodno organizacijo, da izvede ali opusti kakršno koli dejanje ali
- da bi resno rušila ali uničevala temeljne politične, ustavne, gospodarske ali socialne strukture države ali mednarodne organizacije, šteje za teroristična kazniva dejanja:
 - (a) napadi na človekovo življenje, ki lahko povzročijo smrt;
 - (b) napadi na fizično integriteto človeka;
 - (c) ugrabitev ali zajetje talcev;
 - (d) znatno uničevanje vladnih ali javnih objektov, transportnega sistema, infrastrukture, vključno z informacijskim sistemom, pričvrščenih ploščadi, ki se nahajajo na epikontinentalnem pasu, javnega kraja ali zasebne lastnine, ki lahko ogrozi človekovo življenje ali povzroči večjo gospodarsko izgubo;
 - (e) ugrabitev letal, ladij ali drugih sredstev javnega ali tovornega transporta;
 - (f) proizvodnja, posedovanje, nakup, prevoz, dobava ali uporaba orožja, razstreliv ali jedrskega, biološkega ali kemičnega orožja, kot tudi raziskave in razvijanje biološkega in kemičnega orožja;
 - (g) spuščanje nevarnih snovi ali povzročanje požarov, poplav ali eksplozij, ki lahko ogrozijo človekovo življenje;
 - (h) motnje ali prekinitve oskrbe z vodo, elektriko ali drugimi osnovnimi naravnimi viri, ki lahko ogrozijo človekovo življenje;
 - (i) grožnja, da se bo izvršilo katero od dejanj, naštetih v točkah (a) do (h).

Glede na podano definicijo velja, da so vsa teroristična dejanja, ki so prepovedana z mednarodnimi konvencijami o terorizmu zajeta v okvirnem sklepu (Dumitriu, 2004: 595).

3.4 PREPREČEVANJE TERORIZMA

Glede na SSKJ (1994: 1012) je beseda preprečevanje glagolnik besede preprečevati, ki pomeni: delati, povzročati

a) da se kako dejanje, stanje, dogajanje ne uresniči: preprečevati nesreče, zločine...

b) da kaj ne more (nemoteno) potekati: preprečevati razvoj česa...

//delati, povzročati, da kdo česa ne more narediti, doseči: ... njihov namen je bil preprečevati sovražne akcije...

Vse omenjeno je tudi samo bistvo preprečevanja terorizma.

Heymann (2003: 166-168) kot logiko preprečevanja terorizma v ZDA našteva pet točk v preprečevanju terorizma, za katere menim, da so lahko splošno uporabne:

1. zmanjševanje navdušenja za napade na državo;
2. zastraševanje preko organov pregona, vojske ali ekonomskih groženj;
3. onemogočanje dostopa do:
 - a. ciljev,
 - b. sredstev,
 - c. države.
4. zbiranje in analiziranje (obveščevalnih) informacij o posameznikih, skupinah, organizacijah in dejavnostih;
5. razdor vključujoč prikrite operacije, zaplembo premoženja in onemogočanje preko kazenskega pregona in pripora.

Čeprav avtor v teh točkah ne omenja biometričnih metod, sem sam mnenja, da imajo lahko biometrične metode svojo (pozitivno) vlogo v zadnjih štirih točkah, praktično edinstveno in v prihodnosti verjetno primarno vlogo pa vsaj v tretji točki tj. pri onemogočanju dostopa do ciljev, sredstev in države (v primeru, ki ga podaja Heymann so to ZDA, vendar lahko to razširimo na katerokoli državo), kar bom bolj natančno razdelal v sledečih poglavjih.

Neposredno pa vlogo biometričnih metod v preprečevanju terorizma vidi Woodward (2001b: 3). "Ko se država obnavlja po napadih 11. septembra 2001, se moramo ponovno posvetiti naporom, da bi preprečili kakršno koli teroristično dejanje v prihodnosti. Kljub temu, da terorizem nikoli ne more biti popolnoma odstranjen, lahko kot narod naredimo dodatne korake, da se mu zoperstavimo. Raziskati moramo uporabo pojavljajočih se biometričnih tehnologij,²⁹ ki lahko izboljšajo javno varnost. Ker ni enostavnih in nezmotljivih tehnoloških rešitev za preprečevanje terorizma, je uporaba biometričnih tehnologij lahko pomoč narediti Ameriko varnejšo".

Prav to pa je tudi bistvo diplomskega dela. Torej, ali lahko biometrične metode naredijo katero koli državo varnejšo pred vedno izrazitejšo grožnjo terorizma.

²⁹ Biometrične metode so bile v jan/feb številki 2001 MIT Technology Review razglašene za eno izmed deset najbolj obetavnih pojavljajočih se tehnologij, ki bodo v prihodnosti vplivale na svet.

4. ZGODOVINA UPORABE BIOMETRIČNIH METOD

Ko govorimo o zgodovini uporabe biometričnih metod, je to seveda potrebno jemati pogojno, saj o pravi zgodovini, glede na današnjo definicijo - ...avtomatizirane metode..., sploh ne bi mogli govoriti, oziroma šele od vzpostavitve prve take avtomatizacije, ki je po mojem vedenju vzpostavitev avtomatizirane primerjave prstnih odtisov AFIS.³⁰ "Prvi AFIS sistem je bil izdelan in razvit leta 1974 v podjetju Printrak, leta 1975 pa je bil nameščen tudi prvi čitalec desetprstnih daktiloskopskih kartonov" (Dalrymple in Mackillican, 2000 v Trapečar in Vidic, 2004: 181). Naj omenim, da v poglavju nimam namena temeljito raziskati zgodovine, želim zgolj prikazati, da je princip star 'tisoče let', posebej pa bom omenil še kratek oris razvoja biometričnih metod, ki jih bom v nadaljevanju naloge podrobneje opisal.

Že od zgodnjih civilizacij lahko zasledimo uporabo metod, ki so služile za prepoznavo ljudi, pa čeprav niso bile avtomatizirane. Torej v zgodovinskem kontekstu lahko govorimo o uporabi 'neavtomatiziranih biometričnih metod'.

"Uporaba biometrije je znana človeku že iz časa prvih zapisov" (Črnčec, 2004a: 19). Kasekem, uradnik za časa faraona Kefrena (ok. 2575 – 2325 pr.n.št.) je uporabil biometrične metode razvrščanja delavcev, ki so omogočale, da le-ti ne bi bili dvakrat plačani. To je storil s pomočjo sistema za identifikacijo posameznikov, v katerem je imel vsak posameznik svoj dosje, ki je zajemal: ime, starost, kraj rojstva ter natančno opredelitev dela in nalog na gradbišču. Dosje je nato sistematično dopolnjeval z individualnimi, fizičnimi ali značajskimi, karakteristikami. Podrobnosti v dosjeju so Kasekemu omogočile, da je natančno potrdil identiteto vsakega delavca ter tako preprečil zlorabe (Črnčec, 2004a: 19, 21).

"Biometrične metode kot koncept so stare preko tisoč let."³¹ Tako so lončarji v vzhodni Aziji odtisnili svoje prstne odtise na izdelke, da bi se vedelo kdo jih je naredil. V dolini Nila v Egiptu so trgovce, ki so jim zaupali identificirali glede na njihovo višino, barvo oči in barvo polti (Woodward, Orlans in Higgins, 2003: 26).

"Med prvimi znanimi primeri uporabe biometrične metode je bilo odvzemanje odtisov na Kitajskem v 14. st., kot je poročal portugalski zgodovinar Joao de Barros.

³⁰ AFIS – Automated Fingerprint Identification System oz. slovensko 'Avtomatska identifikacija po prstnih odtisih' (Trapečar in Vidic, 2004: 180).

³¹ Pri navajanju starosti biometričnih metod si avtorji vsekakor niso enotni, zato se pojavljajo ocene od nekaj tisoč let (primer Kasekem) do nekaj več kot sto let.

Kitajski trgovci so s črnilom odtisnili na papir otroške dlani in stopala, da bi razlikovali otroke med sabo" (Chirillo in Blaul, 2003: 2).

Iz zgodovinskega vidika biometričnih metod je nedvomno zelo pomemben Alphonse Bertillon, uradnik (in antropolog) v Pariški policiji, ki je leta 1883³² predstavil sistem merjenja človekovih fizičnih lastnosti.³³ Bertillon je osnoval svoj sistem na predpostavki, da se razmerja človeških kosti ne spreminjajo skozi življenje. Merjenja v njegovem sistemu so vključevala: dolžino, višino in širino glave, dolžino različnih prstov, dolžino podlakti idr. (Scrotty History, 2005). Njegov sistem so uporabljale policije po celem svetu, vendar je to kmalu zamrlo, saj so odkrili, da imajo nekateri ljudje zelo podobne meritve (A Brief History of Biometrics, 2005). Njegovo ukinitvev je pospešilo tudi ali predvsem odkritje zanesljivejše metode prepoznave ljudi.

To odkritje pomeni naslednji korak v razvoju biometričnih metod in je mnogo bolj pomembno ter predstavlja pravi mejnik v razvoju teh metod. Gre seveda za prepoznavo prstnih odtisov. To, da so lončarji že pred tisoč leti uporabljali svoje prstne odtise kot dokaz istovetnosti, sem že omenil in gre torej za zelo star princip.

Leta 1684 je angleški rastlinski morfolog Nehemiah Grew izdal prvi znanstveni zapis o sistematični študiji individualnih značilnosti prstnih odtisov (Lee in Gaensslen, 2001 v Maltoni et al, 2003: 21, 22). Temu so v naslednjih desetletjih in stoletjih sledili tudi drugi.

Za razvoj biometrične metode prstnih odtisov je potrebno omeniti še Sira Francisa Galtona in dr. Henryja Fauldsa, ki sta v 80-ih letih 19. st. razvila zelo podobna klasifikacijska sistema prstnih odtisov (The Henry Classification system, 2003: 1).

Leta 1896 je Sir Edward Henry³⁴ odredil zbiranje prstnih odtisov zapornikov in razvil Henryjev klasifikacijski sistem,³⁵ ki je kmalu doživel sprejetje po celem svetu (The Henry Classification system, 2003: 1).

Prva uspešna obsodba, katere podlaga so bili prstni odtisi je bila leta 1902 v VB, ko je bil Harry Jackson obsojen na 7 let zapore zaradi vloma (Metropolitan Police Service Centenary Fingerprint Bureau Press Pack, 2005).

³² Tudi pri navajanju tega podatka sem zasledil različne letnice od 1879 do 1889.

³³ Po njem imenovan tudi bertillonáža. S tem je tudi ustvarjalec antropometrije, ki je "sistem telesnih merenj odraslih posameznikov za osebno identifikacijo" (Alphonse Bertillon and Ear Prints, 2005).

³⁴ Takrat generalni inšpektor Bengalske policije.

³⁵ S pomočjo Azial Haque in Hemchandra Bose v letih 1896 in 1897, s katerim so razširili in dopolnili Galtonov klasifikacijski sistem (Metropolitan Police Service Centenary Fingerprint Bureau Press Pack, 2005).

V naslednjih desetletjih se je zbiranje in iskanje ljudi na podlagi prstnih odtisov zelo razširilo in znanstveno raziskovalo. Naslednji velik korak na trem področju je sledil v 70-ih letih 20. st. z razvojem sistema AFIS, ki nekateri še danes uporabljajo osnove, kot jih je razvil Sir Edward Henry s sodelavcema v svojem klasifikacijskem sistemu.

Začetke obrazne prepoznavne lahko pogojno vidimo "iž/e od leta 1600 (ko) so bile uporabljene skice za iskanje kriminalcev. V letu 1800 je začel poštni sistem objavljati liste najbolj iskanih, na katerem so bile slike tistih, ki so jih iskale agencije organov pregona" (Buskey, 2001: 5).

Začetki računalniške raziskave obrazne prepoznavne segajo v pozna 80. leta 20. st. s prvimi komercialno dostopnimi sistemi v 90. letih (Individual biometrics - Facial Recognition, 2005). Kot vidimo, je obrazna prepoznavna, kot jo poznamo danes, zelo mlada biometrična metoda in so zato problemi, ki jo spremljajo, tudi iz tega vidika lažje razumljivi.

"Idejo uporabe vzorcev šarenice za osebno identifikacijo je prvotno leta 1936 predlagal oftalmolog Frank Burch. Do 80. let se je ideja pojavljala v filmih o Jamesu Bondu, toda ostala znanstvena fantastika in domneva. Leta 1987 sta oftalmologa Aran Safir in Leonard Flom to idejo patentirala in leta 1989 prosila Johna Daugmana, ki je takrat predaval na Harvardski univerzi, naj poskusi izdelati algoritem za prepoznavo šarenice. Ti algoritmi, ki jih je Daugman patentiral leta 1994 in so last podjetja Iridian Technologies, so osnova za vse sedanje sisteme šarenične prepoznavne in izdelke" (Individual biometrics - Iris Scan, 2005).

Če povzamem, je princip biometričnih metod zelo star. Sistematična znanstvena raziskovanja se pojavijo konec 17. st. in se bistveno razmahnejo v 20. st., pri čemer absolutno prednjačijo prstni odtisi, ki kot prvi izpolnijo del definicije, ki se nanaša na avtomatizacijo. Ostale biometrične metode se pojavijo precej pozneje in imajo za sabo tudi precej manjše znanstveno raziskovanje, ki pa se v zadnjih letih precej povečuje.

5. VZROKI UPORABE BIOMETRIČNIH METOD

Glede na preučeno literaturo, kjer sicer ni velikokrat neposredno pisano o vzrokih za uvedbo biometričnih metod, lahko sklepam, da je glavni razlog za uvedbo biometričnih metod oz. biometričnih sistemov v uporabo predvsem povečanje

varnosti. To je na področju, s katerim se ukvarjam (preprečevanje terorizma), nedvoumno. Drugi razlog, ki pa je na področju preprečevanja terorizma daleč v ozadju, je povečana prikladnost oz. enostavnejša uporaba, ki jo prinese uporaba biometričnih metod. Omenjeni vzrok ima precejšno veljavo v civilnih aplikacijah biometričnih metod. Tretji razlog, ki je ponovno prevladujoč v civilnih aplikacijah, je zmanjševanje stroškov. Glede tega tretjega razloga so si mnenja sicer različna. Nekateri želijo predstaviti uvajanje biometričnih metod tudi kot željo države po povečanem nadzoru nad njenimi prebivalci.

Kljub temu, da imata drugi in tretji razlog na področju, ki ga opisujem, v najboljšem primeru sekundarno vlogo, jih glede na možen hiter tehnološki razvoj ni moč povsem zanemariti, zato jih bom na kratko opisal. Četrti možni razlog pa je tako povezan z devetim poglavjem (vprašanje zasebnosti), da ga tu ne bom opisoval.

5.1 POVEČANJE VARNOSTI

Varnost kot zelo kompleksen pojem lahko razumemo na več načinov in v bistveno različnih aplikacijah. Povečanje varnosti, ki jo lahko prinesejo biometrične metode, je precej široko področje in je hkrati povezano s področji uporabe biometričnih metod. Povečanje varnosti gre tako predvsem na račun dostopa do varovanih (zaščitениh, občutljivih) območij, zanesljivejšega ugotavljanja identitete in kontrole vstopa in izstopa iz države ter prepoznavе (znanih) teroristov.

Dandanes si mora praktično vsak zapomniti na desetine gesel in PIN števil, ³⁶ kar zaradi preobilice informacij privede do zapisovanja gesel in PIN števil, pozabljanja le-teh in izbiranja istih gesel, kar je z varnostnega vidika precej tvegano početje. Drug način so takšne in drugačne kartice za dostop, izkaz pooblaščenosti idr. Kartice so lahko ukradene, posojene, ponarejene idr. Nivo varnosti se precej poveča s kombiniranjem obeh omenjenih metod, slabosti pa vseeno ostajajo. Povečanje varnosti se torej tukaj nanaša na manjšo možnost zlorab (in tudi enostavnejšo uporabo) omenjenih dveh avtentifikacijskih mehanizmov za dostop do varovanih območij s pomočjo preverjanja z biometričnimi metodami.

“Biometrične metode se uporabljajo v okoljih, kjer je zahtevana zelo visoka stopnja varnosti, vendar pa se njihova uporaba z napredkom tehnologije ter posledično tudi

³⁶ PIN - Personal Identification Number

manjšimi stroški nakupa in vzdrževanja vedno bolj širi tudi v okolja z zahtevano nižjo stopnjo varnosti” (Fefer, 2004: 150).

Pri zanesljivejšem ugotavljanju identitete ter zmanjševanju možnosti za identitetno krajo in zlorabo z uporabo biometričnih metod v osebne in potovalne dokumente se zmanjša možnost, da bi v državo vstopali ljudje s ponarejenimi potovalnimi dokumenti, kar je danes izrednega pomena, ki se ga zaveda veliko držav. V ta namen v številnih državah potekajo napor za vpeljavo biometričnih potnih listov³⁷ ter viz, ponekod pa celo za vzpostavitev biometričnih osebnih dokumentov. “Nacionalna vlada (ZDA op. M.A.) se zanaša na osebno prepoznavo za nadzor priseljevanja in mejno varnost (z uvedbo biometričnih metod op. M.A.)” (Skokowski, 2002: 2)

Nedvomno so številne države po celem svetu izredno zainteresirane za prepoznavo teroristov. Pri tem, ali so biometrične metode prava oz. vsaj dopolnilna metoda, pa so si mnenja deljena. Se je pa debata izredno povečala in intenzificirala po 11. 9. 2001 predvsem v ZDA, ki močno prednjačijo na tem področju tudi v praktičnih aplikacijah tega namena. “Raziskave biometričnih metod so postale prioriteta številka ena v iskanju države (ZDA op. M.A.) novih metod, ki bi ustvarile varno okolje za Američane in domovino” (Buskey, 2001: 3). “Danes biometrične metode ponujajo rešitve za dvig varnosti ter zavesti v preprečevanju kriminala³⁸ ter terorizma” (Buskey, 2001: 2). “Verjetno je preveč mamljivo misliti o biometričnih metodah kot o srebrnem metku za identifikacijo teroristov” (Skokowski, 2002: 1), kljub temu so “biometrične tehnike vsekakor močno orodje za identifikacijo in avtentifikacijo posameznikov. Vseeno pa je težava teh tehnik, da so popolnoma nemočne pri prepoznavi teroristov, če o njih nimamo točno določenih biometričnih podatkov, ki jih povežejo z znanimi teroristi” (ibidem), tako je bolje, “da vidimo biometrične tehnike kot orodje uporabno pretežno za identifikacijo navadnih državljanov in jim dopustiti, da nadaljujejo s svojim življenjem z več varnosti” (ibidem). Vidimo torej neobhodljivo nujo po biometričnih podatkih o teroristih, če jih sploh želimo prepoznati. Tukaj igrajo glavno vlogo varnostno-obveščevalne službe, ki morajo priskrbeti takšne podatke. Je pa res, da obrazna prepoznavna ne zahteva nič

³⁷ Gre za potne liste, ki imajo poleg običajnih podatkov in zaščit vgrajeno še pametno kartico z biometričnim(i) podatkom(i) o lastniku potnega lista.

³⁸ Vloga biometričnih metod (predvsem prstnih odtisov, odtisov dlani in stopal ter DNK) v preprečevanju kriminala oz. kazenskem preganjanju kaznivih dejanj je nedvoumna že preko stoletje, pojavljajo pa se tudi nove metode, ki bi lahko še nadalje pomagale pri preprečevanju kriminala, kot so npr. prepoznavna obraza idr. Sam se ne mislim nadalje spuščati v preprečevanje kriminala s pomočjo biometričnih metod, saj bi to prekomerno razširilo obseg diplomskega dela.

drugega kot zgolj sliko tistega, ki se ga želi iskati. Kljub posedovanju takšnega podatka je iskanje izredno težko in večinoma neuspešno. "Če smo pošteni, celo obsežni nadzorni sistemi,³⁹ lahko v najboljšem primeru le omejijo tveganje bodočih terorističnih dejanj" (Woodward, Orlans in Higgins, 2003: 355).

Za zaključek je na mestu ugotovitev da "i/zgleda jasno, da je glavna pridobitev, ki jo ponuja biometrija in tehnologija pametnih kartic, obljuba o povečani varnosti v svetu po enajstem septembru" (Skokowski, 2002: 7). Težko pa bi trdil, da je to res v vseh aplikacijah in okoljih, saj je na voljo še bistveno premalo empiričnih dokazov, ki bi lahko celovito podpirale to tezo.

5.2 POVEČANA PRIKLADNOST ZA UPORABNIKE

Povečana prikladnost pride do izraza predvsem v komercialnih aplikacijah. Kot že rečeno se, zaradi problemov z gesli in PIN številkami ter karticami, ponujajo biometrične metode tudi kot (poleg povečanja varnosti) metode, ki lahko povečajo prikladnost oziroma poenostavijo nekatere postopke, ki jih ljudje vsakodnevno uporabljamo. Bistvo povečane prikladnosti se skriva v dejstvu, da 'nosimo kartice, PIN številke in gesla v obliki biometričnih podatkov' vedno s seboj in jih ne moremo izgubiti⁴⁰ oz. pozabiti, ker so pač del vsakega izmed nas.

V ta namen so danes dostopni sistemi, ki uporabljajo različne biometrične metode in so vgrajeni ali priključeni v mobilne telefone, namizne in prenosne računalnike, POS (Point of sale) terminale, bencinske črpalke,⁴¹ kontrolo pristopa in registracijo delovnega časa,⁴² avtomobile⁴³ idr.

Z omenjenim se v sklopu povečevanja prikladnosti dosega predvsem zmanjševanja časa potrebnega za raznorazne dostope, kontrole, registracije idr. ter enostavnejšo uporabo za uporabnike (poleg seveda povečane varnosti in morebitnega zmanjševanja stroškov).

³⁹ Med katere nedvomno lahko uvrstimo tudi vse biometrične metode, ki imajo zmožnost prepoznavne 'na daljavo', predvsem pa sisteme obrazne prepoznavne.

⁴⁰ Teoretično lahko pride do 'izgube' npr. s kakšno nesrečo ali boleznijo, vendar je tako 'izgubo' nato moč nadomestiti.

⁴¹ Na Portugalskem so neko bencinsko črpalko opremili s čitalci geometrije roke, s pomočjo katerih se strošek za bencin pripiše na uporabnikov račun (Jain, 2004).

⁴² Slednje izdeluje tudi slovensko podjetje, ki je vgradilo več kot tisoč sistemov doma in po svetu, danes pa njihovi sistemi nadzirajo pristop in obračunavajo delovni čas za več kot četrtr milijona uporabnikov, iz dneva v dan, iz ure v uro (Špica International, 2005).

⁴³ Konceptualno vozilo Senso predstavljeno na ženevskem avtomobilskem salonu v marcu 2005.

5.3 ZMANJŠANJE STROŠKOV

Kot eden od razlogov za uvajanje biometričnih metod se pogosto navaja tudi zmanjš(ev)anje stroškov. Predpostavka temelji predvsem na dejstvu, da se namesto ostalih avtentifikacijskih tehnologij⁴⁴ uporablja biometrične metode.

Kljub temu si avtorji niso edini ali uvajanje biometričnih metod pomeni zmanjševanje ali povečevanje stroškov. Chirillo in Blaul (2003: 11) sta predstavnika prvih in tako trdita da, "biometrične rešitve pomenijo nižje stroške." Resnica po mojem mnenju leži v tem, da je zmanjševanje stroškov primarno odvisno od aplikacije, v katere so biometrične metode implementirane. Na velikost stroškov pa vplivajo tudi druge stvari in ne samo izbira med biometričnimi metodami in drugimi avtentifikacijskim tehnologijami. "Stroški, povezani z nakupom, uporabo in vzdrževanjem biometričnega sistema so v veliki meri odvisni od zahtevane stopnje varnosti varovanega objekta, torej od arhitekture varovanega objekta, števila uporabnikov in karakteristik njihovega pretoka ter specifičnih potreb varovanega območja.

Stroški se nanašajo na:

- izbiro in načrtovanje sistema,
- nakup naprav in programske opreme,
- namestitev sistema,
- usposabljanje uporabnikov in pooblaščenega osebja,
- vzdrževanje sistema in preostalo podporo" (Fefer, 2004: 152).

Toda, če imamo pri civilnih aplikacijah realno alternativo za biometrične metode (npr. kartica s precej dolgim geslom), po mojem mnenju take alternative pri preprečevanju terorizma (vsaj na nekaterih področjih) ni, saj razen biometričnih metod druge tehnologije ne omogočajo tako visoke stopnje varnosti, preprečevanja identitetne kraje, prepoznave 'na daljavo' idr. Kljub vsemu pa lahko ima zmanjševanje stroškov vlogo tudi pri biometričnih metodah s ciljem preprečevanja terorizma, in to predvsem pri kontroli dostopa. Logiko zmanjševanja stroškov bom ponazoril z dvema primeroma; z enim v civilni in enim v vojaški aplikaciji, ostalih raziskav nisem zasledil.

Chirillo in Blaul (2003: 25-27) primerjata stroške (iz resničnega sveta) med zaščito s pomočjo prstnih odtisov in zaščito s pomočjo gesel. Ugotavljata, da je kar 40 %

⁴⁴ Kartice in izkaznice, nekaj kar imaš, gesla in PIN številke, nekaj kar veš ter biometrične metode, nekaj kar si. Možno pa je tudi kombiniranje. (Woodward, Orleans in Higgins, 2003: 3-7).

vseh klicev za pomoč v podjetju povezanih s pozabljenimi gesli. Npr. da je referenčna točka podjetje z 10.000 zaposlenimi, to pomeni 20.000 klicev (v center za pomoč zaposlenim) na mesec, od tega jih je z gesli povezanih 8.000. Za 20.000 klicev na mesec naj bi podjetje rabilo 21 zaposlenih. Ob povprečni plači za takega uslužbenca (35.000 \$) to znese 291.655 \$ na leto zaradi klicev povezanih z gesli. Temu je potrebno prišteti še ostale stroške (izgubljena produktivnost idr.), tako, da avtorja izračunata, da letnih stroškov zaradi izgube oz. pozabe gesel nanese za 935.640 \$. Nato podata informativen izračun stroškov za tako podjetje, če bi uporabljalo metodo prstnih odtisov namesto gesel. Skupaj z nakupom opreme ter stroški vzdrževanja za triletno obdobje bi nastali stroški v višini 1.710.000 \$ v primerjavi s stroški v triletnem obdobjem pri geslih, ki znašajo 2.806.920 \$, bi bil prihranek podjetja zaradi uvedbe tehnologije prstnih odtisov 1.087.920 \$ v treh letih.⁴⁵ Kljub temu, da gre za primerjalno zelo omejen ter po mojem mnenju tudi poenostavljen primer, je predstavljen, zgolj kot ilustrativen primer logike zmanjševanja stroškov pri uvedbi biometričnih metod.

Drugi primer pa predstavlja delo raziskovalcev iz Univerze Zahodne Virginije (WVU - West Virginia University), ki so naredili pilotno raziskavo stroškovne analize biometričnega sistema (na podlagi čitalcev geometrije rok in PIN kode) v vojaški bazi Scott Air Force Base, I11, v kateri se nahaja 13.000 vojaškega in civilnega osebja. Raziskovalci so ugotovili, da je potencialni prihranek baze približno 412.000 \$ v petih letih.⁴⁶ Poleg prihranka so raziskovalci videli možnost tudi za povečanje varnosti s premestitvijo varnostnikov na bolj zanimive naloge. Ta študija bo služila za prihodnjo implementacijo podobnih sistemov po obrambnem ministrstvu (Riley in Dell, 2004)

Kljub navedenima primeroma še zdaleč ni moč trditi, da uvedba biometričnih metod vedno pomeni zmanjševanje stroškov, še posebej pa ne v vseh aplikacijah. Ni dvoma, da bo uvedba biometričnih potnih listov velik strošek tako za državo kot njene državljane. Zaključim lahko zgolj z mislijo, da biometrične metode lahko pomenijo zmanjševanje stroškov v nekaterih aplikacijah (predvsem kontrola dostopa, poslovanje po spletu, nadomestitev za kartice in gesla idr.), vsekakor pa ne 'vedno in povsod'.

⁴⁵ V mislih pa je potrebno imeti tudi precejšnje zmanjševanje cen za biometrične sisteme.

⁴⁶ Do te številke so prišli, ko so odšteli 148.000 \$ predvidenih stroškov za nakup sistema geometrije roke od predvidenih 560.000 \$ prihranka, primarno zaradi premestitve varnostnikov.

6. NAJPRIMERNEJŠE BIOMETRIČNE METODE ZA PREPREČEVANJE TERORIZMA

Kot sem navedel že v prejšnjih poglavjih obstaja veliko različnih biometričnih metod. Praktično vsaka od njih je precej edinstvena in ima pomanjkljivosti in prednosti, izmed katerih so nekatere lastne le njej. Vsekakor pa velja, da je "u/streznost posamezne biometrične metode za praktično aplikacijo pogojena s specifičnimi zahtevami okolja, v katerega je biometrična tehnologija implementirana. Metoda, ki zagotavlja najvišjo stopnjo varnosti, ni nujno tudi najustreznejša" (Fefer, 2004: 148).

Biometrične metode se uporabljajo na veliko področjih in z različnimi cilji. Vloga biometričnih metod v preprečevanju terorizma pa se nasploh pojavlja in odkriva šele zadnja leta, predvsem po terorističnih napadih 11. 9. 2001. Po teh dogodkih smo namreč priča temu, da se je začelo veliko govoriti o biometričnih metodah, predvsem o tistih, ki naj bi pomenile doprinos pri preprečevanju terorizma. Največkrat se v tem kontekstu v zadnjem času omenja **obrazno prepoznavo**, predvsem zaradi značilnosti, ki so tej metodi (praktično) edinstvene (prepoznavna na daljavo, nepotrebno sodelovanje subjektov in s tem torej možnost prikritega delovanja oz. zajemanja podatkov, možnost identifikacije zgolj na podlagi fotografije). Zaradi teh lastnosti obrazni prepoznavi večinoma namenjajo največji potencial in prihodnost pri preprečevanju terorizma.

Nedvomno je naslednja biometrična metoda, ki ima vlogo v preprečevanju terorizma tudi biometrična metoda **prepoznave prstnih odtisov**. Ta metoda je vodilna v svetu, kar ima za posledico ogromne podatkovne baze, ki vsebujejo prstne odtise. Prstni odtisi so v smislu preprečevanja terorizma zelo primerni za verifikacijo, npr. za kontroliranje dostopa do občutljivih objektov in malo manj za identifikacijo.⁴⁷ Pomembnost prstnih odtisov in še bolj obrazne prepoznavne se kaže v uvajanju teh dveh biometričnih podatkov na potne listine ter od leta 2004 obvezen odvzem le-teh na ameriških letališčih ter pristaniščih.

⁴⁷ Glede na to, da imajo organi pregona le redko prstne odtise teroristov pa tudi zajem 'na daljavo' (še) ni možen.

Menim, da je potrebno opisati tudi metodo **prepoznavne šarenice**, saj velja za eno najnatančnejših biometričnih metod, ki je trenutno prisotna in je kot taka izredno primerna za področja, kjer se zahteva najvišjo stopnjo varnosti.

Opisal bom tudi **multimodalne biometrične metode**, katere so večinoma še v razvojnih ali preizkusnih fazah, imajo pa izjemen potencial, tako pri verifikaciji kot, kar je pri preprečevanju terorizma še bolj pomembno, identifikaciji.

6.1 OBRAZNA PREPOZNAVA

Obrazna prepoznavna ima številne prednosti in tudi številne pomanjkljivosti, zato tudi ni čudno, da v strokovni in laični javnosti poteka pravi boj med zagovorniki in nasprotniki uvajanja obrazne prepoznavne v uporabo.⁴⁸

6.1.1 Princip delovanja

Princip delovanja obrazne prepoznavne oz. sistemov obrazne prepoznavne temelji na splošnem štiristopenjskem postopku, ki je v osnovi enak za vse biometrične sisteme. Razlike nastopijo v fazi zajema in vzorčenja, kar pa je značilno tudi za druge biometrične sisteme.

Slika 6.2: Grafični prikaz poteka obrazne prepoznavne



Vir: Woodward et al (2003: 8).

⁴⁸ Gre predvsem za ljudi, ki so zaposleni v organih pregona, za predstavnike biometrične industrije ter del strokovne javnosti, na eni strani. Na drugi strani, kot nasprotniki, pa se pojavljajo predvsem razne nevladne organizacije (npr. organizacije za civilne svoboščine in zasebnost) ter del strokovne javnosti, večinoma izven področij organov pregona.

Na sliki 6.2 je prikazan poenostavljen prikaz poteka obrazne prepoznavne. Prvi korak vsebuje zajem slike s pomočjo fotoaparata ali kamere. V drugem koraku programska oprema določi obris obraza in ga loči od okolice. V tretjem koraku se nato s pomočjo algoritma določijo značilnosti in se kreira šablona. Četrty korak zajema primerjavo šablone tvorjene v tretjem koraku in že prej tvorjene in shranjene šablone ob registraciji. Pri identifikaciji se šablono primerja z vsemi šablonami, ki so v bazi in se kot rezultat izpiše kako 'podobni' sta si šabloni. Pri verifikaciji pa se na novo tvorjeno šablono primerja le z eno šablono. Peti korak določi ali so odstotki doseženi v četrtem koraku dovolj visoki za potrditev ali ne, na podlagi česar nato sistem sprejme odločitev, npr. dostop omogočen/zavrnjen (Woodward et al, 2003: 8, 9).

Obstaja več tipov tehnologij obrazne prepoznavne, od katerih lahko vsaka deluje bolje v določenih okoliščinah. Nekatere so zelo občutljive na svetlobne pogoje, nekatere na temperaturne, ena pa ima celo sposobnost učenja. Vsaka predstavlja svojo rešitev v dani situaciji. Glede na to se danes uporablja pet različnih načinov (Chirillo in Blaul, 2003: 56-58; 1999 Glossary of Biometric Terms, 1999: 9, 10), ki tvorijo tretji korak obrazne prepoznavne, vendar bistveno določajo lastnosti sistema obrazne prepoznavne. To so:

- **'Eigenface':** T.i. eigenface v bistvu pomeni 'lasten oz. svoj obraz' in uporablja dvodimenzionalne slike, ki predstavljajo razločevalne značilnosti. Eigenface so razvili in patentirali v MIT - Massachusetts Institute of Technology (Smart Computing Encyclopedia, 2005). T.i. Eigenhead pa predstavlja tridimenzionalno verzijo Eigenfacea in analizira tudi obliko glave (1999 Glossary of Biometric Terms, 1999: 9) ter ima zaradi tega precejšen potencial povečanja točnosti.
- **Toplotni (Thermal):** Obstajata dve obliki toplotne obrazne prepoznavne. Ena je z uporabo toplotnih kamer za zaznavo vzorcev krvnih žil, ki se nahajajo pod kožo, na podlagi česar se naredi šablona. To je način, na katerega se loči celo identične dvojčke. Druga oblika pa za zaznavo vzorca toplote uporablja infrardečo kamero. Ta oblika je občutljiva na spremembe v stanju človeka in okolice (Chirillo in Blaul, 2003: 56-57).
- **Analiza lokalnih značilnosti (Local feature analysis):** "Pri obrazni prepoznavi (v načinu analize lokalnih značilnosti op. M. A.) deluje sistem na principu pozicioniranja značilnosti znotraj mreže, npr. položaj oči, nosu, ušes,

ust, brazgotin, ipd. Po končanem postopku oz. procesu lahko na osnovi vsote številnih karakteristik, ki so vpletene v mrežni sistem, le-ta istovetnost potrdi ali zavrže. Večina sistemov uporablja črno-belo video kamero, s katero se posname osebo” (Trapečar, 2003: 79). Danes je to najširše uporabljan način obrazne prepoznave, ki ima zmožnost prilagoditi se nekaterim spremembam pri izrazu in staranju (Chirillo in Blaul, 2003: 57).

- **Avtomatsko predelovanje obraza (Automatic face processing):** Ta način uporablja razdalje in razmerja razdalj med glavnimi obraznimi značilnostmi, kot so oči, nos in usta ter velja za najšibkejšo možnost, lahko pa deluje bolje v okoliščinah pri majhni osvetlitvi s frontalnim zajemom (Chirillo in Blaul, 2003: 57-58).
- **Živčna mreža (Neural network):** Gre za način, ki se je sposoben do določene mere celo učiti in predvidevati možne spremembe.

Tako kot pri vsakem biometričnem sistemu se tudi sistem prepoznave obraza nahaja v nekih okoliščinah, ki v pomembni meri vplivajo na njegovo uspešnost. Okoliščine,⁴⁹ ki vplivajo na uspešnost sistema obrazne prepoznave sem razdelil na spremembe okoliščin, ki so odvisne od osebe (sprememba frizure, očala, poraščenost, plastična operacija, spremembe razpoloženja idr.) ter spremembe okoliščin, ki so odvisne od okolja (osvetljenost, ozadje idr.), v katerem je slika zajeta. Glede na okolje zajema, se le-to deli na kontrolirano (ponavadi v notranjih prostorih) in nekontrolirano (običajno nekje zunaj) okolje. V kontroliranem okolju so oz. bi morali biti pogoji vseskozi čim manj spremenljivi. Gre tako za barvo ozadja, osvetlitev, kot (tako horizontalni kot vertikalni) za sodelovanje posameznika in razdaljo zajema. Precej težji so pogoji v nekontroliranem okolju, npr. nadzorna kamera na ulici. Kot vemo, smo v takih pogojih priča spreminjajoči se osvetlitvi, nesodelovanju posameznikov, pogosto neustreznim kotom zajema, prekrivanju obraza, maskiranju idr. Glede na opisano je povsem na mestu ugotovitev, da “sistem (obrazne prepoznave op. M.A.) deluje najbolje, ko so okoljski dejavniki kot npr. kot kamere, osvetljava in obrazni izraz kontrolirani do največje možne mere” (Woodward, 2001b: 12) ter je prisotno sodelovanje posameznika.

⁴⁹ Te okoliščine imajo precej drugačen vpliv na opisane različne načine zajema. Tako je npr. toplotna kamera skoraj povsem neodvisna za kakršne koli spremembe, na ostale pa imajo spremembe okoliščin različno velike vplive.

Načeloma lahko za zajem biometričnega vzorca uporabimo vsak fotografski aparat, skener (Matyas in Riha, 1999: 22) ali video kamero.⁵⁰ Na splošno velja, da višja kot je ločljivost, natančnejši so rezultati (ibidem).

Sistem obrazne prepoznavne ne zahteva kontakta z osebo in se ga lahko preslepi s sliko, če ni uporabljen noben protiukrep (Matyas in Riha, 1999: 23). Tak protiukrep predstavlja predvsem t.i. 'test živosti' (liveness detection test), ki zahteva npr. nasmeh ali, da se pomežikne (ibidem).

6.1.2 Splošne značilnosti

Za biometrično metodo prepoznave obraza je značilno, da je to praktično edina biometrična metoda, ki omogoča (kar seveda ni tako preprosto in ima številne pomanjkljivosti ter omejitve) prepoznavo 'na daljavo'. "Obrazna prepoznavna je najprimernejša ker deluje z razdalje, v množici in v realnem času ter brez sodelovanja subjekta" (Protecting civilization from the faces of terror, 2001: 2). In, če imamo v mislih, da je verjetno najlažje dostopni biometrični element prav obraz, kar je zelo pomembno pri prepoznavi teroristov, postane jasno, da jo zaradi teh svojih značilnosti večina avtorjev tako pri preprečevanju terorizma kot tudi pri drugih varnostnih aplikacijah postavlja na prvo mesto. Ali kot pravi Woodward (2001b: 10), "sistemi obrazne prepoznavne omogočajo oz. bodo omogočali identifikacijo osumljenih ali poznanih teroristov celo v primeru, ko je edina identifikacijska informacija, ki jo imamo, fotografija". O (prevelikem?) optimizmu avtorja v nadaljevanju.

To dejstvo, ki ima velik potencial pri preprečevanju terorizma, je izrednega pomena, saj je pri večini teroristov to eden redkih, če ne celo edini biometrični podatek, ki je kolikor toliko dostopen (npr. preko obveščevalcev na terenu, nadzornih kamer, satelitskih posnetkov(?)).

Zaradi izjemne pomembnosti za praktično preverjanje uspešnosti sistemov obrazne prepoznavne v najrazličnejših okoliščinah bom na kratko predstavil FRVT (Face Recognition Vendor Test) 2002⁵¹ povzet po Phillips et al (2003: 1-14). V njem so kot sponzor oz. podpornik sodelovale tudi vladne službe in agencije, inštituti idr.

⁵⁰ Ki ima zadovoljivo resolucijo.

⁵¹ Predhodnika FRVT 2002 sta bila FRVT 2000 in FERET (Facial Recognition Technology Evaluation). V pripravi oz. zbiranju interesentov pa poteka že FRVT 2005 (www.frvt.org/FRVT2005/).

kot npr. DARPA (The Defense Advanced Research Projects Agency), FBI (Federal Bureau of Investigation), NIST (National Institute of Standards and Technology), DEA (Drug Enforcement Administration), Department of State, INS (Immigration and Naturalization Service), Australian Customs, Canadian Passport Office, UK Biometric Working Group idr. Je neodvisen ocenjevalni tehnološki test zrelih sistemov obrazne prepoznavne, v katerem je sodelovalo deset komercialnih podjetij. Testiranja so potekala na podlagi 121.589 obraznih slik 37.437 posameznikov, ki so bili vzeti iz arhiva za mehiške nepriseljenske vize Ministrstva za zunanje zadeve ZDA.

Zaradi precejšnje obsežnosti bom predstavil le najpomembnejše zaključke in dognanja tega testa:

- obrazna prepoznavna v notranjih prostorih se je znatno izboljšala v primerjavi s FRVT 2000;⁵²
- obrazna prepoznavna se slabša glede na starost slik v podatkovni bazi pribl. 5 % letno;
- boljši sistemi obrazne prepoznavne niso občutljivi na normalne spremembe v svetlobi v notranjih prostorih;
- sistemi, ki uporabljajo tridimenzionalni način, bistveno izboljšajo zmožnost prepoznavne pri nefrontalnih posnetkih;
- ni bistvene razlike v uspešnosti med sliko in video posnetkom;
- moške je lažje prepoznati kot ženske;
- mlajše ljudi je težje prepoznati kot starejše;
- uspešnost obrazne prepoznavne zunaj je potrebno izboljšati;⁵³
- učinek identifikacije in iskanja po 'listah iskanih' se zmanjšuje linearno z logaritmom podatkovne baze ali 'liste iskanih'. (Phillips et al, 2003: 13, 14).

Brez da bi želel delati reklamo za potencialne uvajalce sistemov obrazne prepoznavne omenjam, da so se na testu najbolje odrezali sistemi proizvajalcev Cognitec, Identix in Eyematic, razlike med proizvajalci pa so bile zelo velike

Menim, da sta za zaključek tega poglavja primerna naslednja citata, s katerima se v veliki meri strinjam. "Kljub temu, da obrazna prepoznavna ni popolna tehnologija, ne smemo dopustiti, da popolno postane sovražnik dobrega. Celoten izziv je narediti jo boljšo" (Woodward, 2001b: 12). "Prihodnost obrazne prepoznavne je pozitivna" (Buskey, 2001: 6).

⁵² Precej upanja dajejo takšne in podobne izboljšave, ki so se zgodile le v dveh letih.

⁵³ Prepoznavna najboljših sistemov slik posnetih zunaj je bila zgolj 50% ob 1% FAR.

Prednosti⁵⁴ metode obrazne prepoznavne so predvsem nevsiljivost metode z zajemom brez fizičnega kontakta, enostavna uporaba, zajem na razdaljo, tako verifikacija kot identifikacija, možnost prikritega zajema in dejstvo, da ni človeka, ki ne bi mogel biti zajet z obrazno prepoznavo (vsi imamo obraz).

Slabosti obrazne prepoznavne pa so predvsem problem zajema v nekontroliranih okoliščinah, točnost je relativno nizka, sprememba obraznih značilnosti s staranjem, možnost (precej enostavnega) maskiranja, potrebne so visoko kvalitetne kamere, nezmožnost razlikovanja med enojajčnimi dvojčki in tudi odpor in strah nekaterih pred nadzorovanjem, ki se ga pri biometričnih metodah pogosto enači s sistemi obrazne prepoznavne.

6.2 PRSTNI ODTISI

Prstni odtisi nedvomno zasedajo posebno mesto med biometričnimi metodami, o čemer govori več dejstev:

- S sistemom AFIS⁵⁵ prvič lahko govorimo o avtomatizirani biometrični metodi.
- Glede na dejstvo, da prstne odtise uporabljajo praktično vsi organi pregona na svetu, so danes baze prstnih odtisov med vsemi biometričnimi podatki daleč največje.⁵⁶
- Daleč največji delež na biometričnem trgu, ki je leta 2004 dosegel 48 % med vsemi biometričnimi tehnologijami⁵⁷ (Biometrics Market and Industry Report 2004-2008, 2005).
- Dolgoletna praksa in množična uporaba prstnih odtisov ter zelo obsežna literatura.

⁵⁴ Prednosti in slabosti povzete po (Trapečar, 2003: 79; Chirillo in Blaul, 2003: 62-64).

⁵⁵ "Danes poznamo in uporabljamo AFIS – računalniški sistem za avtomatsko obdelavo prstnih odtisov, ki drastično reducira čas potreben za pregled celo zelo velike zbirke prstnih odtisov in izdela možnostno listo. V tej aplikaciji (ki je različna od biometrične identitetne verifikacije) sistem išče t.i. individualne značilnosti. Za dobro funkcioniranje sistema AFIS je potrebno zadovoljiti dvema pogojema. Prvi je kvalitetno odvzeti prstni odtis z dobro napravo za odvzem, ter drugi, dobro osnovana baza" (Trapečar in Robek, 2003: 50).

⁵⁶ FBI-jeva kriminalna baza prstnih odtisov zajema 41 milijonov oseb, civilna pa 40 milijonov oseb, čemur se vsak dan povprečno doda 7.000 novih vnosov (Fingerprint Identification, 2005). Slovenski sistem AFIS, ki ga uporablja slovenska policija, vsebuje že preko 100.000 "pretežno oseb osumljenih storitve kaznivih dejanj", ki se povečuje s pribl. 5.000 novimi letnimi vnosi (leta 2002 4.987 oseb) (Trapečar in Vidic, 2004: 180).

⁵⁷ Sledijo prepoznavna obraza (12%), geometrija roke (11%), prepoznavna šarenice (9%) in prepoznavna glasu (6%) (Biometrics Market and Industry Report 2004-2008, 2005).

Vse to pripomore k temu, da so prstni odtisi “verjetno večini ljudi takoj sovpadni z biometrijo, nedvomno tudi zato, ker je za mnoge biometrija sinonim za varnost in identifikacijo, prstni odtisi pa seveda v osnovi pomenijo z zakonom uveljavljeno pozitivno identifikacijo. Moč oziroma uporabnost prstnih odtisov se kaže predvsem v sprejemu, prikladnosti in zanesljivosti” (Trapečar in Robek, 2003: 50).

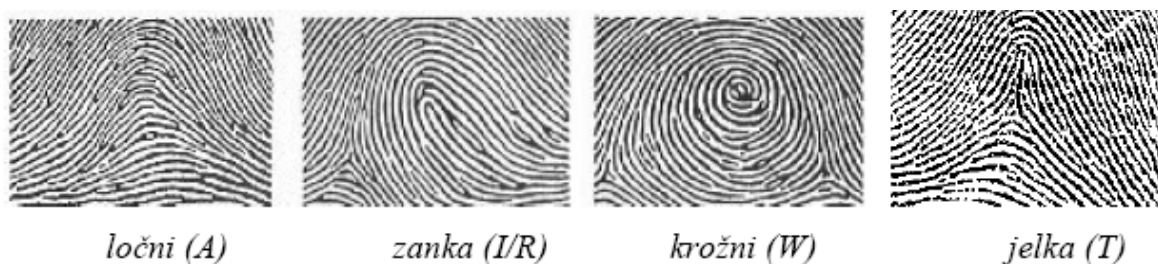
6.2.1 Princip delovanja

“Povrhnjica in usnjica se ne stikata v ravni ploskvi. Usnjica ima brazde in gube, katerim se povrhnjica tesno prilaga. Zato so brazde in gube vidne na površini kože. Razvrstitev in oblika gub sta značilni zlasti na dlaneh in blazinicah prstov. Pri vsakem človeku sta drugačni. Koža na površini prstov, dlani in stopal torej ni gladka, temveč je sestavljena iz ukrivljenih črt. Črte, ki lahko sestavljajo tudi različne vzorce, se imenujejo papilarne linije oziroma kar prstni odtisi” (Trapečar, 2003: 87).

Prstni odtisi so popolnoma razviti pri sedmih mesecih zarodka, kar se ne spreminja skozi življenje z izjemo nesreč, obrabe ipd. (Babler, 1991 v Maltoni et al, 2003: 24).

Vzorci predstavljajo bistvo prstnih odtisov, saj se s pomočjo le teh vrši prepoznavanje. Trapečar in Robek (2003: 50) prepoznavata štiri osnovne vzorce prstnih odtisov (glej sliko 6.3): ločni (arch), zanka (loop), krožni (whorl) in jelka (tented arch).

Slika 6.3: Osnovni vzorci prstnih odtisov



Vir: Trapečar in Robek (2003: 50).

Ter tri najpogostejše individualne značilnosti (glej sliko 6.4), ki so: končujoča linija, vilice in pika (otok).

Slika 6.4: Najpogostejše individualne značilnosti: linija, vilice in pika



Vir: Trapečar in Robek (2003: 50).

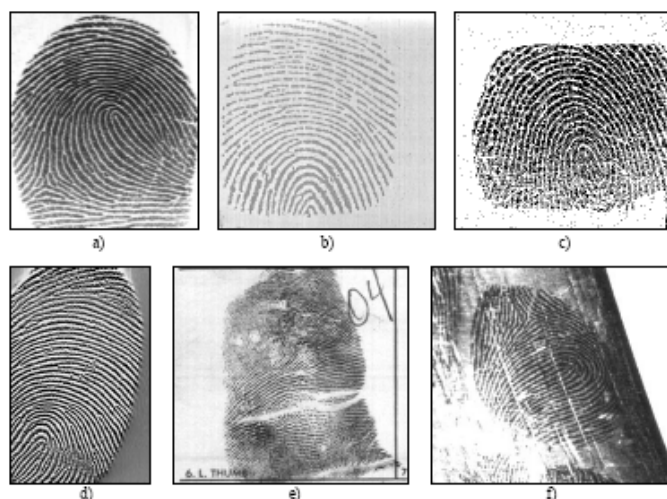
Navedeno je temelj, ki omogoča prepoznavo po prstnih odtisih, tako daktiloskopskih strokovnjakov kot tudi sistemov prepoznave prstnih odtisov.

Odvzem prstnih odtisov je mogoč na več načinov. Tradicionalen način zajema odvzem prstnih odtisov na način, ko se s pomočjo črnila 'povalja' blazinica prsta na papir. Digitalizirano obliko⁵⁸ se nato dobi z uporabo optičnega skenerja ali video kamere visoke resolucije. To je t.i. off-line način (Maltoni et al, 2003: 26).

Drugi način je t.i. live scan, ki se vrši s postavitvijo blazinice prsta na senzor,⁵⁹ ki nato zajame sliko v digitalni obliki (Maltoni et al, 2003: 26).

Zadnji način, ki je izredno pomemben v forenzičnih aplikacijah pa so t.i. latentni prstni odtisi, ki se jih 'vzame' iz neke površine s pomočjo določenih kemičnih tehnik (Maltoni et al, 2003: 26).

Slika 6.5: Slike prstnih odtisov, zajetih na različne načine



Vir: (Maltoni et al, 2003: 27).

⁵⁸ Digitalizacija je pogoj za avtomatizacijo sistema.

⁵⁹ Te senzorji običajno temeljijo na optičnem, silikonskem, toplotnem ali ultrazvočnem principu. Najpogostejši so optični čitalci prstnih odtisov (Matyas in Riha, 1999: 9, 10).

Na sliki 6.5 lahko vidimo na različne načine zajete prstne odtise, pri čemer so slike a, b, c, d zajete z različnimi 'live-scan' senzorji, slika e predstavlja črnilni prstni odtis in slika f latentni prstni odtis.

6.2.2 Splošne značilnosti

“Identifikacijska vrednost daktiloskopije⁶⁰ je zasnovana na dveh znanstveno in mednarodno priznanih dejstvih, to je, da ni dveh oseb s popolnoma enakimi prstnimi odtisi in, da se le-ti ne spremenijo (razen velikosti) od rojstva do razpada trupla” (Trapečar, 2003: 88).

Pri formiranju prstnega odtisa obstaja veliko variacij, tako da je praktično nemogoče, da bi bila dva prstna odtisa popolnoma enaka (Maltoni et al, 2003: 25), kar velja tudi za prste leve in desne roke ter prstne odtise enojajčnih dvojčkov.

Prednosti te metode so:⁶¹ zanesljivost metode, majhna velikost šablone (24B – 1kB), šablone ni potrebno spreminjati, visoka točnost, velika zbirka vzorcev, nevsiljiva metoda, dorečeno klasificiranje in vzorčenje, možnost tako verifikacije kot identifikacije, enostavna uporaba ter velika konkurenca med izdelovalci opreme.

Slabosti te metode pa so (ibidem): metoda je draga, relativno enostavna prevara sistema,⁶² možnost odvzema latentnega prstnega odtisa s čitalca, ne dosega natančnosti kot npr. prepoznavna šarenice.

Če je FRVT najpomembnejši test na področju obrazne prepoznavne je FVC (Fingerprint Verification competition – tekmovanje v verifikaciji prstnih odtisov) to na področju prstnih odtisov. Do sedaj so potekala tri takšna tekmovanja (FVC 2000, FVC 2002 in FVC 2004). Na kratko bom predstavil FVC 2004.

FVC 2004 je ocenjevanje algoritmov za prepoznavo prstnih odtisov. Samo ocenjevanje je potekalo od januarja do aprila 2004 na univerzi v Bologni, na njem pa je sodelovalo 43 družb, akademskih raziskovalnih skupin in samostojnih razvijalcev s 67 algoritmi (Maio et al, 2004). V zvezi z nalogo se mi zdi najpomembnejša ugotovitev rezultatov. Najuspešnejši algoritem je dosegel povprečno vrednost EER

⁶⁰ Daktiloskopija je “/v/eda o kožnem reliefu prstov, dlani in stopal. Jur. primerjanje prstnih odtisov za ugotovitev istovetnosti” (SSKJ, 1994: 113).

⁶¹ Povzeto po (Trapečar 2003: 89; Chirillo in Blaul, 2003: 20,21).

⁶² To je mogoče le pri slabših sistemih brez protiukrepov, npr. z umetnim prstom, prevleko iz lateksa, 'mrtvim' prstom idr. Costello (2002 v Lyon, 2003: 71), poroča, da je Japonski raziskovalec Tsutomu Matsumoto testiral več čitalcev prstnih odtisov, ki jih je preslepil z želatinastimi umetnimi prsti. Prav tako je uporabil latentne prstne odtise, ki jih je vzel iz stekla in jih nato (uspešno) uporabil.

2,07 %, ⁶³ čas potreben za registracijo zgolj 0,08 s, čas potreben za primerjavo 1,48 s ter velikost šablone od 24 kB do 31,5 kB. Najslabši algoritem pa je dosegel EER z vrednostjo samo 37,83 %, ⁶⁴ čas potreben za registracijo 3,72 s, čas potreben za primerjavo 3,81 s ter velikost šablone do 2400 kB (Fingerprint Verification Competition, 2004).

Kot vidimo so razlike ogromne, tako da je potrebno biti ob uvajanju metode preverjanja prstnih odtisov zelo previden pri nameščanju tako strojne kot programske opreme.

6.3 PREPOZNAVA ŠARENICE

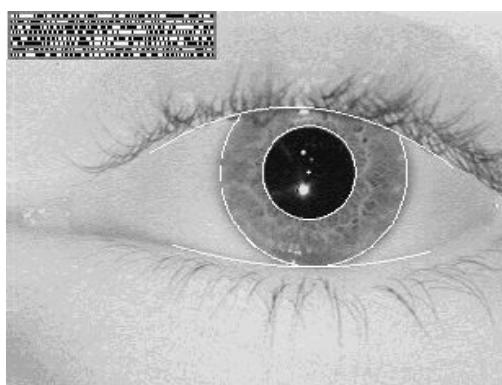
Prepoznavna šarenice ⁶⁵ ima za seboj le kratek razvoj, vendar se vedno bolj uveljavlja kot biometrična metoda prepoznavanja ljudi. Velja za drugo najnatančnejšo biometrično metodo ⁶⁶ (poleg prepoznavanja mrežnice in brez upoštevanja DNA), vendar je od obeh precej cenejša in enostavnejša za uporabo. Tako je povsem na mestu ugotovitev, da “/g/lede na ceno tehnologija šarenice zagotavlja najvišjo stopnjo varnosti” (Chirillo in Blaul, 2003: 101) in je kot taka izredno zanimiva za aplikacije ki zahtevajo zelo visoko stopnjo varnosti.

Slika 6.6: Šarenica



Vir: Vision Based Biometrics – Iris (2005)

Slika 6.7: Lociranje šarenice



Vir: Daugman (2004: 1)

⁶³ Torej je bilo napačnih zavrnitev in napačnih odobritev pribl. dva primera na sto testiranj. Napačno zavrnjen ali napačno odobren je bil povprečno vsak 25 posameznik.

⁶⁴ Pri taki stopnji napake je sistem povsem neuporaben!

⁶⁵ Šarenica je barvasti del žilnice (glej sliko 6.6), ki leži za roženico in daje očesu barvo ter nadzira količino svetlobe, ki vstopa v oko s prilagajanjem velikosti zenice (Cataract and Refractive Eye Care Glossary, 2005).

⁶⁶ Po mnenju Chirillo in Blaul (2003). Toda, kot poroča John Daugman, ki je tudi prvi razvil algoritem za primerjavo šarenice, je v šestih laboratorijskih in terenskih poskusih prepoznavanja šarenice minilo več milijonov poskusov brez napačne prepoznavne ali zavrnitve.

6.3.1 Princip delovanja

“Dober sistem (glej sliko 6.8) ima omrežje s porazdeljeno obdelavo podatkov in strežnikom, vpisno optično enoto ter daljinske postaje z optično-čitalnimi enotami. Oseba mora pogledati v ogledalo naprave, s čimer se avtomatsko sproži fokusiranje očesa in postopek zajema slike šarenice (glej sliko 6.7 op. M.A.). Naprava prav tako tudi z zvočnim signalom obvešča uporabnika o pravilni oddaljenosti od enote (na razdalji med 7 in 25 cm⁶⁷ od optičnega čitalnika). Zajeta slika se pretvori v digitalno obliko ter obdela in shrani v podatkovni bazi na strežniku. Če se zajeta slika šarenice ujema z veljavno kodo v bazi (hitrost prepoznave med 1 in 2 s), sledi sporočilni rezultat o prepoznavi oziroma zavrnitvi” (Trapečar in Robek, 2003: 52).

Slika 6.8: Sistem za analizo šareničnega vzorca



Vir: Trapečar in Robek (2003: 52).

6.3.2 splošne značilnosti

“Tako kot pri mrežnici in prstnih odtisih, tudi za šarenico velja, da je vsak vzorec šarenice edinstven, toda za razliko od prstnih odtisov, vzorec šarenice zajema veliko

⁶⁷ Še veliko večji potencial bi imela prepoznavna šarenice, če bi lahko delovala na večje razdalje. To zaenkrat tehnologija (še) ne dopušča, vendar Iridian Technologies ponujajo optične čitalnike za zajem šarenice, ki le-to zajamejo na razdalji od 25–60 cm (Walkup Iris Cameras, 2005), kar je že določen napredek, vendar še predvsem za enostavnost uporabe.

več edinstvenih podatkov” (Chirillo in Blaul, 2003: 97) kar posledično omogoča tudi višje stopnje točnosti.

Za tehnologijo šareničnega vzorca je značilna tudi zelo velika hitrost iskanja po podatkovnih bazah. V nekaterih implementacijah je lahko ta hitrost tudi do 100.000 primerjav vzorcev na sekundo (Daugman, 2004: 10), kar je ogromna prednost pri identifikaciji, ki ima za podlago zelo veliko podatkovno bazo in je potrebna prepoznavna v t.i. realnem času.

Prednosti⁶⁸ prepoznavne šarenice so predvsem zelo visoka točnost, zelo hiter postopek, možnost tako verifikacije kot identifikacije, majhna velikost šablone, šablone ni potrebno spreminjati, saj je vzorec edinstven in relativno stabilen, razlikovanje tudi enojajčnih dvojčkov, zelo težka ponareditev vzorca ali preslepitev sistema.

Slabosti prepoznavne šarenice pa so vsiljivost metode, nujno potrebno sodelovanje posameznika s sistemom, ni večjih zbirk podatkov šarenic, možnost 'videnja' določenih bolezni, nekateri posamezniki te metode zaradi bolezni ne morejo uporabljati, poleg tega pa je metoda še relativno draga.

6.4 MULTIMODALNE BIOMETRIČNE METODE

“Ne obstaja nobena popolna biometrična metoda, ki bi bila uporabna v vseh primerih. Vsi biometrični sistemi imajo svoje prednosti in slabosti” (Podio in Dunn, 2005: 4). Prav to je temeljno 'gonilo' razvoja in uporabe multimodalnih biometričnih metod, ki v veliki meri odpravljajo pomanjkljivosti, ki se pokažejo ob uporabi le ene biometrične metode. “Ker biometrični sistemi, ki temeljijo zgolj na enem biometričnem podatku, ne dosegajo vedno zahtev uspešnosti delovanja, je razvoj sistemov, ki združujejo dve ali več biometrij postal trend” (Rhodes, 2003: 13). Vsaka biometrična metoda ima pomanjkljivosti, zato se je izkazalo, da ni nobena biometrična metoda najprimernejša v vseh pogledih.

Zato se sedaj podjetja, vladne agencije in raziskovalne ustanove trudijo odpraviti te pomanjkljivosti z združevanjem biometričnih metod v sistem, ki bo fleksibilen, točen in praktično neprevarljiv – to so t.i. multimodalni biometrični sistemi (Jonietz, 2004: 20).

⁶⁸ Prednosti in slabosti povzete po (Trapečar 2003: 79; Chirillo in Blaul, 2003: 62-64).

Poleg multimodalnih biometričnih metod in sistemov je prisoten tudi pojem multibiometrične metode. Zaradi predstavljenih pomanjkljivosti "vsi, ki razvijajo biometrične metode izhajajo iz predpostavke, da je treba uporabljati vsaj dve metodi hkrati. Multibiometrični sistemi oziroma sistemi, ki uporabljajo multibiometrične metode, omogočajo dokaj veliko zanesljivost" (Črnčec, 2004a: 21). 1999 Glossary of Biometric Terms (1999: 6) opredeli multibiometrični sistem kot "biometrični sistem, ki vključuje več kot en biometrični sistem ali biometrično tehnologijo".

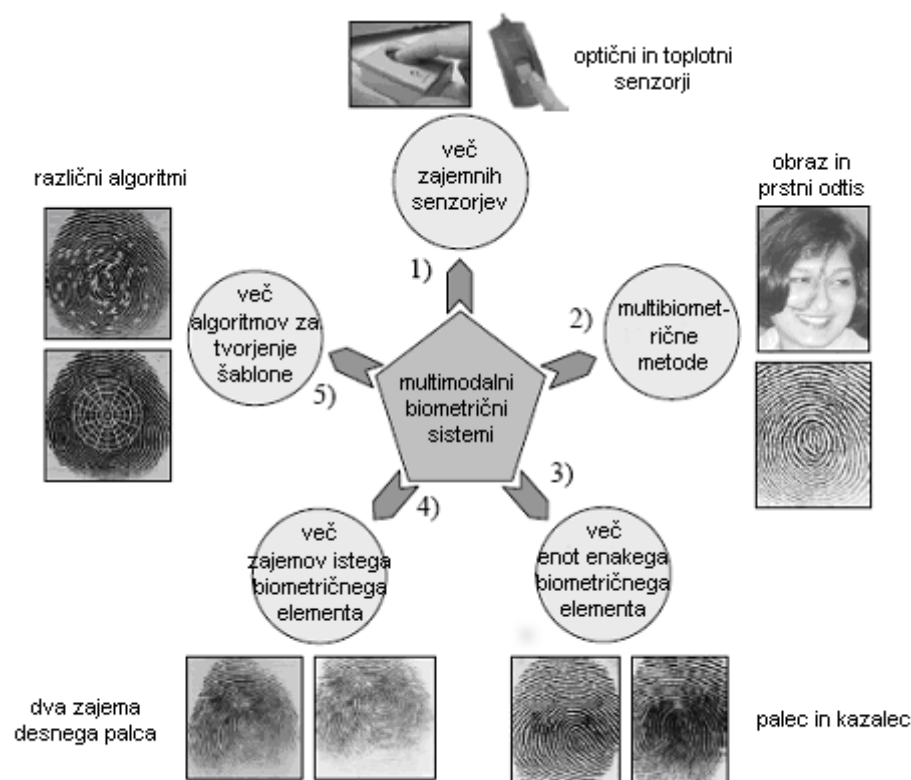
6.4.1 Princip delovanja

Multimodalni biometrični sistemi lahko delujejo v enem od naslednjih petih scenarijev (glej sliko 6.9):

- Več zajemnih senzorjev: biometrična informacija je vzeta iz različnih senzorjev (npr. iz optičnega in toplotnega senzorja).
- Več biometričnih metod oz. multibiometrične metode: zajete so značilnosti več kot enega biometričnega elementa (npr. prstnega odtisa in obraza). Za sistem verifikacije je ta način uveden zaradi povečanja točnosti sistema, pri sistemu identifikacije pa poleg tega še za povečanje hitrosti (npr. s pomočjo obrazne prepoznave, ki je hitra, zmanjšamo število možnih zadetkov, ki ga nato določi prstni odtis).
- Več enot enakega biometričnega elementa: npr. kombiniranje dveh ali več prstov za prstne odtise.
- Več zajemov istega biometričnega elementa: več kot en zajem istega biometričnega elementa je uporabljen za registracijo in/ali prepoznavo.⁶⁹
- Več algoritmov za tvorjenje šablone: ta način vsebuje kombiniranje različnih pristopov k ekstrakciji značilnosti in primerjanju biometričnih značilnosti. To je lahko uporabljeno v dveh primerih. Za verifikacijo ali identifikacijo. Sistem lahko uporabi takšno kombinacijo za odločitev prepoznave (Jain, Ross in Prabhakar, 2004: 21, 22).

⁶⁹ Npr. na podlagi več meritev geometrije roke je izdelana povprečna vrednost značilnosti.

Slika 6.9: Različni primeri delovanja multimodalnega biometričnega sistema



Vir: Jain, Ross in Prabhakar (2004: 22).

Teoretično in tudi praktično je moč združiti dva ali več (lahko tudi vseh pet) predstavljenih načinov, vendar pa je vprašljiva 'dodana vrednost' takšnega združevanja.

Glede na predstavljeno opredelitev bom v nadaljevanju kot multimodalni biometrični sistem razumel sistem, ki deluje na enega od naštetih petih načinov, kot multibiometrični sistem pa le drugi način oz. po že omenjeni prirejeni definiciji: multibiometrični sistem je biometrični sistem, ki vključuje več kot eno biometrično metodo oz. multibiometrična metoda je biometrična metoda, ki vsebuje več kot eno biometrično metodo.

6.4.2 Splošne značilnosti

Prvi primer komercialne programske opreme za multimodalne biometrične metode je bil narejen v Nemčiji (podjetje Human Scan) in uporablja obrazno prepoznavo, glasovno prepoznavo in gibanje ustnic za identifikacijo ljudi (Jonietz, 2004).

“Ministrstvo za domovinsko varnost (DHS – Department of homeland security) sponzorira več laboratorijskih raziskav, ki so že privedle do prototipov, ki združujejo tri, štiri ali celo več biometričnih metod” (Jonietz, 2004), čeprav avtor tega ne navaja gre po mojem mnenju za program Human ID, ki bo podrobneje opisan v nadaljevanju.

“Združevanje biometričnih metod je odločilno za resnično zanesljive identifikacijske sisteme” (Jonietz, 2004). Za multimodalne biometrične sisteme se pričakuje, da so zanesljivejši in točnejši ter, da imajo na razpolago več (precej) neodvisnih 'koščkov dokazov' (Ross in Jain, 2004: 1221). Praktično vsi se strinjajo o tem, toda praktičnih preizkusov je bilo narejeno bolj malo. Eno izjem predstavlja študija združevanja obrazne in šarenične prepoznavave avtorjev Wang, Tan in Jain (2003: 1-8). Ugotavljajo, da je pomen združevanja obrazne in šarenične prepoznavave več kot zgolj izboljšanje točnosti. Povečanje vzorca ljudi, ki so lahko zajeti, in zmanjševanje napak pri registraciji so dodatni razlogi za združevanje obraza in šarenice za verifikacijo.

Obstaja tudi več drugih opisanih združevanj biometričnih metod kot npr. združevanje obraza in glasu, obraza in prstnih odtisov, geometrije roke in odtisa dlani, glasu, premikanja ustnic ter obraza idr. (Jain, Ross in Prabhakar, 2004: 23).

Prikladnost in stroški ostajata največji oviri za uporabo multimodalnih biometričnih sistemov v civilnih aplikacijah. Predvidevamo, da bodo aplikacije z zahtevano visoko varnostjo in biometrični sistemi z velikimi podatkovnimi bazami vedno bolj uporabljale multimodalne biometrične sisteme, medtem ko bodo nizko cenovne komercialne aplikacije verjetno še naprej uporabljale unimodalne biometrične sisteme (Jain, Ross in Prabhakar, 2004: 23).

6.5 PRIMERJAVA BIOMETRIČNIH METOD PO DOLOČENIH KARAKTERISTIKAH

To poglavje sem namenil poenostavljeni primerjavi različnih biometričnih metod (tudi tistih, ki jih v tem poglavju nisem opisoval), da bi omogočil lažji pregled nad značilnostmi določenih biometričnih metod in tako tudi boljši osnovni pregled na tem področju. Predstavil bom “sedem vodilnih biometričnih metod” (Rhodes, 2003: 7). Te so: obrazna prepoznavna, prepoznavna prstnih odtisov, prepoznavna šarenice, prepoznavna podpisa, prepoznavna govora, prepoznavna mrežnice in geometrija roke

(ibidem). Te metode so identične tudi s tabelami (združene v tabelo 6.1) značilnosti, ki jih je predstavil Fefer (2004: 153).

Tabela 6.1: Karakteristike biometričnih tehnologij

Biometrična metoda:	Verifikacija (V)/ Identifikacija (I)	Velikost šablone	Točnost, ki jo navajajo P: proizvajalci, LAB: laboratoriji	Zahtevnost uporabe	Sprejetost s strani uporabnikov	Morebitne ovire za uspešen proces V/I
Prstni odtis	V,I	24B-1kB	Visoka P: FAR=0,1%, FRR=1% LAB: FAR pribl. 1%	Srednja	Srednja	Pribl. 5% ljudi ima neprimeren prstni odtis Optični čitalnik: prah in maščobe Silikonski čitalnik: vlaga
Geometrija roke	V	9B	Nižja P: EER=0,1% LAB: FAR pribl. 3%, FRR pribl. 10%	Nizka	Srednja	Bolezni (artritis, revmatizem)
Očesna mrežnica	V,I	96B	Zelo visoka P: EER = 0,00001%	Visoka	Nizka	Ni znanih omejitev
Očesna šarenica	V,I	256B	Zelo visoka P: EER = 0,00008% LAB: takšno točnost v realnosti težko doseči	Visoka	Srednja	Očala
Človeški obraz	V,I (?)	3-5kB	Nižja P: EER = 1% LAB: točnost v realnosti veliko nižja	Nizka	Visoka	Osvetljenost objekta zaznavanja Sprememba pričeske, brade, brk Očala
Človeški glas	V,I (?)	2-5kB	Srednja P: EER = 1,7% LAB: FAR prib. 0,9%, FRR prib. 4,3%	Nizka	Visoka	Šum v ozadju Prehlad Čustveno stanje uporabnika
Podpis uporabnika	V,I (?)	90B	Nižja P: EER = 2% LAB: točnost v realnosti veliko nižja	Srednja	Zelo visoka	'Enostavni' podpisi Nestabilnost vzorca nepismenost

Vir: Prirejeno po Fefer (2004: 153).

7. PODROČJA UPORABE BIOMETRIČNIH METOD

“Področje uporabe biometričnih tehnologij je zelo široko. Vsaka situacija, kjer interakcija med uporabnikom in procesom zahteva preverjanje identitete tega uporabnika, napeljuje k odločanju za vgraditev naprave, ki temelji na biometrični

tehnologiji. Sistemi varovanja in pristopne kontrole v poslovnih objektih, inštitutih, na državnih mejah, v zaporih, pri nadzoru javnih prostorov - letališč, stadionov, ulic, uporaba na področju kriminalistike, nadzora pooblaščenega dostopa do računalnika in računalniške mreže, ugotavljanje časa prisotnosti zaposlenih ... - vse to so področja, kjer se biometrične metode že uporabljajo, v prihodnosti pa se bodo področja uporabe še širila in dopolnjevala" (Fefer, 2004: 150).

Vlogo biometrije pri varnostnih vprašanjih je svet direktorjev IBIA (International Biometric Industry Association – mednarodno združenje biometrične industrije) takoj po 11. septembru 2001 videl kot (Biometrics and Counter-Terrorism, 2001):

- 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 učinkovite fizične kontrole dostopa;
- preprečitvijo nepooblaščenega dostopa do občutljivih informacij in podatkov ter
- zaščito nacionalne komunikacijske infrastrukture.

"Biometrične metode so bile uporabljene v večih zveznih aplikacijah, ki vključujejo dostop do objektov in računalnikov, identifikacije kriminalcev in varnosti na mejah. V zadnjih dveh letih (2001-2003 op. M.A) so bili sprejeti zakoni, ki zahtevajo povečano uporabo biometričnih tehnologij v zvezni vladi" (Rhodes, 2003: 13). Nadalje jih našteva:

- Kontrola dostopa: za dostop do več kot pol jedrskih tovarn v ZDA se uporabljajo biometrični sistemi idr.
- Identifikacija kriminalcev: npr. FBI-jev sistem IAFIS (Integrated Automated Fingerprint Identification System) idr.
- Mejna varnost: za avtorizirane potnike in njihov lažji prestop meje program INSPASS (INS passenger accelerated service system) kot pilotni program v uporabi že od 1993, US-VISIT delujoč od 2004 idr. (Rhodes, 2003: 13-17).

“Odločitev za uporabo biometričnih metod mora upoštevati stroške in koristi takega sistema in njegov potencialni vpliv na prikladnost in zasebnost” (Rhodes, 2003: 17-18).

“Pričakovano je, da bodo biometrične metode vključene v rešitve za zagotavljanje domovinske varnosti vključujoč aplikacije za izboljšanje letalske varnosti, krepitev nacionalnih meja, v potovalnih dokumentih, vizah in preprečevanju kraje identitet” (What Are Biometrics?, 2005).

Jain, Ross in Prabhakar (2004: 12) razlikujejo tri glavne skupine aplikacij biometričnih metod:

- Poslovne aplikacije kot so npr. logiranje na računalniško mrežo, elektronska varnost podatkov, e-poslovanje, dostop do interneta, kreditne kartice, fizična kontrola dostopa, mobilni telefoni, zdravstveni podatki, učenje na daljavo idr.
- Vladne aplikacije: kot npr. nacionalna osebna izkaznica,⁷⁰ zapori, vozniška dovoljenja, socialna zavarovanja, izplačila socialnih transferjev, mejna kontrola, kontrola potnih listov idr.
- Forenzične oz. sodno-medicinske aplikacije kot npr. identifikacija trupel, kriminalne preiskave, identifikacija teroristov, določanje starševstva, pogrešani otroci idr.

Woodward (2001b: 4-8) prepoznava tri ključna področja za oviranje terorizma, in sicer:

- nadzor (kontrola) dostopa do občutljivih območij na letališčih,
- preprečevanje identitetne kraje in prevare v uporabi potovalnih dokumentov in
- identificiranje znanih ali osumljenih teroristov.

Kot vidimo, avtorji opisujejo možne uporabe biometričnih metod v praksi kljub temu, da imajo le redki v mislih zgolj preprečevanje terorizma. Glede na vse opisano bom naredil svojo razvrstitev možnih področij, kjer se lahko uporabijo biometrične metode s ciljem preprečevanja terorizma. Tako bom izključil področja civilne uporabe, upošteval pa tista vladna in forenzična področja, ki lahko prispevajo oz. imajo zmožnost prispevati k preprečevanju terorizma. V tem poglavju bom predstavil temo na bolj teoretični ravni (ponekod se seveda tega ne bo mogoče v celoti držati in

⁷⁰ “Osebna izkaznica bi imela globoke in zaskrbljujoče učinke na zasebnost in bi bila kmalu razkrinkana kot še ena maginoteva linija v poskusu zaščite pred terorizmom” (Steinhardt, 2003: 35).

bodo podani tudi praktični primeri), saj (ostale) praktične aplikacije sledijo pri analizi držav v naslednjem poglavju.

7.1 KONTROLA DOSTOPA

Pri kontroli dostopa imam v mislih predvsem kontrolo fizičnega dostopa do 'občutljivih' objektov oz. okolij, za katere je zelo pomembno, da do njih nimajo vstopa neavtorizirane osebe ter da imajo avtorizirane osebe čim enostavnejši in hitrejši dostop.

“Standard EN 50133-1:1999 sistem pristopne kontrole opredeli kot sistem, ki obsega vsa konstrukcijska in organizacijska sredstva, ki skupaj kot celota vršijo nadzor nad pristopom v varovana območje” (Fefer, 2004: 148).

“Naloge sistema pristopne kontrole so:

- krajevno omejevanje vhodov in izhodov,
- časovno omejevanje vhodov in izhodov,
- evidentiranje prihodov in odhodov,
- alarmiranje” (Fefer, 2004: 148).

Vse to so naloge, ki jih v okviru kontrole dostopa lahko uspešno izvajajo biometrični sistemi.

“Začetki biometričnega pristopa k varovanju se izražajo v subjektivnem prepoznavanju ljudi po pooblaščenih osebah, ki se je z razvojem dopolnjevalo z legitimiranjem z identifikacijskimi dokumenti. Pristopna kontrola se je izražala tako, da so ljudje prepoznavali ljudi in preverjali pristnost njihovih osebnih dokumentov” (Fefer, 2004: 148). Tako je bil človek nekakšen biometrični sistem obrazne prepoznavne in drugih človekovih značilnosti. Alternativa biometričnim rešitvam kontrole dostopa so lahko: ljudje, gesla in PIN kode ter razne kartice oz. teoretično lahko tudi vse skupaj. Pomanjkljivosti naštetega so bile že omenjene in prav zaradi pomanjkljivosti, ki jih imajo našteje avtentifikacijske metode ter opisa biometričnih metod, se vsekakor lahko strinjam s Feferjem (2004: 150), ki pravi: “biometrične metode so priznane kot metode, ki zagotavljajo najvišjo stopnjo varnosti v okviru sistema pristopne kontrole”. K temu je veliko pripomogel tudi tehnološki razvoj, ki “omogoča zamenjavo tako pooblaščenih prepoznavalcev kot tudi osebnih dokumentov s sistemi pristopne kontrole, ki zagotavljajo objektivnost varovanja,

napake pa so lahko le rezultat nepooblaščenih vstopov v sistem varovanja” (Fefer, 2004: 148). Torej lahko sklepamo, da so oz. bodo sčasoma biometrične metode v okviru kontrole dostopa v uporabi povsod tam, kjer se zahteva najvišja stopnja varnosti (npr. dostop do jedrskih tovarn, skladišč orožja, podatkovnih baz...). Priča pa smo tudi zanimivemu pojavu, ko se biometrične metode uporablja (in to zelo pogosto) tudi v kontroli dostopa v civilnih aplikacijah (npr. dostop do delovnih mest, računalnikov, jedilnic...), kjer zahtevani nivo varovanja še zdaleč ni tako visok. Uporaba biometričnih metod se “z napredkom tehnologije ter posledično tudi manjšimi stroški nakupa in vzdrževanja vedno bolj širi tudi v okolja z zahtevano nižjo stopnjo varnosti” (Fefer, 2004: 150). Razlog za to vidim predvsem v strmem padanju cen biometričnih sistemov in, poleg varnosti, prikladnosti za uporabo.

Namen vsakega sistema kontrole dostopa je dovoliti dostop avtoriziranim posameznikom in ne zgolj njihovim dokumentom, geslom ipd. do določenih prostorov. To je mogoče doseči zgolj z uporabo biometričnih metod oz. biometričnih sistemov (Spence, 2003: 1).

Kontrola dostopa zahteva zmožnost prepoznave posameznika poleg tega pa omogoča še dostop,⁷¹ odobritev ali zavrnitev dostopa in zmožnost alarmiranja. Za dosego tega so na voljo različni biometrični sistemi (Spence, 2003: 1, 2):

- Samostojni (biometrični) sistemi – gre za sisteme, ki kontrolirajo le ena vrata oz. en dostop in niso povezani. Na njih se izvrši registracija in nato ob vsakem dostopu odvzem biometričnega podatka in njegova primerjava z že prej narejeno šablono ob registraciji.⁷²
- Mrežni (biometrični) sistemi – če je potrebna kontrola večih vrat oz. dostopov bi sicer lahko uporabili za vsak dostop po en samostojni sistem, kar pa je potratno, zamudno in nepotrebno. Zato se v takih primerih uporablja mrežne sisteme, v katerih se čitalce poveže s skupnim centralnim računalnikom, na katerem se shranjujejo tudi vsi potrebni podatki. Mrežni sistemi imajo še eno veliko prednost, saj je dostop možen preko katerega koli čitalca in ne le tistega, na katerem je bila opravljena registracija.⁷³

⁷¹ To je lahko npr. fizična odklenitev vrat, omogočen dostop do podatkovne baze idr.

⁷² V praksi bi tak sistem lahko bil vgrajen npr. v vhodna vrata stanovanja. V sistem bi se registrirali družinski člani, ki bi potem imeli dostop do stanovanja. Sistem bi imel šablone shranjene v spominu in bi jih primerjal z na novo vzetiimi ob prepoznavi.

⁷³ V praksi bi bil lahko tak mrežni sistem uporabljen npr. v jedrski tovarni za dostop do varovanih območij. S tem, da je možno razlikovati tudi več varnostnih stopenj in imajo tako nekateri dostop zgolj do nekaterih območij, drugi do vseh ipd.

- Sistemi pametnih kartic – ti sistemi zagotavljajo še dodatne zmožnosti, saj se na pametno kartico shranijo tako biografski kot biometrični podatki in shranjevanje biometričnih podatkov na samem sistemu ni potrebno, zmanjšajo se stroški in zmanjša se zaskrbljenost zaradi zasebnosti. Tak sistem zahteva t.i. dvojno avtentifikacijo z zahtevo po pravi kartici in pravi osebi.

Samostoječi in mrežni sistem v bistvu delujeta v načinu identifikacije in morata vsakega uporabnika primerjati z vsemi šablonami, kar zna biti za določene biometrične metode, ki imajo višje stopnje napake in veliko število uporabnikov, previsoka ovira.⁷⁴ Glede na to so (še posebej pri velikem številu uporabnikov) najobetavnejši sistemi pametnih kartic, s pomočjo katerih lahko sistem vrši način verifikacije⁷⁵ (eden z enim), kar pripelje do manjših napak. Treba je poudariti, da so to le osnovni tipski modeli sistemov, ki so lahko kombinirani še na veliko različnih načinov in tudi z ostalimi avtentifikacijskimi tehnologijami. Npr. mrežni biometrični sistem, ki zahteva vpis gesla, PIN številke ali 'navadne' kartice, ki sistemu priključuje točno določeno šablono in se nato 'priklicano' primerja le z na novo tvorjeno šablono (verifikacija).

“Vrednotenje delovanja biometričnega sistema v okviru sistema pristopne kontrole se izvaja s proučevanjem naslednjih parametrov:

- karakteristike človeškega biometričnega vzorca,
- točnost sistema,
- robustnost sistema, pri čemer je potrebno preučiti robustnost tehničnega dela sistema, kakor tudi robustnost samega biometričnega vzorca,
- hitrost delovanja sistema,
- kompatibilnost sistema,
- težavnost uporabe sistema,
- psihološki faktor ter
- stroške izbire, nakupa, montaže in vzdrževanja sistema” (Fefer, 2004: 150).

Frost & Sullivan's World biometric report 2002 je prepoznal prepoznavo geometrije roke kot dominantno biometrično tehnologijo za kontrolo dostopa in registracijo delovnega časa (Spence, 2003: 4).

⁷⁴ Izjemo predstavljata predvsem prepoznavo šarenice z izredno majhnimi napakami in izredno hitrim časom potrebnim za primerjavo ter prepoznavo prstnih odtisov.

⁷⁵ “Metoda verifikacije se uporablja predvsem v sistemih pristopne kontrole, katerih namen je preprečiti nepooblaščen vstop v določene prostore poslovnih in drugih varovanih objektov” (Fefer, 2004: 150).

7.2 MEJNA VARNOST

Z mejno varnostjo oz. kontrolo imam v mislih predvsem potovalne dokumente, ki vsebujejo biometrične podatke (potni listi⁷⁶ in vize), ki jih je potrebno predstaviti pristojnim organom (in biometričnemu sistemu) ob vstopu v državo in, kjer se to zdi potrebno, tudi ob izstopu iz države. Ob tem imam v mislih tako kopenske mejne prehode kot tudi letališča in pristanišča.

V svetovnem okviru so na tem področju največ storile ZDA. "Povod za širšo uporabo biometrije na potnih listih je odziv ZDA na teroristične napade, ki so se zgodili 11. septembra 2001. Po terorističnih napadih je tako vlada kot tudi javnost, ki v preteklosti ni bila naklonjena biometrični tehnologiji, izrazila potrebo po boljši in univerzalnejši identifikacijski tehnologiji, kar se je odrazilo v ameriški zakonodaji (Patriot Act, Enhanced Border Security Act), ki zagotavlja ne le boljšo varnost, temveč dosega tudi rezultate z uporabo visoke tehnologije biometričnih naprav na letališčih in imigracijskih uradih" (Colja, 2005: 5).

Mejni varnosti se posveča ogromno pozornosti, v čemer prednjačijo ZDA, zato ni čudno, da tudi najvišji predstavniki administracije predsednika Busha razglašajo, da je "zagotavljanje varnosti naših mej naša prioriteta številka ena" (Powell, 2004: 57). Toda tudi druge države posvečajo varnosti mej izreden pomen.

"Obstaja nekaj tipičnih uporab biometrije v procesu vložitve vloge za potni list ali vizum (Colja, 2005: 29, 30):

1. Prosilčeva biometrična šablona narejena v postopku je lahko primerjana z eno ali večimi podatkovnimi bazami (identifikacija), da se določi ali je prosilec znan kakšnemu drugemu povezanemu sistemu (na primer ima potni list z drugo identiteto, ima kriminalno kartoteko, ima potni list druge države).
2. Kadar prosilec prevzame potni list ali vizo (ali se predstavlja na kakršnem koli nivoju v postopku po tem, ko je bila začetna vloga podana in biometrični podatek zajet), je lahko biometrični podatek ponovno zajet in verificiran napram že zajeti šabloni.

⁷⁶ "Potni list v svoji osnovni funkciji služi kot dokument za prehajanje državne meje ter izkazovanje istovetnosti (identitete) imetnika. Omenjeni funkciji se lahko neovirano izvajata le v primeru, ko izdajatelj dokumenta (država) zagotovi zadostno raven kredibilnosti dokumenta, to je, ko zagotovi dve, za varnost imetnika in ciljnih držav potovanja ključni zadevi: da v samem postopku izdaje potnega lista identiteta prosilca in kasneje imetnika ni vprašljiva in sporna ter, da je potni list izdan s strani za to pristojnega organa in ni ponarejen ali prenaresen" (Colja, 2005: 5). Obe ključni zadevi je moč okrepiti oz. izboljšati z uvedbo biometričnih elementov na sam potni list ali tudi vizo, za katero velja podobno.

3. Identitete zaposlenih, ki delajo na postopkih izdaje biometrične dokumente se lahko verificirajo ter se tako potrdi, da imajo pooblastilo za opravljanje dodeljenih nalog. To lahko vključuje tudi biometrično overovitev dostopa do digitalnega podpisa, do pregleda različnih korakov v postopku izdaje in dovoli zaposlenim opravljati tiste naloge, za katere so odgovorni”.

Glavni namen uvajanja biometričnih potnih listin in viz je seveda povečanje varnosti, predvsem pred terorizmom. O biometričnih potnih listih in vizah pred 11. 9. 2001 ni bilo veliko govora, nato pa so predvsem ZDA pokazale veliko energije in tudi pritiskov v smeri, da bi imel vsak tujec, ki pride v ZDA biometrične potovalne dokumente. Kot je dejal takratni ameriški zunanji minister Powell (2004: 54) na pričanju pred parlamentarnim pravosodnim odborom v Washingtonu 21. aprila 2004 je “/vključitev biometričnih podatkov v mednarodne potovalne dokumente odločilen korak v izboljšanju varnosti za Ameriko”. Prav zaradi tega ZDA izvajajo pritiske in postavljajo roke državam predvsem iz VWP – Visa Waiver Program,⁷⁷ za ostale pa je tako ali tako od leta 2003 za vstop v ZDA pogoj viza, katera vsebuje tudi biometrične podatke prstnih odtisov in obrazne fotografije.⁷⁸

Logika mejne varnosti, če imamo v mislih potovalne dokumente z vključenimi biometričnimi podatki, je torej, da se ob izdaji takšnega dokumenta najprej vzamejo biografski in biometrični podatki, ki se jih preveri po čim več podatkovnih bazah in se glede na to odloči o izdaji le tega. Če je posameznik nato sprejet kot ustrezen za pridobitev takšnega dokumenta, je naslednji razlog uvajanja biometričnih podatkov ta, da se ob prehodu meje zagotovi, da je lastnik tako izdanega potnega lista ali vize res ta, kateremu je bil ta dokument tudi izdan. Pojavlja pa se še ena novost, in sicer, da se pri omejenem času bivanja v tuji državi ne preseže rok le-tega in se zato ob odhodu iz države zabeleži tudi to oz. se ob morebitnem nepravočasnem odhodu na to opozorijo ustrezni organi.

⁷⁷ Gre za program, ki državljanom vključenih držav omogoča turistični ali poslovni obisk ZDA do 90 dni brez vize. Trenutno je v programu 27 držav (Andora, Avstrija, Avstralija, Belgija, Brunej, Danska, Finska, Francija, Nemčija, Islandija, Irska, Italija, Japonska, Liechtenstein, Luksemburg, Monako, Nizozemska, Nova Zelandija, Norveška, Portugalska, San Marino, Singapur, Slovenija, Španija, Švedska, Švica in Velika Britanija) (Visa Waiver Program, 2005).

⁷⁸ 22. 9. 2003 so ZDA začele z uvajanjem programa biometričnih viz (Biometric Visa Program) na petih poskusnih mestih, ki je do 26. 10. 2004 deloval na vseh mestih, kjer se izdajajo vize za ZDA (Powell, 2004: 56).

Teoretično sicer obstaja možnost, da se ponaredijo osebni dokumenti⁷⁹ in, da nekega npr. terorista ni v podatkovnih bazah prstnih odtisov in obrazov ter se takemu posamezniku izdajo dokumenti, vendar bo za razliko od ostalih dokumentov brez vključenih biometričnih podatkov, ta posameznik za vedno ostal zapisan in najden pod temi podatki, iz česar sledi, da ne bo mogel pridobiti novih dokumentov in bo lahko ob takem poskusu ali ponovnem prehodu meje tudi aretiran. To je bistvena razlika, saj so znani primeri, ko so posamezniki imeli veliko število potnih listov in drugih (lahko ponarejenih ni pa to nujno) dokumentov.

7.3 NADZOR JAVNIH PROSTOROV

Kot je dejal Thomas Seamon, predsednik mednarodnega združenja šefov policije (International Association of Chiefs of Police) se lahko CCTV in tehnologija obrazne prepoznavne izkaže kot zelo učinkovita v prepoznavi iskanih kriminalcev in povratnikov, v iskanju pogrešanih otrok in ostalih ter v ščitenju žensk s pomočjo uveljavljanja sodne prepovedi približevanja (Milone, 2001: 508). Zastavlja pa se vprašanje ali je možno z nadzorom⁸⁰ javnih prostorov tudi preprečevati terorizem.

Pri nadzoru javnih prostorov imam v mislih predvsem nadzorovanje javnih prostorov, ki se izvaja s pomočjo biometrične tehnologije in ima (vsaj) potencial preprečevanja terorizma. Takšno tehnologijo predstavljajo predvsem CCTV sistemi z vgrajeno programsko opremo predvsem prepoznave obraza, čeprav potekajo tudi poskusi prepoznave značilne hoje, drže idr. Kot nadzor javnih prostorov s ciljem preprečevanja terorizma je potekal, kolikor mi je znano, le t.i. program človeške identitete na daljavo ameriškega obrambnega ministrstva. Predstavil bom še dva, sicer s preprečevanjem terorizma ne povsem neposredno povezana primera, vendar v luči tega poglavja zelo zanimiva primera. To sta uporaba sistema obrazne prepoznavne na XXXV finalu ameriškega nogometa (Super Bowl) januarja 2001 in primer uvedbe CCTV kamer v VB.

⁷⁹ Če je posameznik že znan organom pregona kot terorist. Če pa ima posameznik 'čisto kartoteko', potem naj problemov pri izdaji sploh ne bi bilo.

⁸⁰ Nadzor (Surveillance) – vsaka tehnologija taktičnega opazovanja aktivnosti z namenom preprečiti nezakonito ali škodljivo vedenje ali snemanje in dokumentiranje takega dejanja. Tipična nadzorna tehnologija bi bila sistem za video nadzor in arhiviranje (CCTV - Close Circuit Television), digitalne in optične video kamere (Cavoukian, 2002: 6). "Najbolj pogosta je kombinacija s sistemom za video nadzor in arhiviranje (CCTV sistem), ki je namenjen vizualnemu spremljanju ter arhiviranju dogajanja v varovanem objektu" (Fefer, 2004: 149) ali prostoru.

7.3.1 Prepoznavna človeške identitete na daljavo (Human ID)

Human ID je bil le eden od šestnajstih razvojno-raziskovalnih programov TIA (Total Information Awareness Programs, ki so jih nato zaradi pritiskov organizacij za civilne svoboščine in zasebnost ter javnosti preimenovali v Terrorism Information Awareness Programs). Programi so potekali znotraj DARPA (Defence Advanced Research Projects Agency, ki je centralna raziskovalna in razvojna organizacija ministrstva za obrambo ZDA), ki naj bi jih nato (če bi bilo za razvitje primernih vsaj osem od šestnajstih teh programov) združili v enoten sistem TIA (Belasco, 2003). Z vidika biometričnih metod je zanimiv le Human ID. Šlo je za štirileten program (2000 – 2004), toda septembra 2003 se je kongres odločil, da bo končal s financiranjem celotnega TIA programa (Pentagon's 'Terror Information Awareness' program will end, 2003). Tako je bilo konec tudi s Human ID programom in DARPA naj tako ne bi več razvijala programov znotraj TIA in tudi v resnici na spletni strani DARPA ni moč najti več nobenih informacij o TIA ali Human ID. Nekatere obetavne tehnologije pa so se prenesle v druge vladne agencije (ibidem). Glavni razlog ukinitve programa je zajet v besedah senatorja Rona Wydena, ki si je prizadeval za ukinitve programa: “Američani na ameriških tleh ne bodo tarče TIA nadzora, ki bi kršila njihovo zasebnost in civilne svoboščine” (ibidem).

Kljub navedenemu, bom okvirno predstavil za kaj je sploh šlo pri programu Human ID, ker je šlo za zanimiv program preprečevanja terorizma.

“V luči terorističnih napadov na Khobar Towers se je DARPA lotila 50 milijonov dolarjev vredne pobude znane kot 'Human ID at a Distance' (človeška identiteta na daljavo), katere glavna komponenta je obrazna prepoznavna” (Woodward, 2001a: 9,10). Programski vodja programa je bil Jonathon Phillips (Long-distance identification system tested at INSCOM headquarters, 2002: 10), ki je po mnenju Woodward, Higgins in Orlans (2003: 184, 185) “vodilna biometrična avtoriteta”, kar nedvomno nakazuje, da ni šlo za nek obroben program, temveč za program, kateremu se je namenjal najboljši strokovnjaki in tudi veliko denarja.

Kljub temu, da je glavna komponenta obrazna prepoznavna, pa je program temeljil na “razvoju avtomatiziranih multimodalnih biometričnih tehnologij” (Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates, 2003), ki bi poleg prepoznavne obraza, vključevale še prepoznavo šarenice ter prepoznavo značilne hoje oz. drže.

“Ko bodo te posamezne tehnologije razvite, bo Human ID razvil metode za združitev teh tehnologij v napredni sistem identifikacije ljudi. Sistem bo zmožen multimodalne združitve uporabljajoč različne biometrične tehnike z osredotočenjem na identifikacijo telesnih delov, obrazne prepoznave in človeške kinematike”⁸¹ (Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates, 2003).

Te tehnologije bodo priskrbele ključna zgodnja opozorila za zaščito sil in domovinsko obrambo proti terorističnim, kriminalnim in drugim človeško osnovanim grožnjam ter bodo preprečile ali zmanjšale delež uspešnih napadov na objekte obrambnega ministrstva. Metode za združevanje biometričnih tehnologij v napredni sistem identifikacije ljudi bo razvit, da bi omogočil hitrejšo, natančnejšo in neprisiljeno identifikacijo ljudi na velikih razdaljah (Human ID at a Distance, 2005).

Slika 7.10: Grafični prikaz delovanja prepoznave identitete ljudi na daljavo



Vir: Human ID at a Distance (2005).

“Biometrični podatki bodo pridobljeni z različnimi senzorji vključujoč video, infrardeče in multispektralne senzorje (glej sliko 7.10). Cilj tega programa je identifikacija ljudi kot edinstvenih posameznikov (ne nujno po imenu) na daljavo, kadar koli podnevi ali ponoči, v vseh vremenskih okoliščinah, z nekooperativnimi subjekti, verjetno zakrinkanimi ter samih ali v skupini” (Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates, 2003).

⁸¹ Kinematika je nauk o gibanju teles brez upoštevanja sil, ki gibanje povzročajo (SSKJ, 1994: 395).

Kot poroča INSCOM JOURNAL (Long-distance identification system tested at INSCOM headquarters, 2002: 10) je ta precej abstraktni pojem 'na daljavo' "prepoznavajo ljudi na 150 metrov".⁸²

"Ambiciozen cilj DARPA je pomagati razviti biometrične tehnologije, ki bodo lahko uporabljene za identifikacijo znanih teroristov, preden se približajo njihovim tarčam. Na ta način bodo mogoče lahko rešena življenja" (Woodward, 2001a: 9, 10).

Kot vidimo, je šlo za zelo ambiciozen program, ki pa je doživel precej klavrn konec. O stopnji, do katere je bil sistem razvit in njegovi uspešnosti ter učinkovitosti ne morem soditi, ker ni na voljo ustreznih podatkov, ali pa program še ni bil pripeljan do stopnje preizkušanja. Ostaja pa dejstvo, da je šlo za prvi (vsaj meni znan) resnejši poskus razvitja nadzorne tehnologije z vključitvijo biometričnih metod, ki bi omogočal prepoznavo (znanih) teroristov 'na daljavo' v realnem času, kar je bilo vsekakor zelo obetajoče.

7.3.2 XXXV finale ameriškega nogometa (XXXV Super Bowl) januarja 2001

Prvi preizkus delovanja (biometrične) obrazne prepoznavne v realnih okoliščinah na javnem kraju in na velikem vzorcu ljudi se je (po mojem vedenju) zgodil na XXXV. finalu ameriškega nogometa januarja 2001 v Tampi na Floridi, ko so lokalne oblasti preizkusile to metodo. To je tudi razlog, da opisujem te dogodke, saj so zelo zanimivi, poleg tega pa predstavlja ta primer eno od možnosti za biometrične metode v preprečevanju terorizma – nadzor javnih krajev.

"Nadzorne kamere so pregledovale publiko in zajemale slike obiskovalcev. Oblasti so sporočile, da je sistem odkril 19 računalniških zadetkov" (Woodward, 2001a: 10). Namen tega poskusa je bil "prepoznati grožnje javne varnosti" (ibidem).

Zanimivo (ali pa tudi pričakovano) je, da je ta dogodek požel izredno veliko negativnih opažanj. Ne smemo pa pozabiti, da je to čas pred 11. 9. 2001. Po tem datumu je zaslediti precej manj negativnih mnenj o obrazni prepoznavi in njeni implementaciji, preprosto je to dejstvo predvsem posledica 'obsedenega' stanja, strahu in zelo strogih varnostnih ukrepov, katere pa je zaradi 'vojne proti terorizmu' podpirala tudi večina prebivalstva.

⁸² 500 čevljev – en čevlj meri 0,3048 metra.

O uspešnosti sistema (torej ali je bilo 19 prepoznanih posameznikov res tistih, za katere je sistem trdil da so - FAR in koliko posameznikov, ki bi morali biti prepoznani, sistem ni prepoznal - FRR) žal ni mogoče poročati, saj se oblasti niso odločile za aretacijo prepoznanih posameznikov, katere prepoznavo so izvršili preko list iskanih oseb. Je pa res tudi, da tehnologija obrazne prepoznave še danes ne omogoča visokih stopenj točnosti prepoznave v nekontroliranih okoliščinah, stanje pa je bilo v začetku leta 2001 še slabše.

7.3.3 CCTV kamere v Veliki Britaniji

V Veliki Britaniji (VB)⁸³ so CCTV kamere bile in so sredstvo preprečevanja kriminala (ne vključujoč organe pregona) z največjim proračunom. V triletnem obdobju 1999 – 2001 je britanska vlada odobrila 170 milijonov funtov za CCTV v mestih in mestnih središčih, parkiriščih, stanovanjskih območjih in področjih z visoko stopnjo kriminalitete (Welsch in Farrington, 2004: 499). Število CCTV kamer se je povečevalo od leta 1990, ko jih je bilo 100, 1994 – 400, 1997 – 5.200 in leta 2002 že 40.000 (Armitage, 2002 v Welsch in Farrington, 2004: 499). Vidimo lahko, da je trend povečevanja nadzornih sistemov v Veliki Britaniji zelo očiten, dosti drugače pa ni niti v ostalih državah.

Britanska policija je leta 1999 povezala 300 nadzornih kamer s programsko opremo obrazne prepoznave, da bi našli iskane kriminalce (O'Harrow, 2001 v Milone, 2001: 498). Čeprav je bilo prvotno načrtovano iskanje kriminalcev, menim, da se je že zgodila 'nadgradnja' tudi v smeri prepoznave teroristov.

Glavni namen uvajanja CCTV je zmanjševanje kriminala, kar se je pokazalo tudi v praksi. Welsh in Farrington (2004: 513) tako na podlagi različnih empiričnih podatkov v svoji študiji ugotavljata, da CCTV nadzorne kamere "predstavljajo učinkovito sredstvo za zmanjševanja kriminala".

Sedaj se zastavlja pomembno vprašanje v okviru mojega diplomskega dela, torej, ali lahko CCTV sistemi predstavljajo možnost oz. sredstvo preprečevanja terorizma? Logika takšnega načina je v bistvu v tem, da bi poleg CCTV kamer v nadzorne sisteme vgradili še programsko opremo prepoznave obrazne in/ali drugih biometričnih metod primernih za prepoznavo na daljavo in bi se tako identifikacija

⁸³ Primer Velike Britanije je podan zato, ker je tam že sedaj delujočih ogromno število CCTV sistemov in bi bila njihova nadgradnja s programsko opremo prepoznave obraza razmeroma enostavna.

vršila v t.i. realnem času, kar bi v zvezi s preprečevanjem terorizma pomenilo dvojne možnih pridobitev. Prepoznavo teroristov in ukrepanje preden bi le-ta uspel delovati ter tudi samo prepoznavo iskanih teroristov, ki se npr. skrivajo in so iskani v VB. Kot pri programu Human ID, se tudi tu skrivajo številne pomanjkljivosti in problemi, ki so predvsem v velikih težavah uspešne prepoznave na daljavo, neimetja podatkov o vseh teroristih, vprašanju zasebnosti, (ne)odobravanju oz. nasprotovanju javnosti idr.

Moje mnenje je, da razen 'zastraševalne oz. odvračevalne vrednosti', zaradi vseh omenjenih problemov, ni moč pričakovati takšne implikacije te nadzorne tehnologije, vsaj v bližnji prihodnosti oz. vsaj do takrat, ko bo biometrična tehnologija razvita do te mere, da bo sposobna precej uspešnejše delovati v prepoznavi ljudi na daljavo. In tudi pri uresničitvi povečanja točnosti bo uspešnost preprečevanja terorizma na ta način nepopolna, če ne zaradi drugega pa zaradi pomanjkanja podatkov o prav vsakem teroristu.

7.4 PREPREČEVANJE KRAJ IN ZLORAB IDENTITETE

Ugotovimo lahko, da sta potrebna nadaljnji razvoj in raziskovanje v okoliščinah, v katerih bi bile biometrične tehnologije boljše od ostalih tehnologij za zmanjševanje identitetne kraje⁸⁴ z izboljšanjem verifikacije posameznikov udeleženih v finančnih transakcijah (The Use of Technology To Combat Identity Theft, 2005: 6).

Glede na to, da gre pri identitetni kraji predvsem za pridobivanje materialnih koristi, bi šlo lahko pri preprečevanju le-tega v zvezi s terorizmom za preprečevanje možnega financiranja terorizma s pomočjo identitetne kraje ali pa, da se s krajo identitete poštenega državljana 'skrrije' terorist.

Najpogosteje se identitetna kraja oz. zloraba dogaja preko kraje ali neavtorizirane uporabe kreditne ali druge kartice, kraje magnetnega zapisa takih kartic, poosebljanje legitimnega lastnika bančnega računa preko telefona ali svetovnega spleta, računalniško vdiranje v podatkovne baze idr. (The Use of Technology To Combat Identity Theft, 2005: 6).

“Vprašanje o identitetni kraji, terorizmu in biometričnih metodah je sedaj predmet razprav držav kot sta ZDA in Avstralija v njunem povečevanju mejne varnosti”

⁸⁴ Identitetna kraja je polastitev podatkov o identifikaciji posameznika (npr. številka socialnega zavarovanja, številke kreditne kartice idr.) s strani nekega drugega posameznika z namenom zagrešiti prevaro ali krajo (The Use of Technology To Combat Identity Theft, 2005: 6).

(Development of the Biometrics Institute Privacy Code for the Biometrics Industry, 2005). Tu je vidna tudi povezava med mejno varnostjo in krajo identitete, saj kriminalci in teroristi iščejo načine, kako bi prestopali meje pod izmišljenimi ali ukradenimi identitetami, kar bo nedvomno oteženo z vpeljavo biometričnih potovalnih dokumentov.

Samo v ZDA je bilo leta 2003 prijavljenih 215.000 primerov identitetne kraje, kar je 150% povečanje iz leta 2001, ko je bilo takih primerov (le?) 86.212 (The Use of Technology To Combat Identity Theft, 2005: 6). Primer ZDA glede identitetne kraje je eden največjih v svetu, skrb vzbujajoč pa je tudi velik porast takšnih dejanj. Biometrične metode se v tem kontekstu pojavljajo kot ena od tehnologij, ki omogočajo večjo varnost in zanesljivost vzpostavitve zanesljive 'vezi' med dokumentom in njegovim lastnikom, kar lahko zmanjša število identitetnih krajev in zlorab ter ima s tem tudi ugodne širše varnostne implikacije.

8. ANALIZA IZBRANIH PRIMEROV

V sledečem poglavju bom analiziral stanje v Sloveniji, zanimanje, za katero verjetno dodatna pojasnila niso potrebna. Ker pa je Slovenija sedaj del EU in smo določene zakonodajne rešitve primorani sprejeti, bom opisal tudi stanje v EU kot instituciji in ne v posameznih državah EU. V Sloveniji in tudi EU kot instituciji, razen biometričnih potnih listov in viz, nisem zasledil drugih aktivnosti, ki bi vključevale biometrične metode v zvezi s preprečevanjem terorizma. Ker zaradi povezanosti ni možno povsem ločiti Slovenije in EU bo deloma prihajalo do prekrivanja nekaterih podatkov pomembnih za opisovana področja. Nazadnje pa bom predstavil še stanje v ZDA, ker je tam razvoj biometričnih metod s ciljem preprečevanja terorizma daleč največji, ZDA pa vodilna država na tem področju.

8.1 SLOVENIJA

V Sloveniji nisem zasledil veliko aplikacij biometričnih metod s ciljem preprečevanja terorizma. V ta sklop bi pogojno lahko spadal le omenjeni sistem AFIS ter primarno uvajanje biometričnih potnih listov. Zaradi omenjenega bom opisal predvsem stanje na področju uvajanja biometričnih elementov v potne listine RS.

Razloge uvajanja biometričnih potnih listov prepozna Colja (2005: 17-25) predvsem v zahtevah ZDA (zakona USA PATRIOT ACT in Enhanced border security and visa entry reform act of 2002 ter dveh delujočih programov v ZDA US-VISIT in Visa Waiver Program) ter zahtevah EU⁸⁵ z različnimi resolucijami, uredbami idr. Iz navedenega lahko sklepamo, da Slovenija uveljavlja biometrične potne liste predvsem zaradi zahtev drugih držav in ne zaradi lastnega cilja npr. preprečevanja terorizma. Toda to ne pomeni, da uvedba biometričnih potnih listov ne bo imela pozitivnih varnostnih učinkov tudi za Slovenijo.

Najprej je bila zahteva ZDA, da naj začnejo države, ki ne potrebujejo vize za vstop v ZDA (države VWP) izdajati biometrične potne liste do 26. 10. 2004, sicer bo za vstop v ZDA potrebna viza tudi za državljane teh držav. Ta rok se je izkazal za povsem nedosegljiv, kar so spoznali tudi v ameriški administraciji, zato ne čudi poziv takratnega zunanjega ministra Powella, da nobena od večjih držav (isto velja tudi za majhne države op. M.A.) ne bo sposobna ujeti tega roka, zato je glede na okoliščine menil, da bi moral biti skrajni rok prestavljen za dobri dve leti – na 30. november 2006, kar bi zaveznikom ZDA omogočilo razrešiti znanstvene probleme in razviti bolj varne potovalne dokumente. Powell je še menil, da se bodo, če rok ne bo podaljšan, ZDA soočile z resnimi posledicami kot je npr. ocenjeno povečanje za neimigrantske vize za več kot 5 milijonov v fiskalnem letu 2005, kar pomeni 70% porast in bi za posledico imelo tudi veliko gospodarsko škodo za ZDA (Powell, 2004: 55).

Ameriška administracija je torej prosila za več kot dveletni odlog, toda kongres je sprejel le enoletno podaljšanje.⁸⁶ Podaljšanje je vsekakor bilo tudi v interesu ZDA, saj bi se drugače soočili s precejšnjimi nevšečnostmi, pa tudi novi rok bodo verjetno izpolnile le nekatere države. Rok, ki ga sedaj lovijo vse države VWP in tudi Slovenija, je sedaj verjetno dokončno postavljen na 26. 10. 2005.⁸⁷ EU se je na ameriške

⁸⁵ "Slovenija si bo seveda še nadalje prizadevala za čimprejšnjo uvedbo določenih biometričnih elementov v potovalne dokumente, saj bo kot članica EU morala slediti odločitvam sprejetim v okviru le-te, ki pa se aktivno pripravlja na izdajo takih dokumentov tako državljanom tretjih držav (vizum in dovoljenje za prebivanje), kot tudi državljanom EU (potne listine)". Navedeno so zapisali v projekt, ki poteka v okviru MNZ – Uvajanje biometrije na potne listine državljanov RS – stanje projekta in nadaljnji razvoj iz leta 2004, v nadaljevanju Projekt (2004: 2). "Stališča Evropske unije in posledično tudi Slovenije do uporabe biometričnih metod so dokaj podobna ameriškim. V Sloveniji bomo z vstopom v EU dolžni upoštevati skupno politiko na področju uvajanja novih potnih listov z biometričnimi podatki" (Črnčec, 2004a: 21).

⁸⁶ Od dne 30. 9. 2004 so tudi državljani VWP vključeni v program US-VISIT in morajo ob prehodu meje z ZDA 'oddati' dva prstna odtisa in obrazno fotografijo.

⁸⁷ Toda s samo enoletnim podaljšanjem niso bili navdušeni niti v EU. "Države EU niso sposobne do oktobra leta 2005 pričeti z izdajanjem potnih listov z biometričnimi podatki, kot je to zahtevala ZDA. Zato bo EU od Američanov zahtevala podaljšanje tega roka. Tako je 30. 9. 2004 zatrdil evropski

zahteve odzvala z Uredbo Sveta Evropske unije o standardih zaščitnih elementov ter biometrije v potnih listih in potovalnih dokumentih, ki jih izdajajo države članice,⁸⁸ ki ureja implementacijo biometričnih podatkov v potne liste in časovni okvir, v katerem se naj to zgodi (o uredbi podrobneje v nadaljevanju). Pomembno je povedati še to, da je glavna organizacija, ki sprejema standarde na tem področju ICAO. "Tehnične specifikacije se pripravljajo v skladu z že izdelanimi standardi o uvajanju biometrije na potovalne dokumente, ki jih je kot vodilna mednarodna organizacija s področja strojno-berljivih dokumentov pripravila ICAO (International Civil Aviation Organization) – Mednarodna organizacija za civilno letalstvo s sedežem v Kanadi. Zadnja revizija doc 9303 – Part 1, Machine Readable Passports (dokument, ki opredeljuje tehnične specifikacije za strojno-berljiv potni list) je bil maja 2003 – kot peta izdaja" (Colja, 2005: 6).

Sedaj, ko so razlogi uvajanja jasni, se bom posvetil stanju projekta v Sloveniji. Gre za precej kompleksen in zahteven projekt saj "p/oleg same inkorporacije čipa⁸⁹ v obrazec obstoječega potnega lista bo zaradi obvezujoče uredbe EU potrebno spremeniti tudi normativno ureditev, delovne postopke v zvezi z vložitvijo vloge za potni list, pogodbeno razmerja z izdelovalcem slovenskih potnih listov ter postopke mejne kontrole" (Colja, 2005: 36). "Zahtevane novosti bodo vplivale tudi na dopolnitve slovenske normativne ureditve področja potnih listov (zakona,⁹⁰ podzakonskih predpisov⁹¹ in navodil), ki bo omogočila zbiranje, obdelavo in uporabo biometričnih osebnih podatkov,⁹² trajnosti čipa bo potrebno prilagoditi veljavnost dokumenta, razširiti bo potrebno evidence, pooblastila za uporabo podatkov. Spremeniti bo potrebno tudi postopke vložitve vlog, sam obrazec potnega lista, uvesti novo logistiko v proces proizvodnje in personalizacije ter distribucijski proces.

komisar za pravosodje in notranje zadeve Antonio Vitorino, ki se je v Haagu skupaj s pravosodnimi ministri članic EU sestal z ameriškim sekretarjem za pravosodje" (EU ima težave pri biometričnih potnih listih, 2004). Očitno je, da evropski komisar s svojimi zahtevami ni uspel.

⁸⁸ Council Regulation on standards for security features and biometrics on passports and travel documents issued by Member States OJ L 385/1, 29.12.2004.

⁸⁹ Gre za medij, na katerem bodo shranjeni biometrični podatki.

⁹⁰ Zakon o potnih listinah državljanov Republike Slovenije (Uradni list RS, št. 65/00).

⁹¹ Pravilnik o izvajanju Zakona o potnih listinah državljanov Republike Slovenije (Ur, list RS, št 10/01, št. 100/03).

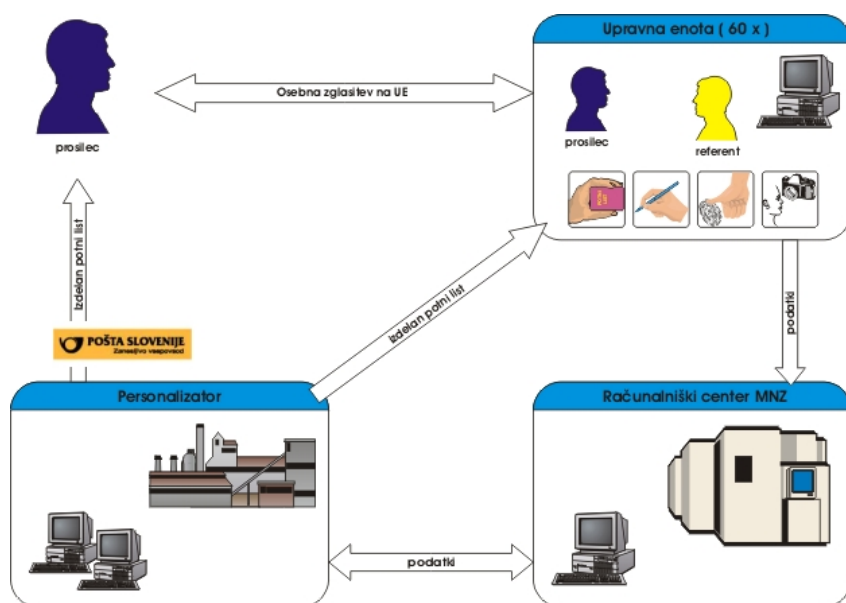
⁹² "V RS bo ob obvezni vključitvi biometrične metode prepoznavanja obraza v potno listino potrebno spreminjati zakonodajo tega področja, pa tudi vsaka druga vključitev opsijskih biometričnih metod (prstnih odtisov, očesne roženice...) pomeni spremembo Zakona o potnih listinah državljanov RS (UR. List RS, št. 65/00), zaradi varovanja osebnih podatkov imetnika potne listine. Ustava RS in Zakon o varstvu osebnih podatkov namreč določata, da se lahko podatki o posamezniku zbirajo, obdelujejo in uporabljajo le na podlagi zakona ali njegove pisne privolitve" (Projekt, 2004: 4).

Pojavile se bodo nove razsežnosti mejne kontrole ob identifikaciji ali verifikaciji posameznikov pri prehajanju državne meje itd. (Colja, 2005: 6, 7).

Pomemben vir informacij o uvajanju biometričnih podatkov v potne liste je že omenjeni projekt v okviru MNZ – Uvajanje biometrije na potne listine državljanov RS. V njem je zapisano, da: "RS aktivno spremlja vsa dogajanja povezana z uvajanjem biometrije v potovalne dokumente (vizum, dovoljenje za prebivanje državljanov tretjih držav, potni list) predvsem zaradi znanih zahtev, ki so jih ZDA leta 2002 postavile skupini 27 držav Visa Waiver Programa (VWP), ki za vstop v ZDA ne potrebujejo vizuma" (Projekt, 2004: 2).

Izdaja potnega lista v RS bo potekala po sledečem postopku (glej sliko 8.11). V prvih 18 mesecih (do sredine leta 2006), ko je edini obvezni biometrični element prepoznavna obraza, bo najprej prosilec zaprosil za nov dokument na upravni enoti (UE), na kateri ima prijavljeno stalno bivališče. Referent na UE bo po identifikaciji prosilca vnesel podatke za izdajo novega potnega lista v centralni računalniški sistem, računalnik bo izpisal vlogo, na katero se bo pritrdila fotografija (katere karakteristike so točno določene s standardom ICAO) in jo bo prosilec podpisal. Referent bo fotografijo in podpis skeniral in ju shranil v računalniškem sistemu k ostalim podatkom prosilca. Fotografija se bo v sistemu procesirala kot biometrični element. Vsi računalniško zajeti podatki se bodo samodejno posredovali v centralni računalnik MNZ (on-line) in nato k proizvajalcu (on-line), ki bo potni list personaliziral, kar pomeni, da bo poleg ostalega shranil tudi biometrični podatek obrazne prepoznavne na brezkontaktni čip. Ko bosta obvezna oba biometrična elementa (začetek leta 2008) bo moral prosilec ob vložitvi vloge za nov dokument, poleg naštetega, položiti še zahtevana prsta na napravo za elektronski zajem prstnih odtisov. V okviru biometrije se bo preverjanje identifikacije imetnika potnega lista lahko izvajalo na način verifikacije in/ali identifikacije, saj se bodo biometrični podatki, ki bodo zajeti ob vlogi shranili v centralnem računalniku Ministrstva za notranje zadeve, proizvajalec pa jih bo moral takoj po personalizaciji izbrisati iz svojega računalniškega sistema (Projekt, 2005: 6), kar bo varnostni ukrep pred morebitnimi zlorabami osebnih podatkov.

Slika 8.11: Delovni postopek izdaje biometričnega potnega lista



Vir: MNZ (Projekt, 2005: 7)

V Projektu (2005, 9) so navedene tudi stroškovne postavke projekta, ki izvirajo iz:

- posodobitve in nabave nove strojne ter programske opreme za zajemna mesta ter njena implementacija,
- posodobitve in ojačitve varnih povezav za prenos podatkov med zajemnim mestom, glavnim računalnikom MNZ ter proizvajalcem listin,
- opreme mejnih prehodov,
- opreme kontrolnih mest za preveritev vsebine čipa na zahtevo imetnika,
- izvedbe pilotskega projekta,
- usposabljanja upravnih enot, diplomatsko konzularnih predstavništev in mejnih kontrolnih organov.

Brez, da bi se spustil v natančno analizo predvidenih stroškov, katera umestitev bo razporejena v proračun za leto 2005 in leto 2006, je navedeno, da bo bremenitev proračuna za leto 2005 znašala 247.096.000 sit in za leto 2006 140.242.600 sit, kar skupaj znaša približno 387 milijonov sit (Projekt, 2005: 15). Pri tem bo “/s/trošek povišanja cene potnega lista iz naslova stroška čipa bremenil državljana” (Projekt, 2004: 11).

V projektu navajajo tudi opremo mejnih prehodov. “Mejna kontrola mora omogočiti identifikacijo in verifikacijo imetnika potnega lista. Sestavni del mejne kontrole bo z uvedbo biometrije postala naprava za branje zapisa biometričnih podatkov shranjenih

na čipu in naprava za odvzem prstnega odtisa ter kamera. Programska oprema na meji mora omogočiti uparjanje podatkov shranjenih na čipu (npr. prstnega odtisa) z drugimi bazami podatkov. Za preverjanje biometrije pri prehodu državne meje bo opremljenih 159 kontrolnih stez (toliko kontrolnih stez je, oz. v kratkem bo, opremljenih tudi z OCR-B čitalci⁹³) mejnih prehodov na meji z Italijo, Avstrijo, Madžarsko in Hrvaško” (Projekt, 2004: 11). Glede na to, da bodo tudi po uvedbi biometričnih potnih listov, stari potni listi veljali še do njihovega izteka, ne vem zakaj bi morali mejne prehode opremiti za preverjanje biometrije oz. se bo biometrično preverjanje izvajalo le za lastnike biometričnih potnih listov, kar je po mojem mnenju sporno. V novejšem Projektu (2005: 10) se omenja tudi “/p/ovezovanje s policijskim AFIS sistemom” kar bi poleg dodatnih stroškov (6.000.000 SIT za eno oddaljeno AFIS zajemno mesto) sprožilo tudi druge pomisleke, ki bodo (vsaj posredno) obravnavani v 9. poglavju, zato jih tu nimam namena opisovati.

Zanimivo bo videti, koliko bo stal 'novi' biometrični potni list, ki ga bodo (zaenkrat) v resnici potrebovali le tisti (manjši del) slovenskih državljanov, ki bo potoval v ZDA. Za zdaj pa so nam na voljo nekatera predvidevanja. “Poslanka nemške liberalne stranke v Bundestagu Gisela Piltz je poudarila, da izračuni strokovnjakov kažejo, da bodo morali zaradi proizvodnih in drugih stroškov novi nemški potni listi stati najmanj 300 evrov (približno 72.000 sit op. M.A.). Zdaj morajo Nemci za svoj potni list odšteti le 26 evrov (okoli 6200 sit), kar je nekaj manj, kot stane slovenski potni list z veljavnostjo pet let (7710 sit). Na 300 evrov pa svoj potni list že sedaj cenijo v Italiji, tako da bodo pri njih novi biometrični potni listi še bistveno dražji. Na precejšen strošek za povprečno EU-družino zaradi novih potnih listov so opozorili tudi poslanci nemških Zelenih. Njihov izračun je sicer nekoliko nižji. Izračunali so, da bo proizvodna cena najmanj 130 evrov (pribl. 31.000 sit op. M.A.), vendar pa so poudarili, da niso upoštevali upravnih in drugih stroškov” (Cerar, 2005).

8.2 EVROPSKA UNIJA (EU)

“Usklajevanje varnostnih značilnosti in vključitev biometričnih identifikatorjev pomenita z vidika prihodnjega razvoja na evropski ravni pomemben korak naprej v smeri uporabe novih elementov, ki bolje zaščitijo potovalni dokument in vzpostavijo

⁹³ Čitalci strojno berljivih potnih listov.

zanesljivejšo povezavo med potnim listom oziroma potovalnim dokumentom in njegovim imetnikom, kar pomembno prispeva k zagotavljanju zaščite potnega lista oziroma potovalnega dokumenta pred zlorabo” (Colja, 2005: 22, 23).

Evropski svet je 19. in 20. 6. 2003 v kraju Tesaloniki v Grčiji potrdil, da je znotraj EU potreben usklajen pristop glede biometričnih identifikatorjev ali biometričnih podatkov za dokumente državljanov tretjih držav, potne liste državljanov EU in informacijske sisteme (VIS in SIS II). Navedena potreba se je odrazila z Uredbo Sveta Evropske unije o standardih zaščitnih elementov ter biometrije v potnih listih in potovalnih dokumentih, ki jih izdajajo države članice⁹⁴ (v nadaljevanju Uredba) sprejeta 13. 12. 2004 in je stopila v veljavo 18. 1. 2005 ter ima 14 uvodnih točk in 6 členov ter prilogo – Minimalni varnostni standardi za potne liste in potovalne dokumente, ki so izdani s strani držav članic. Glede na Uredbo je uvajanje biometričnih podatkov na potovalne dokumente potrebno zaradi zaščite pred ponarejanjem in zaradi vzpostavitve zanesljive vezi med pravim lastnikom in dokumentom (2. točka).

1.člen določa, da morajo biti potni listi in potovalni dokumenti v skladu z minimalnimi varnostnimi standardi določenimi v prilogi.

Potni listi in potovalni dokumenti morajo imeti vključen podatkovni medij z zadostno kapaciteto, ki vsebuje obrazno sliko ter prstne odtise. Podatki morajo biti varovani, podatkovni medij po mora imeti zadostne kapacitete in sposobnosti za zagotovitev integritete, avtentičnost in zaupnost podatkov.

Uredba se nanaša na potne liste in potovalne dokumente, ki jih izdajo države članice in se ne nanaša na osebne izkaznice ali potne liste in potovalne dokumente z veljavnostjo 12 mesecev ali manj.

2. člen določa, da se v skladu s postopkom iz 5. člena določijo dodatne tehnične zahteve za potne liste in potovalne dokumente v zvezi z:

- dodatnimi varnostnimi značilnostmi in zahtevami, vključno s povečanjem zaščite pred ponarejanjem in prenarejanjem;
- tehničnimi zahtevami za podatkovni medij z biometričnimi informacijami in njihovo zaščito, vključujoč tudi preprečevanje neavtoriziranega dostopa;

⁹⁴ Council Regulation on standards for security features and biometrics on passports and travel documents issued by Member States OJ L 385/1, 29.12.2004. Uredba Sveta (ES) št. 2252/2004 z dne 13. decembra 2004 o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice (OJ: Official Journal L 385 , 29/12/2004 P. 0001 - 0006).

- zahtevami glede kakovosti in skupnih standardov za obrazno sliko in prstne odtise.

3. člen določa, da so specifikacije, navedene v 2. členu tajne in se ne objavijo. Dostopne so lahko le državnim organom, ki izdajajo potne liste, in osebam, ki jih ustrezno pooblasti država članica ali Komisija.

Vsaka država članica imenuje en organ, ki ima odgovornost za tiskanje potnih listov in potovalnih dokumentov, katerega ime tudi posreduje Komisiji in državam članicam. Dve ali več držav lahko imenujejo isti organ. Vsaka država članica lahko spremeni ta organ, o tem pa obvesti tudi Komisijo in države članice.

4. člen določa, da imajo osebe, katerim je bil izdan potni list ali potovalni dokument, pravico preveriti osebne podatke zajete v potnem listu ali potovalnem dokumentu in, kjer je to upravičeno, zahtevati popravo ali izbris.

Na potnem listu ali potovalnem dokumentu ne sme biti nobenih podatkov v strojno berljivi obliki, če ti niso predvideni v tej uredbi ali aneksu, razen če so ti podatki v potnih listih ali potovalnih dokumentih držav članic, ki imajo za to podlago v nacionalni zakonodaji.

Za namen te Uredbe so lahko biometrične značilnosti v potnih listih in potovalnih dokumentih uporabljene zgolj za verifikacijo:

- avtentičnosti dokumenta;
- identitete imetnika s pomočjo neposredno dosegljivih primerjalnih značilnosti, kadar mora biti potni list ali drug potovalni dokument izdelan skladno z zakonom.

5. člen določa, da Komisiji pomaga odbor, ustanovljen s členom 6(2) Uredbe (EC) št. 1683/95. Pri sklicevanju na to določilo se uporabljata člena 5. in 7. Sklepa 1999/468/EC. Obdobje, določeno v členu 5(6) Sklepa 1999/468/EC, znaša dva meseca. Odbor sprejme svoj poslovnik.

Države članice uporabijo to Uredbo za vključitev obrazne slike v 18 mesecih ter prstnih odtisov v 36 mesecih.

Uredba ne vpliva na veljavnost že izdanih potnih listov in potovalnih dokumentov.

V zaključku še piše, da je ta Uredba v celoti zavezujoča in se neposredno izvaja v državah članicah v skladu s Pogodbo o ustanovitvi Evropske skupnosti.

Skrajni roki uvedbe biometričnih podatkov (obrazna slika in prstni odtisi), ki izhajajo iz sledeče Uredbe, če upoštevamo začetek veljavnosti uredbe, 18. 1. 2005, so torej

18. 7. 2006 za vključitev obrazne slike in 18. 1. 2008 za prstne odtise. Vidimo lahko, da so roki, ki so jih postavile ZDA, precej preseženi.

Kot kaže skoraj nobena država, niti Slovenija, ne bo imela potnih listov do roka.⁹⁵ V začetku februarja so tri tehnološko zelo razvite države, Japonska, Francija in Velika Britanija, objavile, da ne bodo uvedle oziroma izdelale biometričnih potnih listov do določenega roka. Pač ne gre. Na slovenskem MNZ še ne vedo, ali bodo biometrični potni listi izdelani do roka ali ne. Budno pa naj bi spremljali, kaj se dogaja v EU. Nekateri slovenski proizvajalci naj bi pripravljali prototipe novih slovenskih potnih listov, na MNZ pa so opozorili, da bodo glede njih izvedli mednarodni razpis⁹⁶ za izbor najboljšega ponudnika, tako da jih bo lahko proizvajalo tudi kakšno tuje podjetje (Cerar, 2005).

“Do okoli ameriško zapovedanega roka pa sta izdajo svojih potnih listov optimistično napovedali le Švedska in Belgija. Nemčija pa naj bi proizvodnjo biometričnih potnih listov začela letos novembra” (Cerar, 2005).

8.3 ZDRUŽENE DRŽAVE AMERIKE (ZDA)

ZDA glede uvajanja biometričnih metod zaseda prav posebno mesto, kar je rezultat tudi (a ne zgolj) dogodkov 11. 9. 2001. Danes so ZDA nesporno vodilne na področju uvajanja biometričnih metod s ciljem preprečevanja terorizma. ZDA po 11. 9. 2001 vneta iščejo metode, ki imajo potencial preprečevanja terorizma in iskanja oseb osumljenih terorizma. Vendar je to zgolj del ameriških naporov povezanih z biometričnimi metodami. Že nekaj let so npr. v nekaterih ameriških zaporih prisotne biometrične metode⁹⁷ in predvideva se, da se bo njihova uporaba še razširila.

Nadalje šest ameriških držav uporablja biometrične aplikacije širokega obsega v programih socialnih služb (Arizona, California, Connecticut, Massachusetts, New York in Texas). Namenjeni so predvsem preprečevanju goljufij, ko nekateri

⁹⁵ Kot poroča Delo (8. 4. 2005: 17) bo med 25 članicami EU le šestim – Belgiji, Finski, Luksemburgu, Nemčiji, Avstriji in Švedski uspelo ujeti ameriški rok. Za vse ostale je evropski komisar za pravosodje, svobodo in varnost zaprosil ameriški predstavniški dom še za drugi odlog do 28. 8. 2006.

⁹⁶ Mednarodni razpis s katerim bo MNZ poiskalo izdelovalca potnih listin z biometričnimi elementi je bil že objavljen, ponudbe pa se že zbirajo. Razpis bo končan sredi maja letošnjega leta (Delo, 8. 4. 2005: 17).

⁹⁷ Glavni način uporabe biometričnih metod v ameriških zaporih je spremljanje odhodov in izhodov osebja in zapornikov iz zapora (Turner, 2003: 63).

posamezniki pod različnimi imeni pobirajo večkratna izplačila (Woodward, Orlans in Higgins, 2003: 284).

Izredno zanimiv je tudi primer policije v Gwinnet County, Georgia, ki uporablja biometrične podpise za izdajo zapornega naloga. Policist po video konferenci preko interneta vzpostavi stik s sodnikom, ki, če je zadovoljen z dokazi, avtorizira nalog z elektronskim podpisom. Celoten proces vzame le 15 minut in bistveno zmanjša čas potreben za izdajo zapornega naloga in razbremeni delo policistov in omogoči njihovo učinkovitejše delo (Woodward, Orlans in Higgins, 2003: 291, 292).

To je le nekaj primerov programov, ki vključujejo biometrične metode na vladni ali državni ravni. Samo DHS skupaj ima več kot 60 programov, ki uporabljajo biometrične metode (Buxbaum, 2005: 15), poleg tega pa obstaja seveda obširna uporaba biometričnih metod v forenzičnih aplikacijah ter številčno ogromna uporaba biometričnih metod v poslovnih in civilnih aplikacijah, ki postaja zares široka in množična.

V nadaljevanju bom opisal le tiste programe, za katere menim, da uporabljajo biometrične metode s ciljem preprečevanja terorizma in jih nisem opisal že v preteklih poglavjih.

8.3.1 US-VISIT: Visitor and Immigrant Status Indicator Technology

ZDA so v preteklosti, še bolj pa po dogodkih 11. 9. 2001, namenile ogromno pozornosti varnosti mej oz. kontroli potnikov na mejnih prehodih v ZDA. Da je to resnično izredno zahtevna in težavna naloga, pričajo tudi nekateri empirični podatki: V letu 2002 je bilo pribl. 440 milijonov⁹⁸ prehodov meje v ZDA na več kot 300 mejnih prehodih. Poleg tega pride po ocenah INS (Immigration and Naturalization Service) vsako leto v ZDA tudi 275.000 novih ilegalnih priseljencev, pri čemer se jih pribl. 60 % (165.000) izogne mejnim prehodom (Kingsbury, 2003: 3, 8), večinoma gre to na račun meje z Mehiko nekaj pa tudi na račun meje s Kanado.

“Temeljna vladna (vlada ZDA op. M.A.) strategija je postaviti 'navidezno' mejo zunaj naših geografskih meja kot prvi varnostni nivo, ki se začne na točki izvora vsakega tujega obiskovalca, tovornjaka ali zabojnika, tako da fizične meje postanejo zadnja črta obrambe, namesto prva” (Stein, 2004). Ta prvi varnostni nivo naj bi se

⁹⁸ Od tega pribl. 12 milijonov morskih, 70 milijonov zračnih in 358 milijonov kopenskih prehodov meje (Kingsbury, 2003: 3).

uresničeval z uvedbo biometričnih potnih listov in biometričnih viz ter vsaj pri vizah še temeljitega preverjanja po podatkovnih bazah.

Zavedajoč se naloge, so začeli v ZDA vzpostavljati poseben program, ki se skrajšano pomenljivo imenuje US-VISIT in vsebuje tudi precejšnje število biometričnih rešitev.⁹⁹

US-VISIT je kontinuum varnostnih ukrepov, ki se začnejo v tujini na mestih za izdajo viz in se nadaljujejo s prihodom in odhodom iz ZDA. Cilji US-VISIT so:

- povečati varnost državljanov ZDA in obiskovalcev,
- olajšati zakonita potovanja in trgovanje,
- zagotoviti celovitost ameriškega imigracijskega sistema in
- varovati zasebnost obiskovalcev (What is US-VISIT?, 2005).

Kljub temu pa je "v/eliko postopkov na točkah vstopa ostalo nespremenjenih. Carina in mejna policija še vedno pregledujeta potovalne dokumente, vizum in potni list. Pristojne osebe pa še vedno postavljajo vprašanja vezana na bivanje v ZDA. Novost v okviru US-VISIT je, da carina in policija uporabljata digitalne fotoaparate in naprave za skeniranje dveh prstnih odtisov (glej sliko 8.12 op. M.A.), ti postopki pa ne pomenijo večjih časovnih zamud v celotnem procesu" (Colja, 2005: 20).

Ko bo US-VISIT dokončno implementiran, bo delujoč na vseh mejnih prehodih v ZDA (kopenskih, morskih in zračnih), da bi preskrbel obširne informacije o tujih državljanih, ki vstopajo in izstopajo iz ZDA ter povezal te posameznike z njihovimi potovalnimi dokumenti (potni listi in vize) (Most, 2004: 18).

"US-VISIT je pomembna iniciativa, ki jo je DHS postavila na pomembno mesto, da bi bolje zaščitili nacionalne mejne prehode pred terorizmom in omogočili enostaven vstop za legitimne potnike in blagovni promet" (Schwartz, 2004). US-VISIT trenutno velja za vse obiskovalce v starosti od 14 do 79 let¹⁰⁰ ne glede na državo izvora (What is US-VISIT?, 2005).

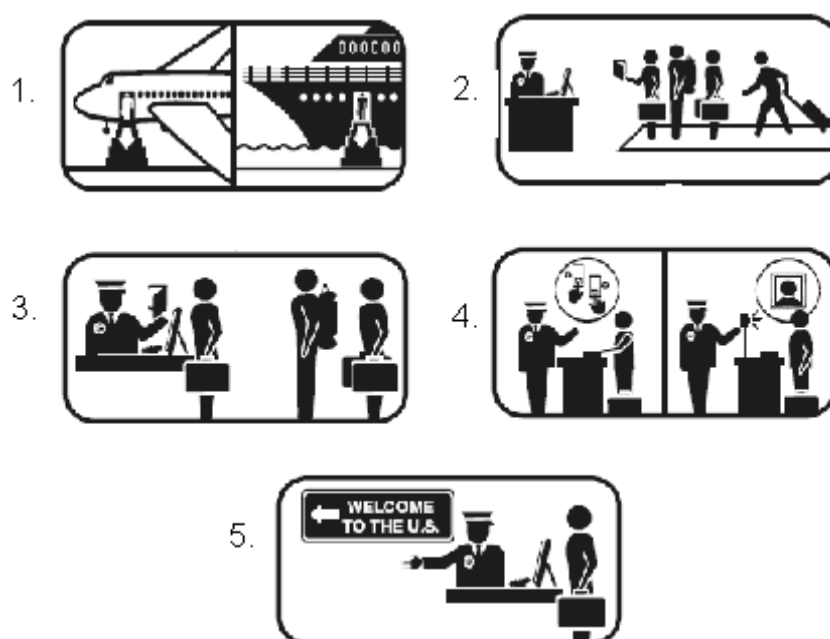
Če povzamem in poenostavim zadevo, gre pri US-VISIT za to, da se pridobi biometrične in druge podatke ljudi, ki prihajajo v ZDA, najprej na ambasadah in konzulatih v tujini, ki izdajajo vize, nato še ob prihodu na mejni prehod v ZDA, kjer se

⁹⁹ Zakoni sprejeti v času po 11. 9 zahtevajo širšo uporabo biometričnih metod za mejno kontrolo. Takšna zakona sta predvsem Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public Law 107-56, §403(c) and §414, Oct. 26, 2001) ter the Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107-173, May 14, 2002) (Kingsbury, 2003: 4).

¹⁰⁰ Razen za ameriške državljane in nekatere druge posebne izjeme. Izjeme dostopne na http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0527.xml.

tistim brez viz in brez biometričnih potnih listov odvzame prstna odtisa levega in desnega kazalca ter obrazno fotografijo. Namen je dvojen. Ugotoviti, da je oseba, ki vstopa v državo, res tista, ki je pridobila vizo, ter primerjava podatkov z vladnimi podatkovnimi bazami,¹⁰¹ da se ugotovi ali je posameznik 'varnostno problematičen'. Vendar US-VISIT uveljavlja še eno pomembno novost, saj gre tudi za avtomatizirano kontrolo izhoda¹⁰² iz države na za to namenjenih napravah.¹⁰³ Primaren razlog uvedbe US-VISIT pa je preprečevanje dostopa teroristom oz. sumljivim posameznikom do ZDA.

Slika 8.12: Grafični prikaz delovanja US-VISIT na primeru letališč in pristanišč



Vir: US-VISIT Arrival Process for Visitors traveling with a Visa (2005).

¹⁰¹ "Namen US-VISIT je zbiranje biometričnih podatkov obrazne fotografije in prstnih odtisov za vsakega obiskovalca, ki obišče ZDA, in jih shraniti v podatkovno bazo, ki je lahko primerjana s kriminalnimi, obveščevalnimi ali imigracijskimi podatkovnimi bazami številnih zveznih agencij" (Stein, 2000), kar je potrjeno tudi s strani tiskovne predstavnice DHS-a, ki "je povedala, da je US-VISIT kompatibilen z drugimi podatkovnimi bazami organov pregona, tudi z IAFIS, in da so podatki deljeni med DHS in zunanjim ministrstvom" (Marois, 2004: 3).

¹⁰² Predhodnico vhodno-izhodnega nadzora je pomenil NSEERS (National Security Entry Exit Registration System). Gre za program, ki ga je razvilo ameriško pravosodno ministrstvo (Department of Justice) in je bil implementiran v septembru 2002. NSEERS je posledica zahteve kongresa po vhodno-izhodnem programu. NSEERS je pomenil prvi korak k celovitemu vhodno-izhodnemu sistemu, ki ga danes predstavlja US-VISIT. NSEERS velja samo še za državljane Irana, Iraka, Libije, Sirije in Sudana, kar pa bo sčasoma tudi preneseno na US-VISIT (US-VISIT FAQs: NSEERS and US-VISIT, 2005).

¹⁰³ "Splošno tvoj odhod iz države vključuje skeniranje vizuma ali potnega lista in ponovitev postopka skeniranja prstnih odtisov. Potrdilo o izhodu je dodano k potovalni kartoteki obiskovalca, da se dokaže skladnost z roki vstopa. Vsi podatki, ki jih pridobijo o obiskovalcu, so varno shranjeni kot del njegove potovalne kartoteke. Ta informacija je na voljo le avtoriziranim uradnim osebam in določenim vladnim agencijam, ki so odgovorne za zagotavljanje varnosti državljanov ZDA in tujih obiskovalcev" (Colja, 2005: 21).

US-VISIT je (zgolj za prihode) začel delovati 5. januarja 2004¹⁰⁴ na 115 mejnih prehodih na letališčih in 14 mejnih prehodih v pristaniščih, pilotno pa je začel potekati program izhodnih procedur na po enem letališču in pristanišču (What is US-VISIT?, 2005). Dne 9. 11. 2004 je DHS objavil 50 najfrekventnejših kopenskih mejnih prehodov, na katerih je 31.12.2004 začel delovati US-VISIT (Fact Sheet: U.S. – Mexico Land Borders, 2005). Tako se je začel proces, ko bo deloval US-VISIT na vseh (uradnih) vstopnih točkah v ZDA.

Postavlja se zanimivo vprašanje, ali so ogromni finančni¹⁰⁵ in človeški resursi upravičeni oz. ali US-VISIT uresničuje razloge zaradi katerih je (oz. dokončno še bo) uveden (pri tem imam v mislih predvsem preprečevanje terorizma)?

“Po uporabi vseh teh orodij te mejni organi ZDA bodisi spustijo v državo ali pa uvedejo nadaljnji postopek poizvedbe, ki temelji na verifikacijskih rezultatih. Ta postopek zmanjšuje sleparstvo, krajo identitet in tveganje, da teroristi in kriminalci vstopijo v ZDA neodkriti ali z uporabo ukradenih ali ponarejenih dokumentov” (Colja, 2005: 20).

“V samo nekaj tednih je bilo na desetine pozitivnih prepoznav. Ujet je bil obsojen kriminallec, ki je imel pet identitet in tri rojstne datume. Ujet je bil tudi preprodajalec mamil, ki je bil že dvajset let na begu. Teroristi lažejo; prstni odtisi ne”¹⁰⁶ (Ridge, 2004: 11). Da se ob ujetju kriminalcev omenja teroriste je po mojem mnenju demagogija s katero se poskuša upravičevati velike stroške US-VISIT in ostalih programov preprečevanja terorizma.

Še nekoliko kasneje je “Robert Bonner¹⁰⁷ povedal, da je US-VISIT že preprečil več sto ljudem, iskanim za resna kriminalna dejanja, da bi vstopili v ZDA (čeprav ni želel povedati, ali je bil kdor koli od njih osumljen terorist)” (Stein, 2004). Teroristi torej verjetno res (še?) niso bili prepoznani oz. so se preprosto izogibali mejnim prehodom, kjer US-VISIT že deluje, kar roko na srce niti ni tako težko, saj le-ta še ni (bil) operativen na kopenskih mejah, ki so precej bolj prepustne. Treba pa je vzeti v obzir tudi možni zastraševalni učinek, ki teroriste 'prepriča', da verjetno ni najbolj pametno vstopati v državo tam, kjer ste podrobno izprašani, sta vam odvzeta prstna

¹⁰⁴ Dne 30. 9. 2004 so začele procedure veljati tudi za državljane VWP (Visa Waiver Countries, 2005).

¹⁰⁵ Po ocenah DHS se pričakuje, da bo za program US-VISIT do leta 2014 porabljenih od sedem do deset milijard dolarjev (Jones, 2004).

¹⁰⁶ Zakaj se omenja teroriste, ko se govori o ujetem preprodajalcu mamil mi ni povsem jasno, verjetno gre za ameriško obsedenost s terorizmom in poskusom vladnih uslužbencev, da prepričujejo javnost kako dobro delajo na področju boja proti terorizmu tudi kadar pravzaprav ne gre za terorizem.

¹⁰⁷ Pooblaščenec carine in mejne zaščite ZDA.

odtisa in ste slikani ter še dodatno preverjeni po obsežnih podatkovnih bazah. Toda to je vse teoretično razmišljanje, ki pa je ob pomanjkanju (vsaj meni znanih) empiričnih podatkov edino možno. Je pa res, da se je US-VISIT vsaj delno izkazal pri iskanju kriminalcev, kar je tudi kar spodbudno dejstvo.

Eden od razlogov, zakaj ni bil prepoznan noben terorist, se skriva v še eni podrobnosti. "US-VISIT ima še eno resno omejitev: če želi terorist prvič vstopiti v ZDA pod izmišljenim imenom in strokovno ponarejenim potnim listom, ni nobene možnosti, da bi ugotovili njegovo identiteto. Kot posledico tega bo vlada ZDA v prihodnosti zahtevala, da imajo vsi tuji obiskovalci potne liste z biometričnimi podatki (Stein, 2004). Po mojem mnenju še težji primer predstavlja dejstvo, da so VSE biometrične metode "popolnoma nemočne pri prepoznavi teroristov, če o njih nimamo točno določenih biometričnih podatkov, ki jih povežejo z znanimi teroristi" (Skokowski, 2002: 1). Torej, če ne vemo, da je XY terorist, nam nič ne pomaga, če spoznamo o XY vse drugo.

Strinjam se tudi s Steinom (2004) ko pravi "k/ljub temu, da je vlada ZDA naredila impresiven napredek v zavarovanju naših mej (mej ZDA op. M.A.), toda vseeno se vsi strinjajo v eni stvari: mora biti še boljše. Ne smemo zapravljati časa". Potrebno je pojmovati vsako varnostno delovanje kot tudi seveda varovanje mej oz. kontrolo prihodov in odhodov kot dejavnost, ki se mora nenehno izboljševati in dopolnjevati, saj ne počivajo niti tisti, ki želijo takšne namene zaobiti ali preslepiti.

8.3.2 INSPASS: INS Passenger Accelerated Service System

INSPASS je avtomatiziran sistem,¹⁰⁸ ki lahko pomembno zmanjša čas potreben za običajne postopke na meji in je namenjen avtoriziranim potnikom, ki poslovno potujejo v ZDA tri ali večkrat na leto, diplomate, predstavnike mednarodnih organizacij ali letalsko osebje iz držav ZDA, Kanade in Bermudov ter držav VWP, ki se prostovoljno registrirajo v program INSPASS. Praktično poteka postopek tako, da potniki ob prihodu na mejno točko nadaljujejo svojo pot proti INSPASS kiosku, kjer sistemu predstavijo posebno kartico z biometričnimi podatki dobljeno pri registraciji in položijo svojo roko na čitalec geometrije roke. Če je verifikacija pozitivna, potnik nadaljuje svojo pot direktno na oddajo prtljage, če je verifikacija negativna, se ga

¹⁰⁸ Kot pilotni program INSPASS poteka že od leta 1993 in ima trenutno več kot 45.000 sodelujočih in je do sedaj vseboval več kot 300.000 potnikov (Rhodes, 2003: 16).

napoti na nadaljnjo preveritev. Vse to traja le 15 do 20 sekund. Sistem je delujoč na devetih ameriških letališčih. V primeru, da DHS dvigne stopnjo ogroženosti¹⁰⁹ na oranžno, je sistem zamrznjen (povzeto po Rhodes, 2003: 16 in INS PASSENGER ACCELERATED SERVICE SYSTEM, 2005).

Glavni doprinos INSPASS naj bi bil v tem, da se razbremeni mejna kontrola tistih posameznikov, ki ne predstavljajo grožnje varnosti ZDA in se lahko le-ta bolj posveti ostalim potnikom. Verjetno pri majhnem odstotku potnikov, ki so vključeni v ta in podobne programe, res ne prinese večjih koristi, toda če se bo odstotek avtoriziranih potnikov večal, se tak program lahko izkaže za koristnega tudi v luči preprečevanja terorizma.

8.3.3 TWIC: Transportation Worker Identification Credential (Identifikacijska poverilnica za delavce na področju transporta)

Za vzpostavitev TWIC so bili sprejeti glavni trije zakoni; The Aviation and Transportation Security Act (ATSA), Public Law (P.L) 107-71, Maritime Transportation Security Act iz leta 2002 (MTSA), P.L. 107-295 in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), P.L. 107-56, ki zahtevajo 'preveritev ozadja' in izdajo biometričnih dokumentov za delavce na področju transporta. Da bi se to uresničilo, je zadolžena Transportation Security Administration (TSA), ki je začela delati na programu TWIC v decembru 2001 z namenom narediti in implementirati standardizirano varno poverilnico za identifikacijo delavcev v transportu, ki potrebujejo fizični dostop do varovanih območij nacionalnega transportnega sistema ali dostopa do računalniško osnovanih informacijskih sistemov, ki so povezani z varnostjo transportnega sistema. TSA začneja implementiranje prototipa na 36 mestih na podlagi prostovoljnosti. Za registracijo bo potrebno podati svoje biografske podatke (ime, telefonsko številko, številko socialnega zavarovanja, datum rojstva idr.), ki bodo temeljito preverjeni, in biometrične podatke (prstni odtis in/ali šarenico ter elektronski podpis in digitalno fotografijo), kar bo omogočilo verifikacijo identitete vsakega lastnika TWIC (pametne) kartice, da je bila identiteta le-tega tudi varnostno preverjena in da je vsaka poverilnica izdana upravičenemu posamezniku. Prototipna

¹⁰⁹ Obstaja pet stopenj ogroženosti. Zelena - nizka, plava - previdnost, rumena - zvišana, oranžna - visoka in rdeča – zelo resna (severe) (Homeland Security Advisory System, 2005).

faza se je začela jeseni 2004 in naj bi se končala konec prvega četrtertletja 2005 (Dean, 2004: 2-5). Lolie Kull, vodja TWIC, pričakuje, da bo program deloval po celi državi v začetku leta 2006 (Buxbaum, 2005: 17). Namen TWIC je predvsem zagotoviti dve stvari. Prvič, da imajo dostop do varnostno tveganih območij le posamezniki, ki ne predstavljajo varnostne grožnje (predvsem teroristične) in drugič, da se dodatno zagotovi zanesljivost ugotovitve povezave med TWIC kartico in avtoriziranim posameznikom. TWIC se uvaja predvsem zaradi skrbi ameriških oblasti pred terorizmom.

9. VPRAŠANJE ZASEBNOSTI PRI UVAJANJU BIOMETRIČNIH METOD

V večini demokratičnih držav se človekovim pravicam v zadnjem času daje velik poudarek. In zasebnost je "ena izmed temeljnih človekovih pravic" (Črnčec, 2004b: 8). "Poglavitni dokument (ki ureja to področje op. M.A.) našega stoletja je Splošna deklaracija o človekovih pravicah, ki jo je 10. decembra 1948 sprejela Generalna skupščina OZN.¹¹⁰ V deklaraciji je pravica do zasebnosti posebej poudarjena (Črnčec, 2004b: 8). Ta pravica je še posebej izražena v 12. členu:

Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi (Splošna deklaracija o človekovih pravicah, 1948).

Brez da bi se nadalje spuščal v teoretične razprave o zasebnosti, sprejeti zakonodaji ali njeni pomembnosti bom podal le delovno definicijo, ki jo bom imel v mislih v tem poglavju. Takšno delovno definicijo zasebnosti z vidika biometrije so navedli tudi Woodward, Orlans in Higgins (2003: 200) in se glasi: *zasebnost je naš nadzor nad informacijami o nas samih, nadzor nad tem kdo nas lahko zaznava in nadzor nad zaupnostjo osebne identitete*. Ta nadzor nad informacijami o nas samih se imenuje tudi 'informacijska zasebnost' in je ključni del zaskrbljenosti za zasebnost,

¹¹⁰ Najvišji pravni dokument, ki ureja to področje v RS je slovenska ustava v kateri je "pravica do zasebnosti /.../ podrobneje urejena v določbah o nedotakljivosti stanovanja, tajnosti pisem in drugih občil ter varstvu osebnih podatkov" (Črnčec, 2004b: 8).

ki jo sproža nova tehnološka realnost. Posamezniki imajo interes določiti kako, kdaj, zakaj in komu bodo informacije v obliki biometričnih podatkov razkrite.

O povezavi med zasebnostjo in biometričnimi metodami piše oz. to vsaj omeni praktično vsak, ki vsaj malo pozna in spremlja to področje, saj se v zvezi z implementacijo biometričnih metod odpira precej vprašanj, ki (lahko) vplivajo na zasebnost. "Osnoven problem uporabe biometričnih sistemov na splošno je vprašanje zasebnosti v družbi" (Skokowski, 2002: 1). "Pomemben faktor, ki vpliva na odločitev o tem, ali bo implementirana metoda identifikacije oz. verifikacije biometrična, je tudi psihološki faktor. Biometrične metode se pogosto smatrajo za relativno vsiljive metode, ki jih uporabnik lahko razume kot vdor v njegovo zasebnost. Uspeh pri doseganju široke uporabe biometrične tehnologije v praksi je zatorej odvisen od stališča javnosti, glede uspešnosti biometričnih tehnologij z vidika varovanja zasebnosti" (Fefer, 2004: 150). Tudi iz pričujočih in podobnih navedkov lahko sklepam, da vprašanje zasebnosti pri uvajanju biometričnih metod ni le domneva paranoidnih posameznikov, ki v vsem vidijo 'velikega brata', temveč povsem umestno vprašanje, ki potrebuje široko znanstveno in javno razpravo in ki ji morajo slediti tudi ustrezne zakonske rešitve ter njihova implementacija.¹¹¹ Pri tem ne bo šlo le za doseganje široke uporabe, temveč tudi za uspešnost biometričnih metod na vseh področjih. Glede na preučeno literaturo se tega dobro zavedajo tudi države, strokovnjaki in celo podjetja,¹¹² ki razvijajo in prodajajo biometrične rešitve, saj temu namenjajo precej pozornosti. Je pa res, da smo včasih priča nekoliko dramaturško in demagoško obarvanim zapisom prav s strani takšnih podjetij kot npr. "grožnja naši zasebnosti je teoretična, medtem ko je grožnja terorizma na žalost zelo resnična" (Visionics Corporation, 2001: 7). Res je tudi, da se javnost odziva na trenutne varnostne razmere in je včasih, če se počuti ogroženo, pripravljena sprejeti tudi zmanjšanje standardov zaščite človekovih pravic in zasebnosti, čemur smo nedvomno priča po 11. 9. 2001, še posebej v ZDA (seveda 'v konkurenci' demokratičnih držav). Takrat takšne navedbe nedvomno lahko padejo na plodna tla, kar je v zelo določenih in časovno omejenih primerih mogoče celo koristno. Toda bistveno je, da 'posebni ukrepi' prenehajo v čim krajšem času, da le-ti ne postanejo

¹¹¹ Kaj nam pomaga tudi odlična zakonodaja, če ostaja le 'mrtva črka na papirju'.

¹¹² "Ni dvoma, da identifikacijska varnostna infrastruktura sproža zaskrbljenost glede zasebnosti" (Visionics Corporation, 2001: 6).

'normalni oz. običajni', ker se potem raven že pridobljenih pravic zasebnosti trajno zmanjša.

Večinoma potekajo razprave o tem, da naj bi se našlo ustrezno razmerje med varnostjo in človekovimi pravicami oz. zasebnostjo.¹¹³ Eden izmed razpravljavcev je tudi Woodward (2001b: 15,16), ki medtem, ko zagovorniki človekovih pravic lahko obsojajo uporabo tehnologije obrazne prepoznave¹¹⁴ kot vdor v zasebnost, trdi, da leži rešitev v ravnovesju potrebe med potrebo po varnosti in potrebo po zaščiti državljskih svoboščin. V tem smislu morajo biti omenjene naslednje tri točke (primer velja za ZDA):

- Prvič, nimamo ustavne pravice do zasebnosti obraza, ki ga kažemo v javnosti, kar je potrdilo tudi vrhovno sodišče ZDA.
- Drugič, sedanji pravni standardi prepoznavajo, da smo vsi predmet povišane natančne preiskave na mejah in vstopnih točkah. Ta 'mejna izjema' 4. amandmaja prepozna "dolgoletno pravico (suverena, vladarja), da se zaščiti z ustavitvijo in pregledom oseb in lastnine, ki prihajajo v državo" (United States v. Ramsey U.s. 606, 616 (1977)).
- Tretjič, velja omeniti, da sistemom obrazne prepoznave niso zaupane končne odločitve o človekovi identiteti. Namesto tega sistem opozori odgovorne na potrebo po nadaljnjih poizvedbah (Woodward, 2001b: 15, 16).

"Seveda je individualna varnost za posameznika najpomembnejša, kakor je tudi zanj najpomembnejša njegova zasebnost. Ena in druga pravica sta povezani in v medsebojni soodvisnosti ter nemalokrat tudi v obratnem sorazmerju, saj povečevanje ene povzroča zmanjševanje druge" (Črnčec, 2004b: 11).

"V zvezi z uporabo biometričnih tehnologij gre evidentno za aktivnosti, ki tako ali drugače posegajo v področje človekove zasebnosti. Hkrati pa narašča obseg raznih

¹¹³ Zgodovinsko sta bila zasebnost in varnost obravnavana kot nasprotujoči si sili v igri ničelne vsote. Takšen pogled vsebuje ravnovesje, kjer povečanje enega pomeni zmanjšanje drugega. Toda to razpoloženje predstavlja veliko grožnjo zasebnosti predvsem zaradi razloga, da je želja javnosti po varnosti po dogodkih 11. 9. 2001 tako zelo visoka. Nadaljevanje debate po 11. 9. 2001 v tem okviru ogroža same temelje zasebnosti in pušča prihodnost pod vprašajem. Zaradi tega je potrebno spremeniti to paradigmo, saj ni inherentnega razloga, zakaj bi večja varnost morala priti na račun zasebnosti. Veliko varnostnih tehnologij (tudi biometrična) je lahko narejenih tako, da ostanejo visoko učinkovite in se obenem minimalizira ali odstrani njihova grožnja zasebnosti. Če spremenimo staro paradigmo in jo nadomestimo z novo, tj., da sta zasebnost in varnost dve komplementarni strani iste nedeljive celote, lahko načrtujemo tehnologije, ki ščitijo javno varnost brez žrtvovanja zasebnosti (Cavoukian, 2002: 1). Je pa res, da je razmišljanje avtorice prej izjema kot pravilo, pogostejši so zapisi, v katerih avtorji menijo, da je "potrebno v ljudeh prebuditi občutek, da se je za višji nivo varnosti potrebno odreči delu svoje zasebnosti" (Trapečar in Robek, 2003: 55).

¹¹⁴ Največ je govora pri vprašanju zasebnosti glede obrazne prepoznave, zaradi že opisanih značilnosti kot so možnost prikritega nadzora, delovanja na daljavo idr.

oblik kriminalitete; aktualno smo priče vse bolj razširjajočega se terorizma na svetovni ravni. V dilemi med svobodo oziroma varovanjem zasebnosti in varnostjo na splošno, se kažejo trendi, ki dajejo prednost varnosti, družbeni varnosti. Na biometrijo lahko z vidika ogrožanja zasebnosti gledamo kot na sistem za zbiranje elektronskih sledi o posameznikih, saj biometrična tehnologija fizične lastnosti posameznika pretvori v enoličen elektronski zapis. V težnji, da bi se izognili zlorabam in uredili to področje v splošno dobro, so opazni napori, da se to področje pravno ureja vzporedno z razvojem možnosti, ki jih nudijo tehnologije” (Fefer, 2004: 155).

“Obstajata dva nasprotujoča si pogleda glede na vprašanje, ali so biometrične metode grožnja zasebnosti ali ne” (Van der Ploeg, 2003: 1), ki sta si največkrat diametralno nasprotna. Nekateri avtorji menijo, da so biometrične metode t.i. 'zaveznik' oz. prijatelj zasebnosti¹¹⁵ in drugi, da so biometrične metode t.i. sovražnik zasebnosti.¹¹⁶ Po mojem mnenju je odločno vztrajanje na eni ali drugi poziciji ne samo nepotrebno, temveč tudi škodljivo in zavajajoče. Oboji imajo (vsaj do določene mere) prav. Velikokrat razprave tečejo na preveč splošni ravni, ko se celotno področje obravnava kot zaveznik ali sovražnik zasebnosti. Menim, da so biometrične metode istočasno (lahko) zaveznik in (lahko) sovražnik zasebnosti, odvisno je pač od področja njene aplikacije, njene uporabe¹¹⁷ ter nenazadnje tudi od družbene realnosti, v kateri so uporabljene. Povsem enostavno si je zamisliti zlorabo biometričnih metod za (biometrično) nadzorovanje politične opozicije v totalitarnih državah kot sovražnika zasebnosti in po drugi strani omogočenega varnega dostopa do podatkovnih baz osebnih podatkov le avtoriziranih posameznikov kot zaveznika zasebnosti.

V nadaljevanju predstavljam najpogostejše predstavljene primere, v katerih naj bi bile biometrične metode zaveznik, in najpogostejše primere, kjer naj bi bile biometrične metode sovražnik zasebnosti.

¹¹⁵ Npr. Woodward (1997 v Van der Ploeg, 2003: 85), ki pravi: “/m/edtem, ko kritiki biometričnih metod trdijo, da je ta nova tehnologija sovražnik zasebnosti, je resnica prav nasprotna. Biometrične metode so prijatelj (zaveznik) zasebnosti, pa naj si bodi v privatnem ali javnem sektorju”.

¹¹⁶ Pojavljajo se tudi drugi izrazi, ki pa v bistvu označujejo podobno kot omenjena dva. To so npr.: tehnologija za povečevanje zasebnosti (PET-Privacy Enhancing Technology) oz. intruzivna tehnologija za zasebnost (PIT – Privacy Invasive Technology). Pojavljajo se tudi dramatičnejši zapisi, kot npr.: biometrične metode oz. implikacije le-teh na zasebnost pomeni konec sveta kot ga poznamo in na drugi strani biometrične metode oz. implikacije le-teh na zasebnost kot vitez na belem konju za zasebnost (glej npr. v Crompton, 2002: 1, 2).

¹¹⁷ “/G/lavna grožnja zasebnosti nastaja zaradi zlorabe in ne zaradi uporabe” (Alterman, 2003: 147).

9.1 BIOMETRIČNE METODE KOT 'PODPORNIK, ZAVEZNIK oz. PRIJATELJ' ZASEBNOSTI

Norton (Crompton, 2002: 6) trdi, da "je vedno težje in težje obvarovati zasebnost brez uporabe biometričnih metod. Napačno domnevanje je, da biometrične metode nekako ogrožajo zasebnost; v resničnosti so najboljši način za zaščito dokumentov in zagotovitev, da identiteta ne more biti ukradena. Biometrične metode so narejene tako, da dajo uporabniku popoln nadzor nad tem kdo ima dostop do njegovih informacij in zagotavljajo jasno sled, če kdo poskuša pridobiti podatke iz podatkovnih baz", zatorej "biometrične metode dvignejo letvico za prevaro in zlorabo brez dodatne škode za zasebnost" (ibidem).

Boljša zaščita identitete (in s tem tudi zasebnosti), ki se jo lahko doseže z uporabo biometričnih metod se kaže v dveh bistvenih pridobitvah za zasebnost. Prvič se s tem doseže, da je dostop npr. do podatkovnih baz osebnih podatkov dostopen le avtoriziranemu osebu in, kar je še zanimivejše, lahko se natančno ugotovi kdo, kdaj in o kom je pregledoval podatkovne baze z osebnimi podatki, saj za sabo pušča elektronsko sled.

Drugi primer je zanesljivo povezovanje prave identitete človeka z njegovimi identifikacijskimi dokumenti, ki morajo biti obenem tudi težko za prenarediti, ponarediti, ukrasti ipd. Če se to doseže (kar menim, da je vsekakor možno), je rezultat tega preprečitev oz. zmanjšanje možnosti identitetne kraje in zlorabe, dostopa neavtoriziranih posameznikov idr., kar je seveda (če le-to tudi res deluje) izreden doprinos k zasebnosti, saj praktično ni hujše kršitve zasebnosti, kot je identitetna kraja.

Vseeno pa je na mestu tudi slednja trditev. "Kakor koli že, trditi, da so biometrične metode zaveznik zasebnosti, nevarno podcenjuje količino dela in prizadevanj, ki so potrebna, da bo to res" (Van der Ploeg, 2003: 101).

9.2 BIOMETRIČNE METODE KOT 'SOVRAŽNIK oz. NASPROTNIK' ZASEBNOSTI

Nekateri zagovorniki zasebnosti opisujejo biometrične metode celo kot glavno grožnjo zasebnosti, nekateri pa celo kot konec svobodnega sveta, kot ga poznamo.

Clarke (Crompton, 2002: 7) tako meni, da so “biometrične metode ena izmed najbolj grozečih od vseh nadzornih tehnologij in najavljajo neobzirno zmanjšanje svoboščin in zatiranje različno mislečih zagovornikov javnega interesa in tistih, ki povzročajo težave”.

Pri navajanju biometričnih metod kot sovražnika zasebnosti smo priča precej 'argumentom', izmed katerih so nekateri zelo realni in vredni pozornosti, spet drugi malo manj. Predstavil bom tudi to drugo vrsto, saj je navsezadnje potrebno odgovoriti na vsa takšna vprašanja, če naj bo uporaba biometričnih metod dobro sprejeta s strani državljanov oz. uporabnikov.

- Izguba individualne neodvisnosti in anonimnosti

“Glavna kritika biometričnih metod je, da mi, kot posamezniki, tvegamo izgubo naše anonimnosti in neodvisnosti, kadar koli so uporabljeni biometrični sistemi” (Woodward, Orlans in Higgins, 2003: 204). Torej, da nimamo več nadzora nad informacijami o nas samih in ne nadzora nad tem, kdo nas lahko zaznava, kar pride do izraza predvsem, kadar so uporabljeni prikriti biometrični sistemi.

- Biometrične metode kot sredstvo nadzora države nad državljani – scenarij 'velikega brata'

Kritiki pravijo, da kombinacija biometričnih metod in velik napredek v računalniških in podobnih tehnologijah, državi omogoča spremljanje dejanj in obnašanja njenih državljanov (Woodward, Orlans in Higgins, 2003: 206). Ta možnost se zdi v razvitih demokratičnih družbah precej omejena in manj verjetna (čeprav do določene mere možna in celo že videna), precej drugačno pa je stanje v totalitarnih režimih, ki imajo tako ali tako že brez biometričnih metod željo pa nadzorovanju nad svojimi državljani in bi jim biometrične metode lahko pomenile še dodatno sredstvo v njihovih naporih.

- T.i. function creep

T.i. function creep je problem, ko se biometrične informacije zbrane z nekim namenom naknadno uporabijo širše in tako posameznik izgubi nadzor nad osebnimi informacijami (Biometric&Security, 2001: 4). Klasičen primer takšne zlorabe se je v ZDA zgodil na primeru številke socialnega zavarovanja (SSN), ko ob uvedbi leta 1936 nikakor ni bila namenjena za identifikacijske namene. Danes ta ista številka služi kot “praktično predpisana identifikacija” (Woodward, Orlans in Higgins, 2003: 207, 208). Tudi danes nismo daleč podobnim primerom, saj se (tudi biometrični) podatki delijo po različnih podatkovnih bazah z različnimi nameni in celo med civilnimi in kriminalnimi podatkovnimi bazami različnih držav.

- Kulturni, verski, filozofski in higienski pomisleki.

“Avtomatične metode individualne prepoznavne, še posebej tiste, ki temeljijo na biometriji, so lahko kulturno zaznane kot nedostojanstvene za človeka /.../, ker nosijo negativno konotacijo zaradi njihove prevladujoče uporabe v kazenskih preiskavah” (Prabhakar, Pankanti in Jain, 2003: 41).

“Nekatere biometrične metode so zaradi svoje narave (merijo karakteristike delov človekovega telesa ali pa vedenjske lastnosti posameznikov) in zaradi zgodovine njihove uporabe (uporaba prstnih odtisov na področju kriminalistike) v javnosti sprejete z določeno stopnjo nezaupanja in zadržanosti” (Fefer, 2004: 152).

“Različne verske skupine kritizirajo biometrične metode, saj naj bi bili posamezniki prisiljeni žrtvovati del sebe brezbožnemu monolitu v obliki države” (Woodward, Orlans in Higgins, 2003: 209). Pogosto se navaja primer določenih kristjanov, ki interpretirajo biometrične metode kot vsiljevanje 'znamenja zveri', kar temelji na zapisu v razodetju (13: 16-18) (Woodward, Orlans in Higgins, 2003: 209).

Filozofski pomisleki temeljijo na tem, da so biometrični podatki pojmovani kot biometrično označevanje in visoko tehnološko tetoviranje, kar naj bi spominjalo na označevanje sužnjev kot lastnine v 18. in 19. st. ter tetoviranje, ki so ga uporabljali nacisti za identifikacijo ljudi zaprtih v koncentracijskih taboriščih (Woodward, Orlans in Higgins, 2003: 210).

Higienski pomisleki temeljijo na strahu nekaterih ljudi pred senzorji, ki zahtevajo dotik in so uporabljani s strani veliko ljudi (Prabhakar, Pankanti in Jain, 2003: 41).

- Pridobitev občutljivih (medicinskih) informacij

Obstaja možnost, da se z zajemom biometričnega podatka, poleg namena prepoznavne ugotovijo še nekatere človekove zdravstvene lastnosti. “Možno je, da lahko skeniranje šarenice razkrije ali je nekdo nagnjen h kapi; kar je nekaj, kar posameznik ne bi rad, da ve tudi njegov delodajalec ali zavarovalnica” (Biometrics&Security, 2001: 4).

- Fizična poškodba

Nekateri se bojijo, da jih lahko nekatere biometrične metode celo fizično poškodujejo, kot npr., da bi skeniranje šarenice lahko poškodovalo posameznikov vid.

Dokumentiranih primerov, ko naj bi biometrični sistem dejansko povzročil poškodbo ni, je pa res, da je večina biometričnih tehnologij relativno novih (Woodward, Orlans in Higgins, 2003: 210).

- Kraja biometričnih podatkov

Grožnjo zasebnosti Cavoukian (1998 v Van der Ploeg, 2003: 97) vidi tudi v “zmožnosti nekoga tretjega, da dobi dostop do te identifikacijske oblike in jih poveže z drugimi informacijami, kar se odrazi v nepredvideni uporabi te informacije brez privoljenja subjekta”. Ta možnost se kaže s pomočjo kraje in/ali ponarejanja nekega biometričnega podatka kot npr. prstnega odtisa, s pomočjo katerega bi lahko imela tretja oseba dostop do določenih območij, spletnih strani, podatkov idr. Je pa res, da je že prevara boljših sodobnih čitalcev prstnih odtisov precej težka, kaj šele kakšnih drugih biometričnih podatkov, ki ne puščajo latentnih sledi.

9.3 VARNOSTNI IN DRUGI UKREPI, KI OMOGOČAJO VARNEJŠO UPORABO BIOMETRIČNIH METOD V RAZMERJU DO ZASEBNOSTI

Potrebno je storiti vse, da se pri uporabi biometričnih metod izkoristijo njene najboljše lastnosti in omejijo ali odpravijo slabosti oz. pomanjkljivosti tudi v zvezi z vprašanjem ogrožanja zasebnosti. Zelo prepričljivo izzvenijo besede Ann Cavoukian (1998 v Van der Ploeg, 2003: 90), ko pravi: “/o/bstoj strogih zaščit tako pravnih, proceduralnih kot tudi tehnoloških bo postalo ključno, če naj biometrične metode postanejo zaveznik zasebnosti”.

V ACLU¹¹⁸ verjamejo, da mora biti “uporaba vsiljivih novih nadzornih tehnologij podvržena procesu pazljivega in tehtnega nadzora. Še posebno, vsiljivost tehnologije mora biti uravnotežena z varnostnimi pridobitvami, ki naj jih doseže. Breme je na tehnologijah, da prikažejo, da bodo njihove rešitve v resnici učinkovite pri ustvarjanju večje varnosti” (ACLU opposes use of face recognition software in airports due to the ineffectiveness and privacy concerns, 2002).

“Verjamemo, da lahko izboljšamo varnost, ne da bi se odpovedali varnosti do zasebnosti. Ključ leži v zagotovitvi odgovorne uporabe, tako da ti sistemi, ki so namenjeni za odkrivanje teroristov, niso zlorabljeni za namene, za katere niso namenjeni” (Visionics Corporation, 2001: 6).

“Temelj odgovorne uporabe leži v naslednjem:

- vedenju javnosti,
- integriteti podatkovnih baz,

¹¹⁸ American Civil Liberties Union – Ameriška zveza za državljanske svoboščine.

- brez zadetka – brez zaznamka,
- avtoriziranem delovanju in dostopu,
- uveljavljanje in kaznovanje” (ibidem).

Poleg naštetih bi omenil še nekaj drugih.

- Kriptiranje in kodiranje

“Sistemi, ki vključujejo shranjevanje podatkov njihovo predelovanje in prenos /.../ so predmet možnih vdorov ter neavtoriziranega dostopa, uporabe in razkritja” (Crompton¹¹⁹, 2002: 12). Zatorej so potrebni ukrepi, ki kaj takega preprečujejo, če pa se to že zgodi, onemogočajo 'branja' takih podatkov, kar lahko omogoči kriptiranje in kodiranje.

- Nadzor tako nad civilnimi kot vladnimi aplikacijami

Da se bo v delujoči demokraciji nadziralo vladne aplikacije, je bolj kot ne logično in razumljivo, kar pa še ni zadosti. Potrebno je uvesti tudi nadzorne mehanizme, ki bodo nadzorovali tudi stanje v civilnih aplikacijah biometričnih metod, saj lahko tudi tam prihaja do kršenja zasebnosti.¹²⁰

- Pravno urejanje

Pravna zaščita bi lahko vključevala posebne ukrepe:

- vzpostavitev sistemov, v katerih uporaba podatkov za druge namene kot za tiste, ki so bili zbrani ne bi bila mogoča brez posebne zakonske pooblastitve,
- ločitev biometričnih podatkov in ostalih osebnih podatkov,
- varnostni ukrepi, ki upoštevajo grožnje zasebnosti,
- točno določena zakonska pooblastitev za uporabo biometričnega sistema,
- močni mehanizmi za odgovornost in transparentnost kot npr.: ravnanje s pritožbami, podatki o tem, kdo je dostopal do sistema idr. (Crompton, 2002: 22, 23).

“Zaradi hitrega tehnološkega napredka na področju biometrije in zaradi vse širše uporabe le-te, bo za uspešno varovanje osebnih podatkov potrebna konkretnjša pravna regulacija tega področja” (Fefer, 2004: 155).

¹¹⁹ Malcolm Crompton je avstralski zvezni pooblaščenec za zasebnost oz. je le to bil za časa objave članka.

¹²⁰ Če smo pozorni, pogosto vidimo nadzorne kamere v trgovinah, fitness klubih idr., ki očitno ne delujejo v skladu z zakonom o varstvu osebnih podatkov (ZVOP-1). Ta problem bi postal še precej hujši, če bi obstoječe nadzorne kamere nadgradili s programski opremo obrazne prepoznavne. O ZVOP-1 podrobneje v nadaljevanju.

- Samoregulacija

Gre predvsem za nekakšen poziv podjetjem, ki izdelujejo biometrične sisteme, da se že sami zavežejo k 'ustvarjanju' sistemov, ki ne bodo mogli kršiti zasebnosti.

- Sorazmernost uporabe

S tem je mišljeno, da tudi npr. organi pregona ne bi uporabljali biometričnih metod, če lahko z ostalimi metodami dosežejo enake rezultate.

- Problem nepovratnosti

“Ko nekdo ukrade vaš biometrični podatek, ostane ukraden celo življenje” (Schneier v Crompton, 2002: 11). Kar je deloma res, zato je potrebno v vsakem sistemu predvideti tudi takšno možnost in sistemske rešitve tega problema.

9.4 ZAKON O VARSTVU OSEBNIH PODATKOV (ZVOP-1) V RS IN UPORABA BIOMETRIČNIH METOD

Biometrične metode vedno bolj postajajo del vsakdanjega življenja ljudi. V Sloveniji se bomo kmalu srečali z biometričnimi potnimi listi in drugimi biometričnimi aplikacijami. Zakon o varstvu osebnih podatkov iz leta 1999 nikjer ne omenja oz. ne predvideva uporabe biometričnih metod, zato se je izkazala potreba po novem takem zakonu, kar se je uresničilo 1. 1. 2005, ko je začel veljati nov zakon o varstvu osebnih podatkov, ki za razliko od prejšnjega vsebuje tudi člene, ki se dotikajo biometričnih metod. Na kratko bom opisal tiste člene, ki so zanimivi iz konteksta obravnavane teme.

V 19. točki 6. člena so v zakonu kot občutljivi osebni podatki tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi z rasnim, narodnim ali narodnostnim poreklom, političnim, verskim ali filozofskim prepričanjem idr. V 21. točki istega člena je podana definicija biometrične značilnosti.

Poleg tega pa je celotno 3. poglavje (78. - 81. člen) namenjeno biometriji.

78. člen: Splošna določba

Z obdelavo biometričnih značilnosti se ugotavljajo ali primerjajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija oziroma preveri njegova identiteta (v nadaljnjem besedilu: biometrijski ukrepi) pod pogoji, ki jih določa ta zakon.

79. člen: Biometrijski ukrepi v javnem sektorju

(1) Biometrijske ukrepe v javnem sektorju se lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

(2) Ne glede na prejšnji odstavek se biometrijske ukrepe lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja.

80. člen: Biometrijski ukrepi v zasebnem sektorju

(1) Zasebni sektor lahko izvaja biometrijske ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Biometrijske ukrepe lahko izvaja le nad svojimi zaposlenimi, če so bili predhodno o tem pisno obveščeni.

(2) Če izvajanje določenih biometrijskih ukrepov v zasebnem sektorju ni urejeno z zakonom, je upravljavec osebnih podatkov, ki namerava izvajati biometrijske ukrepe, dolžan pred uvedbo ukrepov posredovati državnemu nadzornemu organu opis nameravanih ukrepov in razloge za njihovo uvedbo.

(3) Državni nadzorni organ je po prejemu posredovanih informacij iz prejšnjega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometrijskih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se lahko podaljša za največ en mesec, če bi uvajanje teh ukrepov prizadelo več kot 20 zaposlenih v osebi zasebnega sektorja, ali če reprezentativni sindikat pri delodajalcu zahteva sodelovanje v upravnem postopku.

(4) Upravljavec osebnih podatkov sme izvajati biometrijske ukrepe po prejemu odločbe iz prejšnjega odstavka, s katero je izvajanje biometrijskih ukrepov dovoljeno.

(5) Zoper odločbo državnega nadzornega organa iz tretjega odstavka tega člena ni pritožbe, dovoljen pa je upravni spor.

81. člen: Biometrijski ukrepi v zvezi z zaposlenimi v javnem sektorju

Ne glede na določbe 79. člena tega zakona se v javnem sektorju lahko uvedejo biometrijski ukrepi v zvezi z vstopom v stavbo ali dele stavbe in evidentiranjem prisotnosti zaposlenih na delu, ki se izvedejo ob smiselni uporabi drugega, tretjega in četrtega odstavka 80. člena tega zakona.

V 99. in 100. členu pa so navedene še globe za kršitev določb o biometriji v javnem in zasebnem sektorju v višini od 300.000 sit do 3.000.000 sit.

Bistvo tega zakona na področju preučevanja je seveda 3. poglavje, ki je v celoti namenjeno biometriji. Glede na to, da je vprašanje zasebnosti največkrat povezano z

vpeljavo biometričnih rešitev s strani države oz. njenih organov je še posebno pomemben 79. člen – biometrijski ukrepi v javnem sektorju. Gre za precej omejitvena določila, ki predvidevajo uporabo 'biometrijskih ukrepov' le na podlagi zakona in ob drugih strogih omejitvah. Menim, da je tako omejitveno pisan zakon nedvomno v interesu javnosti, saj je na ta način omejena možnost zlorabe biometrijskih ukrepov s strani državnih organov, ki bi lahko takšne ukrepe uporabljali le na podlagi uredb ali navodil.

Po mojem mnenju pa je ustrezno urejeno tudi področje biometrijskih ukrepov (80. člen) v zasebnem sektorju. Uvajanje takšnih ukrepov mora biti urejeno z zakonom ali pa mora upravljavec pred uvedbo dobiti soglasje državnega nadzornega organa.

Da zakon ne bo ostal le 'mrtva črka na papirju' bo potrebno zagotoviti nadzorovanje tega področja s strani nadzornih organov in dosledno ter hitro kaznovanje kršiteljev. To bo po mojem mnenju še najtežji del. Slabe izkušnje pri takšnem nadzoru so se izkazale pri videonadzoru. Kršitve zakonskih določil so pri videonadzoru vidne pozornemu posamezniku kadar koli se sprehodi po npr. trgovinskih centrih, v javnost pa so pred časom prišli tudi posnetki, ki v javnost nedvomno ne bi smeli priti in so očitno kršili posameznikovo zasebnost.

Trenutno je zakon po mojem mnenju ustrezen in bo služil za varovanje osebnih podatkov tudi pri uporabi biometrijskih ukrepov. Menim pa, da bo potrebno stalno spremljanje tega področja, ker ga bo sčasoma, zaradi hitrega razvoja tehnologije in njenih aplikacij, potrebno tudi ustrezno dopolnjevati in/ali spreminjati.

Ob koncu celotnega poglavja o zasebnosti bi rad še enkrat poudaril, da gre pri vprašanju zasebnosti pri uvajanju biometričnih metod za kompleksno zadevo in poenostavljanje v smislu, da so biometrične metode le zaveznik ali le sovražnik zasebnosti neutemeljene in nekoristne. Dejstvo je, da gre za tehnologijo, ki ob zlorabi omogoča tudi vdor v posameznikovo zasebnost, toda takšnih tehnologij je več (npr. prisluškovalne naprave, video kamere idr.), pa so kljub temu prepoznane kot nujno potrebne v najrazličnejše namene. Menim, da je potrebno, da se javnost obvešča o obstoju oz. uporabi teh metod ter predvsem, da se zagotovi delovanje v okviru točno določenih (ustreznih) pravnih okvirov. Ko in če bo to in še nekaj drugih omenjenih pogojev izpolnjenih, bomo lahko videli oz. doživljali predvsem koristne strani biometričnih metod tudi z vidika zasebnosti.

10. ZAKLJUČEK IN VERIFIKACIJA HIPOTEZ

Prva hipoteza, ki sem jo postavil se glasi '*Biometrične metode so bile za preprečevanje terorizma uporabljane že pred 11. 9. 2001*'. Takojšen odgovor ni mogoč, zato bom najprej osvetlil ozadje, na podlagi katerega bo moč podati verifikacijo hipoteze. V okviru preprečevanja terorizma s pomočjo biometričnih metod je prvi meni znan projekt Human ID (prepoznavna človeške identitete na daljavo v okviru TIA), ki je posledica terorističnih napadov, in sicer na Khobar Towers v Savdski Arabiji leta 1996. Zaradi tega so v okviru DARPA leta 2000 začeli s programom Human ID, ki je imel za cilj s prepoznavo znanih teroristov na daljavo preprečiti tovrstne in podobne teroristične napade. Teroriste bi po prepoznavi lahko onemogočili, še preden bi uspeli delovati. Toda ta projekt je ostal nedokončan in ni začel delovati ne pred 11. 9. 2001 ne kasneje. Drugi možni primer predstavlja poskus oblasti v kraju Tampa na Floridi v ZDA januarja 2001, ko so posneli vse ljudi, ki so se udeležili dogodka, in jih s pomočjo obrazne prepoznave primerjali s podatkovnimi bazami kriminalcev in teroristov. Šlo je le za poskus, tako da prepoznavam niso sledile aretacije, kljub 19 zadetkom. Sklepam pa lahko, da bi oblasti ukrepale, če bi sistem prepoznal kakšnega terorista. Tudi v tem primeru je šlo za poskusni projekt, ki se kasneje ni splošno uporabljal. Na podlagi opisanega zavračam prvo hipotezo z omembo, da so potekali poskusi in napor v smeri preprečevanja terorizma s pomočjo biometričnih metod, vendar se v praksi niso 'materializirali'.

Drugo hipotezo, ki se glasi '*Najprimernejša biometrična metoda za preprečevanje terorizma je obrazna prepoznavna*' delno potrjujem. Razlogi za to so predvsem naslednji. Biometrična metoda prepoznave obraza je trenutno edina, ki ima realno možnost prepoznav na daljavo in je že precej tehnološko razvita. Fotografije oz. posnetki teroristov so večinoma edini dostopni (biometrični) podatek o njih, kar omogoča prepoznavo teroristov, saj so biografski podatki s precejšnjo lahkoto ponarejeni, ukradeni... Biometrična metoda prepoznave obraza omogoča tudi nadzor nad določenimi (varnostno tveganimi) območji in v realnem času ugotavlja identiteto ljudi (seveda le tistih, ki so zajeti v podatkovnih bazah, po katerih sistem išče). To so precej optimistični razlogi v prid obrazni prepoznavi. Pomembnost obrazne prepoznav se kaže tudi v projektih, kot je bil npr. Human ID, katerega glavna (a ne edina) sestavina prepoznav na daljavo je bila prav obrazna prepoznavna in FRVT

testi, v katerih sodeluje veliko vladnih agencij (ne samo iz ZDA) in to na velikih vzorcih. Razlog, da le delno potrjujem hipotezo, je predvsem v tem, da ima tehnologija precejšnje težave s točnostjo sistemov, ki so predvsem posledica zajema slike v nekontroliranem okolju in nekooperativnost nekaterih posameznikov, ki se kaže v njihovem maskiranju ali teoretično celo s plastično operacijo. Je pa po drugi strani tudi res, da se tehnologija obrazne prepoznavne nenehno izboljšuje in da se nekatere omenjene pomanjkljivosti odpravljajo. Obrazna prepoznavna je za preprečevanje terorizma najprimernejša biometrična metoda, saj se ukvarja s prepoznavo znanih teroristov, vendar pa je podvržena tudi številnim tehničnim težavam.

Tretja hipoteza se glasi *'Poglavitna 'dodana vrednost' biometričnih metod kot oblike preprečevanja terorizma je v njihovi zastraševalni oz. odvračevalni vlogi'*. Zaradi pomanjkanja empiričnih dokazov bi težko sodil o hipotezi, ostaja pa dejstvo, da ZDA, kljub implementaciji velikopoteznega programa US-VISIT in tudi drugih programov (verjetno) niso 'ujeli' nobenega terorista oz. tega nočejo povedati. Ali to pomeni, da so se teroristi izognili sistemu, da jih sistem ni našel ali pa program dejansko vpliva zastraševalno in odvračevalno, je težko soditi, ustrezne odgovore bomo verjetno dobili v prihodnosti. Ostaja pa dejstvo, da je sistem odkril večjo število kriminalcev, ki so jih iskali organi pregona, kar v določeni meri potrjuje, da je sistem vsaj delno uspešen. In prav ta uspešnost sistema bo (če ne že) verjetno delovala zastraševalno oz. odvračalno, kar se bo odrazilo v tem, da bodo teroristi (in kriminalci oz. vsi tisti, ki so iskani v podatkovnih bazah) iskali druge poti, v tem primeru prestopa meje z ZDA. Hipotezo lahko torej potrdim le delno oz. z 'zadržkom'.

Četrta hipoteza se je glasila *'Pri uvajanju biometričnih metod so najodločnejši akter ZDA, v EU in Sloveniji pa na tem področju ni (bilo) storjenega dovolj'* in jo delno potrjujem. Vsekakor menim, da so ZDA najodločnejši akter pri uvajanju biometričnih metod s ciljem preprečevanja terorizma. O tem priča vrsta programov, med katerimi izstopa predvsem US-VISIT, ki je po svojem obsegu ogromen in zajema vse meje z ZDA. Bistvo US-VISIT pa je, da bo moral vsak posameznik, ki bo želel vstopiti v ZDA, predstaviti svoje biometrične podatke, ki se jih bo nato primerjalo z veliko podatkovnimi bazami, na potnem listu (države programa VWP) ali vizi (za ostale države). Do popolne uvedbe biometričnih potnih listov držav VWP se bo takšne biometrične podatke odvzelo ob prehodu meje. ZDA so s tem tudi glavno svetovno 'gonilo' implementacije biometričnih potnih listov. Poleg tega poteka v ZDA še vrsta

programov, kot so opisani INSPASS, TWIC pa tudi dostop do npr. jedrskih tovarn, ki je ščiten s pomočjo biometričnih metod, testiranja tehnologije obrazne prepoznavne na velikem vzorcu (FERET, FRVT 2000, 2002, 2005) in mnogo drugega. Nenazadnje ima samo Ministrstvo za domovinsko varnost (DHS) več kot 60 programov, ki uporabljajo biometrične metode, čeprav seveda niso vse v povezavi s preprečevanjem terorizma. Da v okviru EU in Slovenije ni bilo storjenega dovolj, bi težko potrdil, saj je kljub vsemu sedaj jasno, da bosta EU in Slovenija vpeljali v uporabo biometrične potne liste in vize. Sicer je očitno, da na ravni Slovenije in EU poteka bistveno manj aktivnosti povezanih z uporabo biometričnih metod pri preprečevanju terorizma, kar pa je posledica tako objektivnih (npr. manjša grožnja terorizma kot so ji priča ZDA) kot subjektivnih (npr. večji občutek varnosti državljanov EU). Glede na povedano sem mnenja, da EU in Slovenija relativno ustrezno ukrepata pri uvajanju biometričnih metod in se upirata uvajanju povečanih nadzornih mehanizmov države, pri čemer temu, po mojem mnenju, sledi tudi nov zakon o varstvu osebnih podatkov. Pri stanju v Sloveniji in EU me čudi predvsem dvoje. Prvič, zakaj bi morali (nanašam se na Projekt 2004 in Projekt 2005) mejne prehode opremiti z napravami za preverjanje biometričnih potnih listov, glede na to, da bodo tudi po uvedbi biometričnih potnih listov, stari potni listi veljali še do njihovega izteka in se bo tako biometrično preverjanje izvajalo le za lastnike biometričnih potnih listov, kar pa je po mojem mnenju sporno. In drugič, zelo neracionalno in konfuzno je uvajanje biometričnih elementov v dveh fazah z 18 mesečnim zamikom, saj bo to privedlo do več težav, predvsem ponovno prilagajanje postopkov za nove biometrične elemente ter dejstvo, da bodo v uporabi istočasno tri vrste potnih listov; sedanji 'običajni' brez biometričnih elementov, biometrični z enim biometričnim elementom (obrazna slika) ter biometrični z dvema biometričnima elementoma (obrazna slika in dva prstna odtisa). Očitno je, da je to stanje nastalo zgolj zaradi pritiskov ZDA, posledice, tudi finančne, pa bomo nosili tudi uporabniki. Poleg tega menim, da bi bilo tako v okviru Slovenije kot tudi v okviru EU smotrno v večji meri vpeljevati biometrične metode predvsem tam, kjer so bile do sedaj že preizkušene, da delujejo dobro in zanesljivo, tj. pri dostopu do občutljivih objektov oz. sredstev, ki bi lahko pomenila možne tarče ali sredstva za teroriste.

Peta hipoteza se glasi *'Uvajanje biometričnih metod pomeni vdor v zasebnost posameznika'*. Pri tej temi gre za najkompleksnejše in najobčutljivejše vprašanje pri uvajanju biometričnih metod ne samo na področju preprečevanja terorizma, temveč

povsod tam, kjer se le te uvaja v uporabo. Če bi pogledali problematiko le z enega ali drugega zornega kota, bi našli precej argumentov tako za zavrnitev kot potrditev hipoteze. Problem je v tem, da ista tehnologija omogoča tako varovanje kot vdor v zasebnost. O tem, da biometrične metode lahko pomenijo vdor v zasebnost, ni dvoma (npr. zloraba nadzornih zmožnosti obrazne prepoznavne), obenem pa dvoma ni tudi o tem, da lahko biometrične metode pomenijo varovanje zasebnosti posameznika (dostop do baz osebnih podatkov le avtoriziranih posameznikov). Zato je pri uvajanju biometričnih metod izrednega pomena, da se za njihovo implementacijo zagotovi ustrezna zakonodaja, ki bo vsebovala varnostne mehanizme, ki bodo preprečevali možne zlorabe tako v civilnih kot vladnih aplikacijah. Glede na to menim, da ob ustrezni legalni in legitimni uporabi biometričnih metod, lahko le-te pripomorejo celo k varovanju zasebnosti in bi s tega vidika, torej ob upoštevanju naštetega, hipotezo zavrnil. Na mestu je po mojem mnenju ugotovitev Altermana, ko pravi, da "glavna grožnja zasebnosti nastaja zaradi zlorabe in ne zaradi uporabe".

Biometrične metode se vedno bolj uveljavljajo na vseh področjih. Gre za tehnologijo, katere princip je poznan že dolgo, avtomatizacijo pa je omogočil razvoj strojne in programske opreme. Predvsem v zadnjih letih je viden zelo velik napredek, ko se hitro pojavljajo nove biometrične metode in bistveno izboljšujejo 'stare'. Verjetno se bodo biometrične metode pospešeno razvijale še naprej, dileme, ki so danes zelo aktualne in problematične (točnost, hitrost, kooperativnost idr.), pa se bodo sčasoma zmanjšale in tudi odpravile. Gre za tehnologijo, ki ima, bolj kot katera koli druga trenutno dostopna tehnologija, zmožnost zanesljivega prepoznavanja ljudi, zaenkrat še predvsem v potrjevanju identitete (verifikacija).

Ta dejstva so naredila biometrične metode zelo zanimive organom pregona, za katere je ugotavljanje identitete posameznikov velikokrat ključno za njihovo učinkovito in uspešno delo. Po dogodkih 11. 9. 2001 so predvsem v ZDA videli velik potencial v biometričnih metodah kot sredstvu preprečevanja terorizma. Občutek sem dobil, da je prvotno navdušenje in prevelika pričakovanja zamenjalo trezno razmišljanje in ugotovitev, da je potreben še nadaljnji razvoj teh metod in 'pametna' implementacija tam, kjer biometrične metode že sedaj lahko okrepijo varnost. Ugotovim lahko, da biometrične metode niso 'srebrni metek' za preprečevanje

terorizma, vsekakor pa nudijo nekatere možnosti, ki lahko delujejo komplementarno pri preprečevanju terorizma.

SEZNAM SLIK, GRAFOV IN TABEL

Slika 3.1: Štiristopenjski postopek biometričnega sistema	9
Slika 6.2: Grafični prikaz poteka obrazne prepoznavе.....	26
Slika 6.3: Osnovni vzorci prstnih odtisov	32
Slika 6.4: Najpogostejše individualne značilnosti: linija, vilice in pika	33
Slika 6.5: Slike prstnih odtisov, zajetih na različne načine	33
Slika 6.6: Šarenica.....	35
Slika 6.7: Lociranje šarenice.....	35
Slika 6.8: Sistem za analizo šareničnega vzorca.....	36
Slika 6.9: Različni primeri delovanja multimodalnega biometričnega sistema	39
Slika 7.10: Grafični prikaz delovanja prepoznavе identitete ljudi na daljavo	51
Slika 8.11: Delovni postopek izdaje biometričnega potnega lista	59
Slika 8.12: Grafični prikaz delovanja US-VISIT na primeru letališč in pristanišč.....	66
Graf 3.1: Delež napačnih odobritev/zavrnitev	11
Graf 3.2: Prikaz izbire stopenj napak glede na aplikacijo biometričnega sistema.....	11
Tabela 6.1: Karakteristike biometričnih tehnologij.....	41

11. SEZNAM VIROV

KNJIGE:

1. Chirillo, John in Scott Blaul (2003): Implementing Biometric security. Indianapolis: Wiley Publishing.
2. Heymann, Philip B. (2003): Terrorism, Freedom and Security: Winning Without War. Cambridge, Massachusetts in London: The MIT Press.
3. Lyon, David (2003): Surveillance after September 11. Cambridge: Polity Press.
4. Medicinska Enciklopedija (1980): 3. zvezek, 1. knjiga, Ljubljana: Državna Založba Slovenije, str. 127.
5. Slovenski medicinski slovar (2002): Ljubljana: Medicinska fakulteta, str. 97.
6. Smolej, Gregor (2003): Kaj je terorizem? Diplomaska naloga. Ljubljana: FDV.
7. Slovar slovenskega knjižnega jezika (1994): Ljubljana: Državna Založba Slovenije, str. 46, 113, 395, 1012.
8. Trapečar, Matej (2003): Prometne nesreče – uporabnost sodobnih biometričnih metod pri policijskih postopkih ugotavljanja istovetnosti udeležencev. Magistrsko delo. Portorož: Fakulteta za pomorstvo in promet, str. 74-90.
9. Woodward, John D. Jr., Nicholas M. Orlans in Peter T. Higgins (2003): Biometrics. New York: McGraw-Hill.

ČLANKI:

1. Alterman, Anton (2003): A piece of yourself: Ethical issues in biometric identification. Ethics and Information Technology, 5(3), 139-150.
2. Ceglar, Miha (2005): EU zaprosila ZDA za odlog. Delo, 8. 4. 2005: 17.
3. Črnčec, Damir (2004b): Človekove pravice in sodobna demokratična država. Revija Obramba, 36(5), 8-11.
4. Črnčec, Damir (2004a): Biometrija: Sodoben način zagotavljanja varnosti!? Revija Obramba, 35(2), 19-21.

5. Drobnič, Katja (2001): Vpliv zbirke podatkov DNK na učinkovitost preiskovanja kaznivih dejanj. *Varstvoslovje*, 3(3), 141-148.
6. Fefer, Dušan (2004): Uporaba biometričnih tehnologij v sistemih pristopne kontrole. *Varstvoslovje*, 6(2), 148-156.
7. Ganor, Boaz (2002): Defining Terrorism: Is one man's terrorist another man's freedom fighter? *Police Practice and Research* 3(4), 287-304.
8. Jonietz, Erika (2004): Boosting biometrics. *Technology Review*, junij: 20-21.
9. Marois, Denise (2004): Lawmakers Eye Loopholes In Visa Program, US VISIT. *Aviation daily*, 23. 8.: 3.
10. Milone, Mark G. (2001): Biometric Surveillance: Searching for Identity. *The Business Lawyer* 57(1), 497-512.
11. Ploeg, Irma van der (2003): Biometrics and privacy. A note on the politics of theorizing technology. *Information, Communication & Society* 6(1), 85-104.
12. Ridge, Tom (2004): U.S. is more secure. *USA Today*, 2. 2.: 11.
13. Rizman, Rudi (2004): Naši borci, njihovi teroristi: njihovi teroristi, naši borci. *Sobotna priloga* 11. 9.
14. Ruby, Charles L. (2002): The definition of Terrorism. *Analyses of Social Issues and Public Policy*, 9-14.
15. Sorel, Jean-Marc (2003): Some Questions About the Definition of Terrorism and the Fight Against Its Financing. *EJIL* 14(2), 365-378.
16. Stein, Nicholas (2004): America's 21st-Century Borders. *Fortune*, 6. 9.: 114-118.
17. Steinhardt, Barry (2003): Does Privacy Have a Future after 9/11?. *Journal of Contingencies and Crisis Management* 11(1), 32-36.
18. Symeonidou-Kastanidou, Elisabeth (2004): Defining Terrorism. *European Journal of Crime, Criminal Law and Criminal Justice*, 12(1), 14-35.
19. Trapečar, Matej in Andrej Robek (2003): Sodobne biometrične metode pri verifikaciji identitet posameznikov ter njihova uporabnost v letalskem prometnem sistemu. *Varstvoslovje* 5(1), 49-56.
20. Trapečar, Matej in Gorazd Vidic, (2004): Vloga in pomen sistema AFIS v slovenski policiji. *Varstvoslovje* 6(2), 180-185.
21. Turner, Allan (2003): Biometrics in Corrections: Current and Future Deployment. *Corrections Today*, julij: 62-64.

22. Welsch, Brandon C. in David P. Farrington (2004): Surveillance for Crime Prevention in Public Space: Results and Policy Choices in Britain and America. *Criminology and Public Policy* 3(3), 497-526.

PRISPEVKI, GRADIVO, ANALIZE Z MEDMREŽJA:

1. 1999 Glossary of Biometric Terms (1999): <http://www.afb.org.uk/downloads/glossary.pdf> (9. 3. 2005).
2. A Brief History of Biometrics (2004): http://www.galwayeducationcentre.ie/athenry/a_brief_history_of_biometrics.htm (9. 3. 2005).
3. ACLU opposes use of face recognition software in airports due to the ineffectiveness and privacy concerns (2002), <http://www.aclu.org/Privacy/Privacy.cfm?ID=9397&c=39> (9. 3. 2005).
4. Alphonse Bertillon and Ear Prints (2005): http://www.forensic-evidence.com/site/ID/ID_bertillion.html (9. 3. 2005).
5. Belasco, Amy (2003): Total Information Awareness Programs: Funding, Composition, and Oversight Issues. Report for Congress, http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL31786_03212003.pdf (9. 3. 2005).
6. Biometric Glossary and Abbreviations (2005): <http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=401> (9. 3. 2005).
7. Biometrics & Security (2001): <http://www.parliament.uk/post/pn165.pdf> (9. 3. 2005).
8. Biometrics and Counter-Terrorism (2001): <http://www.ibia.org/Press%20Release%209.21.01.htm> (20.10.2004 – stran ni več dostopna).
9. Biometrics Market and Industry Report 2004-2008 (2005): http://www.biometricgroup.com/reports/public/market_report.html (9. 3. 2005).
10. Bowman, Erik (2000): Everything You Need to Know About Biometrics, <http://www.ibia.org/EverythingAboutBiometrics.PDF> (10.11.2004 - stran ni več dostopna).
11. Buxbaum, Peter A. (2005): The Biometrics Dilemma. V *Homeland Security*, jan/feb 2005, str. 14-17, http://www.mcgraw-hillhomelandsecurity.com/media/pdf/HSQ/HLS_Article02_issue_6.pdf (9. 3. 2005).

12. Cataract and Refractive Eye Care Glossary (2005):
<http://www.ascrs.org/eye/gloss.html> (9. 3. 2005).
13. Cavoukian, Ann (2002): Security Technologies Enabling Privacy (STEPS): Time for a Paradigm Shift, <http://www.ipc.on.ca/docs/steps.pdf> (9. 3. 2005).
14. Cerar, Gregor (2005): Biometrična kaprica, http://www.mladina.si/tednik/200507/clanek/uvo-manipulator--gregor_cerar/ (9. 3. 2005).
15. Counter - Terrorism Committee (2005): <http://www.un.org/Docs/sc/committees/1373/definition.html> (9. 3. 2005).
16. Crompton, Malcolm (2002): Biometrics and Privacy: The End of The World as We Know It or The White Knight of Privacy?, <http://www.privacy.gov.au/news/speeches/sp80notes.pdf> (9. 3. 2005).
17. Daugman, John (2004): How Iris Recognition Works, <http://www.cl.cam.ac.uk/users/jgd1000/csvt.pdf> (9. 3. 2005).
18. Dean, Lisa S. (2004): Privacy Impact Assessment: Transportation Worker Identification Credential (TWIC) Prototype, http://www.dhs.gov/interweb/assetlibrary/privacy_pia_twic.pdf (9. 3. 2005).
19. Development of the Biometrics Institute Privacy Code for the biometrics industry (2005): <http://www.biometricsinstitute.org/bi/codeofconduct.htm> (9. 3. 2005).
20. Dumitriu, Eugenia (2004): The E.U.'s Definition of Terrorism: The Council Frame-work Decision on Combating Terrorism. V German Law Journal No. 5 - Special Edition, http://www.germanlawjournal.com/pdf/Vol05No05/PDF_Vol_05_No_05_585602_special_issue_Dumitriu.pdf (9. 3. 2005).
21. EU ima težave pri biometričnih potnih listih (2004): <http://www.delo.si/article.print.php?ID=14468> (9. 3. 2005).
22. Face Recognition Vendor Test 2005 (2005): <http://www.frvt.org/FRVT2005/> (9. 3. 2005).
23. Facial Recognition (2005): <http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html> (9. 3. 2005).
24. Fact Sheet: U.S. – Mexico Land Borders: http://www.dhs.gov/interweb/assetlibrary/US-VISIT_Mexico_Fact_Sheet-English.pdf (9. 3. 2005).
25. Fingerprint Identification (2005): <http://www.fbi.gov/hq/cjisd/ident.pdf> (9. 3. 2005).

26. Fingerprint Verification Competition 2004 (2005): http://bias.csr.unibo.it/fvc2004/results/Open_resultsAvg.asp (9. 3. 2005).
27. Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates (2003): Research, development, test and evaluation, defense-wide, Volume 1 – Defense advanced research projects agency, http://www.darpa.mil/body/pdf/FY04_FY05BiennialBudgetEstimatesFeb03.pdf (9. 3. 2005).
28. Homeland Security Advisory System (2005): <http://www.dhs.gov/dhspublic/display?theme=29> (9. 3. 2005).
29. How is 'Biometrics' Defined? (2005): http://www.biometricgroup.com/reports/public/reports/biometric_definition.html (9. 3. 2005).
30. Human ID at a distance (2005): <http://www.eff.org/Privacy/TIA/hid.php> (9. 3. 2005).
31. INS Passenger Accelerated service System (2005): http://www.cbp.gov/linkhandler/cgov/travel/frequent_traveler/inspass.ctt/inspass.doc (9. 3. 2005).
32. Iris Image (2005): http://www.machinevisiononline.org/images/Vision_Based_Biometrics_Fig5_Iris.jpg, (9. 3. 2005).
33. Iris Scan (2005): <http://ctl.ncsc.dni.us/biomet%20web/BMIris.html> (9. 3. 2005).
34. Jain, Anil K. (2004): Biometric Authentication: How Do I Know Who You Are?, <http://biometrics.cse.msu.edu/> (9. 3. 2005).
35. Jain, Anil K., Arun Ross in Salil Prabhakar (2004): An Introduction to Biometric Recognition, <http://biometrics.cse.msu.edu/JainRossPrabhakarCSVTV15.pdf> (9. 3. 2005).
36. Jain, Anil K., Sharath Pankanti, Salil Prabhakar, Lil Hong, Arun Ross in James L. Wayman (2004): Biometrics: A Grand Challenge, <http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf> (9. 3. 2005).
37. Jones, Roland (2004): Homeland security seen spurring biometrics, http://www.biometricgroup.com/in_the_news/01_20_04.html (9. 3. 2005).
38. Kingsbury, Nancy (2003): Border Security: Challenges in Implementing Border Technology, <http://www.gao.gov/new.items/d03546t.pdf> (9. 3. 2005).
39. Kontrola pristopa in registracija delovnega (2005): http://www.spica.si/default.asp?f=ts_ac (9. 3. 2005).

40. Long-distance identification system tested at INSCOM headquarters (2002): V INSCOM JOURNAL, [http://www.inscom.army.mil/PAO/journal/winter 2002.pdf](http://www.inscom.army.mil/PAO/journal/winter%202002.pdf) (9. 3. 2005).
41. Maio, Dario, Davide Maltoni, Ricardo Capelli, James L. Wayman in Anil K. Jain (2004): FVC 2004: Third Fingerprint Verification Competition, http://biometrics.cse.msu.edu/FVC2004_ICBA.pdf (9. 3. 2005).
42. Maltoni, Davide, Dario Maio, Anil K. Jain in Salil Prabhakar (2003): Handbook of Fingerprint Recognition. New York: Springer, 1-52, <http://bias.csr.unibo.it/maltoni/handbook/> (9. 3. 2005).
43. Metropolitan Police Service Centenary Fingerprint Bureau Press Pack (2005): <http://www.met.police.uk/so/100years/henry.htm> (9. 3. 2005).
44. Most, Maxine C. (2004): Biometrics and Border Control. V Digital World, September/Oktobre 2004: <http://magazine.digitalidworld.com/Sep04/Page18.pdf> (9. 3. 2005).
45. Novice – TIGR (2005): http://www.tigr-drustvo.si/novice/Novice.php?subaction=showfull&id=1083075488&archive=&start_from=&ucat=7&go=rodoljub (9. 3. 2005).
46. Patterns of Global Terrorism 2003 (2003): http://www.globalsecurity.org/security/library/report/2004/pgt_2003/ (9. 3. 2005).
47. Pentagon's 'Terror Information Awareness' program will end (2003): V USA Today, 25. 9., http://www.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm (9. 3. 2005).
48. Phillips, Jonathon P., Patrick Grother, Ross J. Michaels, Duane M. Blackburn, Elham Tabassi in Mike Bone (2003): Face Recognition Vendor Test 2002: Overview and Summary. <http://www.biometricsinstitute.org/bi/FaceRecognitionVendorTest2002.pdf> (9. 3. 2005).
49. Podio, Fernando L. in Jeffrey S. Dunn (2005): Biometric Authentication Technology: From the Movies to Your Desktop, <http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf> (9. 3. 2005).
50. Powell, Colin L. (2004): Passports and Visas with Embedded Biometrics and the October Deadline. V The DISAM Journal, poletje 2004, 54-57, <http://www.state.gov/secretary/former/powell/remarks/31639.htm> (9. 3. 2005).

51. Prabhakar, Salil, Sharath Pankanti in Anil K. Jain (2003): Biometric Recognition: Security and Privacy Concerns, <http://biometrics.cse.msu.edu/j2033.pdf> (9. 3. 2005).
52. Protecting Civilization from the Faces of Terror (2001): A Primer on the Role Facial Recognition Technology can Play in Enhancing Airport Security, http://www.securitymanagement.com/library/Visionics_counter1101.pdf (29. 8. 2004 - stran ni več dostopna).
53. Rhodes, Keith A. (2003): Challenges in using Biometrics, <http://www.gao.gov/new.items/d031137t.pdf> (9. 3. 2005).
54. Ross, Arun in Anil K. Jain (2004): Multimodal Biometrics: An Overview. http://biometrics.cse.msu.edu/RossMultimodalOverview_EUSIPCO04.pdf (9. 3. 2005).
55. Schwartz, Jeffrey (2004): Biometrics Boost: Protecting the Nation's Borders, V VARbusiness, 26. 1., http://www.varbusiness.com/sections/news/dailyarchives.jhtml;jsessionid=M3R2T24AMOGJWQSNDBCSKHSCJUMKJVN?articleId=18825257&_requestid=100806 (9. 3. 2005).
56. Scrotty History (2005): <http://library.thinkquest.org/TQ0313041/scrottyhistory.htm> (9. 3. 2005).
57. Skokowski, Paul (2002): Can biometrics defeat terror?, <http://www-hoover.stanford.edu/research/conferences/nsf02/skokowski.pdf> (9. 3. 2005).
58. Spence, Bill (2003): Biometrics' Role in Physical Access Control, http://www.ibia.org/membersadmin/whitepapers/pdf/5/CS25Loss_Prevention_Apr2003.pdf (9. 3. 2005).
59. Smart Computing Encyclopedia (2005): <http://www.smartcomputing.com/editorial/dictionary/detail.asp?guid=&searchtype=1&DicID=17273&RefType=Encyclopedia> (9. 3. 2005).
60. Špica International: Kontrola pristopa in delovnega časa (2005): http://www.spica.si/default.asp?f=ts_ac (9. 3. 2005).
61. The Henry Classification System (2003): <http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf> (9. 3. 2005).
62. The Use of Technology To Combat Identity Theft (2005): http://www.treas.gov/offices/domesticfinance/financialinstitution/cip/biometric_study.pdf (9. 3. 2005).

63. Total/Terrorism Information Awareness (TIA): Is It Truly Dead? (2003): http://www.eff.org/Privacy/TIA/20031003_comments.php (9. 3. 2005).
64. US-VISIT: Who Is Required to Enroll? (2005): http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0527.xml (9. 3. 2005).
65. US-VISIT FAQs: NSEERS and US-VISIT (2005): http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0441.xml (9. 3. 2005).
66. US-VISIT Arrival Process for Visitors Traveling with a Visa (2005): <http://dsa.emich.edu/ois/images/us-visit.jpg> (9. 3. 2005).
67. Visa Waiver Program (2005): <http://immigration.about.com/blvisawaiver.htm> (24.3.2005).
68. Visa Waiver Countries (2005): http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0443.xml (9. 3. 2005).
69. Vision Based Biometrics – Iris (2005): http://www.machinevisiononline.org/images/Vision_Based_Biometrics_Fig5_Iris.jpg (9. 3. 2005).
70. Walkup (Iris) Cameras (2005): <http://www.iridiantech.com/products.php?page=4> (9. 3. 2005).
71. Wang, Yunhong, Tieniu Tan in Anil K. Jain (2003): Combining Face and Iris Biometrics for Identity Verification, <http://biometrics.cse.msu.edu/WangTanJainAVBPA03.pdf> (9. 3. 2005).
72. What Are Biometrics? (2005): <http://www.findbiometrics.com/Pages/guide1.html>, (9. 3. 2005).
73. What is US-VISIT? (2005): <http://www.dhs.gov/dhspublic/display?theme=50&content=4085> (9. 3. 2005).
74. Woodward, John D. Jr. (2001a): Biometrics, Facing up to Terrorism, <http://www.rand.org/publications/IP/IP218/IP218.pdf> (9. 3. 2005).
75. Woodward, John D. Jr. (2001b): Super Bowl Surveillance, Facing up to Biometrics, <http://www.rand.org/publications/IP/IP209/IP209.pdf> (9. 3. 2005).
76. Woodward, John D. Jr., Christopher Horn, Julius Gatune in Aryn Thomas (2003): Biometrics: A Look at Facial Recognition, <http://www.rand.org/publications/DB/DB396/DB396.pdf> (9. 3. 2005).
77. WVU researchers explore the cost savings of biometrics (2004): http://www.nis.wvu.edu/2004_Releases/biometric_costs.htm (9. 3. 2005).

DOKUMENTI:

1. Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States. OJ L 385/1, 29.12.2004.
2. Sklep sveta z dne 13. junija 2002 o boju proti terorizmu (Council Framework Decision of 13 June 2002 on Combating Terrorism): (2002/475/PNZ).
3. Zakon o varstvu osebnih podatkov (ZVOP-1) (2004): Uradni list RS, št. 86/2004.
4. Splošna deklaracija o človekovih pravicah (1948): <http://www.unhchr.ch/udhr/lang/slv.htm> (9. 3. 2005)

NEOBJAVLJENI VIRI:

1. Buskey, Carlos Delano (2001): How Face Recognition Will Be Used To Counter Terrorism: A Biometric Report.
2. Colja, Alenka (2005): Povečevanje varnosti z vključitvijo biometričnih elementov v potne liste. Zasnova magistrske naloge. Kranj: Fakulteta za podiplomske državne in evropske študije.
3. Matyas, Vaclav in Zdenek Riha (1999): Biometric Authentication System
4. Uvajanje biometrije na potne listine državljanov Republike Slovenije – stanje projekta in nadaljnji razvoj (2004): Direktorat za upravne notranje zadeve, Ljubljana.
5. Uvajanje biometrije na potne listine državljanov Republike Slovenije – Informacija o stanju projekta in nadaljnji razvoj (2005): Direktorat za upravne notranje zadeve, Ljubljana.