Biometrija i zaštita privatnosti

Konjevod, Mihaela

Undergraduate thesis / Završni rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Humanities and Social Sciences / Sveučilište Josipa Jurja Strossmayera u Osijeku, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:142:787558

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-11-28**

FILOZOFSKI FAKULTET
SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

Repository / Repozitorij:

FFOS-repository - Repository of the Faculty of Humanities and Social Sciences Osijek

zir.nsk.hr

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Sveučilište J. J. Strossmayera u Osijeku
Filozofski fakultet Osijek
Odsjek za Informacijske znanosti
Preddiplomski studij informatologije

Mihaela Konjevod

Biometrija i zaštita privatnosti

Završni rad

Mentor: doc. dr. sc. Boris Badurina
Sumentor: dr. sc. Anita Papić

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Odsjek za Informacijske znanosti

Preddiplomski studij informatologije

Mihaela Konjevod

Biometrija i zaštita privatnosti

Završni rad

Društvene znanosti, informacijske i komunikacijske znanosti, informacijski sustavi i informatologija

Mentor: doc. dr. sc. Boris Badurina

Sumentor: dr. sc. Anita Papić

Osijek, 2016.

Sažetak

Cilj ovog rada je pobliže opisati biometriju i načine na koje se ona odražava na privatnost pojedinaca. Rad daje uvid u nastanak i razvoj biometrije, pregled osnovnih definicija vezanih uz biometriju, načine rada biometrijske identifikacije, biometrijske sustave, moguće pogreške sustava te biometrijske karakteristike. Ukratko će se biometrija usporediti s tradicionalnim metodama prepoznavanja, a naglasak će se u ovom radu staviti na poveznici između biometrije i zaštite privatnosti i sigurnosti. Kroz rad će biti opisani načini na koje privatnost korisnika i njegovih osobnih podataka može biti ugrožena uporabom biometrijske tehnologije. Spomenut će se i neka od brojnih pitanja i problema vezanih uz biometriju i zaštitu sigurnosti i privatnosti koja su danas u porastu budući da su biometrijski podaci osobno i osjetljivo područje. Najčešći problemi vezani uz biometriju su podvale, prijetnje i napadi. Također, navest će se četiri ključne smjernice za učinkovitu zaštitu biometrijski sustava i samim time podataka pohranjenih u njima. U radu će se osvrnuti i na biometrijske aplikacije i programe povezane s vladom, policijom i komercijalnom uporabom te na informacijske sustave i informacijsku sigurnost. Informacijski sustavi i biometrija usko su povezani. Informacijska sigurnost izuzetno je bitna za očuvanje anonimnosti podataka, a sačinjavaju ju pet područja: fizička sigurnost, sigurnost podataka, sigurnost poslovne suradnje, sigurnosna provjera i sigurnost informacijskog sustava. U zaključnim razmatranjima u radu iznose se stavovi i percepcije korisnika o biometrijskim tehnologijama te neka od provedenih istraživanja koja dokazuju koliko korisnici danas imaju povjerenja u suvremene tehnologije poput biometrijskih tehnologija prepoznavanja.

Ključne riječi: biometrija, biometrijska identifikacija, privatnost, sigurnost

Sadržaj

1. Uvod

Biometrija je inovativna tehnologija koja postaje sve prisutnija u sferama ljudskog života. Suvremeno doba otvorilo je vrata ovoj vrsti tehnologije te njezin razvoj i značaj raste svakim danom. Ljudi su danas suočeni s porastom opasnosti poput terorizma, napada, prijetnji, krađe i zbog toga je potreba za društvenom i osobnom sigurnošću sve veća. Ljudi žele zaštiti svoju imovinu, predmete, financije, podatke i svoju sigurnost. Potrebno je zaštiti osobna računala, prijenosna računala, pametne telefone i aktivnosti na internetu. Također, ljudi žele zaštiti svoja vozila, strojeve i druge vrijedne predmete od neovlaštenog pristupa ili uporabe. U području financija cilj je spriječiti krađu i krivotvorenje, a u područjima povećane sigurnosti cilj je omogućiti pristup radnim mjestima isključivo ovlaštenim osobama (npr. vojna područja). Za uspješno osiguravanje društvene i osobne zaštite potrebna je provjera identiteta osobe u osobnim dokumentima kao što su vozačke dozvole, osobne iskaznice i kartice zdravstvenog osiguranja. Potrebno je i održavati nadzor u zračnom prometu. Biometrijske tehnologije su pokazale izuzetno veliku učinkovitost i pouzdanost u održavanju sigurnosti u navedenim područjima i sferama ljudskog života.[1] Tradicionalne tehnologije koje se temelje na znanju i materijalnom posjedovanju ne mogu biti funkcionalne kao biometrijske tehnologije [2]

Biometrija je namijenjena prvenstveno za poboljšanje sigurnosti no, priroda takvih podataka može otkriti više informacija nego što je potrebno. Iako su brojna istraživanja u području biometrije donijela prijedloge za zaštitu podataka još uvijek postoji jaz što se tiče privatnosti u ovom relativno mladom području. Osnovna načela zaštite kvalitete podataka se rješavaju na način da se podaci minimaliziraju, da su podaci točni i potpuni, da je prisutna suglasnost, transparentnost, povjerljivost i sigurnost. Zahtjevi za privatnošću i sigurnošću svakako se uključuju u ranoj fazi projektiranja biometrijskih sustava.[3]

[1] Usp. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 164.
[2] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 40. URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
[3] Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. str. 1 URL: https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf (2016-06-25)

2. Biometrija

Pojam biometrija nastao je od grčke riječi *bios* što znači život i *metrikos* što označava mjeru. Biometrija je znanost prepoznavanja pojedinca koja se temelji na identificiranju ponašanja i bioloških karakteristika pojedine osobe, kao što su otisci prstiju, glas, hod, lice, šarenica oka i sl.[4] Možemo reći da biometrija koristi fizičke i biološke karakteristike osobe u svrhu identifikacije te osobe.[5] Naravno važno je naglasiti da se tu radi o mjerenju karakteristika ljudi.[6] Biometrijska karakteristika može biti svako ljudsko ponašanje i fizičke i psihičke osobine sve dok one udovoljavaju zahtjevima jedinstvenosti, univerzalnosti, stalnosti i mogućnostima prikupljanja. Jedinstvenost označava da bilo koje dvije osobe na svijetu trebaju biti različite u pogledu tih karakteristika. Univerzalnost označava da ta karakteristika mora biti prisutna kod svih osoba. Stalnost karakteristika znači da se one ne bi trebale mijenjati tijekom vremena. I naravno mogućnost prikupljanja znači da su te karakteristike kvantitativno mjerljive. Biometrija se u potpunosti oslanja na ono tko je osoba i što ona radi, a ne na ono što osoba zna kao što je npr. lozinka ili ono što ona posjeduje kao što je osobna iskaznica. Njena prednost je i što može nadopuniti ili u potpunosti zamijeniti postojeću tehnologiju te je u nekim tehnologijama upravo ona jedini održivi pristup osobnom identificiranju.[7]

Kada se govori o biometriji i biometrijskim metodama identifikacije postoje dvije oprečne skupine autora koji zastupaju različita stajališta. Jedna skupina smatra da su sve metode identifikacije biometrijske, te su to sve klasične metode primijenjene u digitalnom okruženju, dok druga skupina smatra da suvremene tehnološke mogućnosti omogućuju jednostavniju primjenu klasičnih identifikacijskih metoda, ali i razvoja novih.[8]

Biometrija je daleko više pouzdana nego tradicionalne tehnologije prepoznavanja. Tradicionalne tehnologije prepoznavanja temelje se na znanju korisnika (PIN, lozinka) ili na onome što korisnik fizički posjeduje (ključ, kartica). Ukoliko se koriste lozinke, preporuča se da ih se često mijenja i da se koriste različite lozinke za različita područja što velika većina ljudi ne

[4] Usp. Biometrics Security and Privacy Protection. // IEEE Signal Processing Magazine, 2015. str 1. URL: URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7192815 (2016-06-25)
[5] Usp. Uddin, Jasmin. Matrix of Biometrics // Biometrics, 2016, str. 1. URL: URL: https://www.researchgate.net/publication/301542522_Matrix_of_Biometrics (2016-06-25)
[6] Usp. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 162.
[7] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str. 33.URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
[8] Usp. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 162

radi. Velika većina ljudi postavlja svoje lozinke u obliku slova i brojki kojih se oni mogu najlakše sjetiti kao što su imena, prezimena, datumi rođenja njihovih najbližih, ime najdražeg pjevača, pjevačice, grupe, filma, knjige i sl. Istraživanje provedeno 2001. godine među jednom skupinom radnika u uredu u Velikoj Britaniji pokazalo je da je skoro polovina ispitanika za lozinku izabrala ime svog ljubimca, člana obitelji ili čak svoje ime. Ostatak ispitanika izabrao je za lozinku ime slavne osobe ili lika iz filma. Dobro je poznato da je takve lozinke lako otkriti unaprijed osmišljenim napadom riječi ili jednostavnim pogađanjem. No, dulje lozinke teže su za pamtiti pa ih mnogi korisnici zapisuju što narušava njihovu sigurnost. Kriptografske tehnike mogu pružiti vrlo dugačke lozinke koje korisnik ne mora pamtiti. Što se tiče ključeva i kartica, oni se mogu dijeliti, duplicirati, izgubiti ili ukrasti. S druge strane, biometrija ne može biti izgubljena te je puno teže dijeliti ili kopirati biometriju. Biometrija je puno teža za napasti te je razina sigurnosti u biometrijskom sustavu jednaka za sve. Glavna prednost biometrije je što korisnici ne moraju pamtiti duge i složene lozinke, često ih mijenjati ili sa sobom nositi ključeve i kartice. [9]

2.1 Nastanak i razvoj biometrije

Ljudi su od svog nastanka koristili karakteristike tijela kao što su lice, glas, hod i sl. da bi prepoznali jedini druge. Otisci prstiju već su se u 3. st. pr. Kr. koristili u Kini kao potpisi, a tek su krajem 17. stojeća Europljani spoznali da se otisci mogu koristiti za identifikaciju, što su Kinezi već odavno znali. Kinezi su još u davnoj prošlosti koristili i daktiloskopiju kako bi spriječili zamjenu novorođenčadi. Neke od metoda identifikacije koristili su Asirci i Babilonci, kao dokaz autorstva na dokumentima su se utiskivali otisci papilarnih linija prsta.[10]

Do 18. stoljeća već je bilo poznato da se može upravljati identitetom pomoću jedinstvenih fizičkih karakteristika ljudi.[11] Sredinom 19. st šef odjela za kriminalistu u Parizu, Alphonse Bertillon razvio je ideju korištenja fizičkih mjera kao što su visina, dužina ruku, stopala i prstiju kako bi lakše identificirao kriminalce. Krajem 19. st Bertillonova ideja postajala je sve popularnija, no ubrzo je potisnuta budući da se otkrila jedinstvenost otiska prstiju. Ubrzo nakon toga mnogi veliki pravni i zakonski odjeli poduprli su ideju uzimanja otisaka prstiju od kriminalaca te njihovo

[9] Usp. 2. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 36. URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
[10] Usp. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 160.
[11] Usp. Uddin, Jasmin. Matrix of biometrics // Biometrics, 2016, str. 1. URL: https://www.researchgate.net/publication/301542522_Matrix_of_Biometrics (2016-06-25)

spremanje na početku u kartoteke, a zatim u baze podataka. Nije trebalo dugo da policija razvije način uzimanja fragmenata otiska prstiju s mjesta zločina te ih usporedi s onima u bazi podataka i tako identificira potencijalnog počinitelja zločina.[12] Tijekom 2005. godine RTE vijesti su obavijestile kako se biometrijske tehnologije sve više razvijaju i usvajaju na radnim mjestima u Irskoj. U to vrijeme brojni radnici i sindikati bili su u strahu od prihvaćanja biometrijske tehnologije zbog mogućnosti gubitka privatnosti nad osjetljivim podacima. U tom razdoblju počinju se pojavljivati brojna problemska pitanja i etičke rasprave vezane uz biometriju. [13] Kao što se može zaključiti biometrija se prvo koristila u pravne svrhe i forenziku, zatim za utvrđivanje očinstva i zaštitu zaposlenika koji su bili zaposleni na vrlo riskantnim i osjetljivim poslovima. Danas se biometrija sve više koristi od strane privatnih i državnih organizacija[14]

No, tijekom povijesti tri bitne stvari su se promijenile kod biometrije. Prvo, vrste i oblici biometrijskih informacija, metode i upravljanje biometrijskim podacima i njihova pouzdanost su prošle kroz tehnološku transformaciju. Danas su biometrijski sustavi gotovo nepogrešivi. Mnoge tehnologije prepoznavanja lica, otisaka prstiju ili mrežnica oka koriste se u provedbi zakona. Druga promjena se odnosi na značaj biometrijskih karakteristika točnije otisaka prsta. Otisak prsta upotrebljavao se kao osobni potpis, a do danas je prerastao iz pravnog u identifikacijski i pretraživački alat. Treća velika promjena su pitanja o vlasništvu biometrijskih podataka. S razvojem informacijsko-komunikacijskih tehnologija, porastom računalne snage koja je namijenjena biometriji raste i broj pitanja o tome tko posjeduje biometrijske podatke, mogu li se biometrijski podaci dobiti bez dozvole ili znanja osobe čiji su, mogu li se slobodno diseminirati i reproducirati, mogu li se prodavati, i sl. Na brojna pitanja koja su proizašla iz biometrije i biometrijskih karakteristika još se uvijek traži odgovor. [15]

[12] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 33-42 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)

[13] Usp. Parke, Conor. Biometrics in the Workplace. Str 3. . URL: http://www.academia.edu/11950137/The_use_of_Biometrics_in_the_Workplace (2016-06-10)

[14] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 33-42 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)

[15] Usp. Uddin, Jasmin. Matrix of Biometrics// Biometrics, 2016. str 3. URL: https://www.researchgate.net/publication/301542522_Matrix_of_Biometrics (2016-06-25)

2.2 Biometrijska identifikacija

Kao što je već poznato, svaka osoba, životinja kao i svaki objekt u prirodi razlikuju se jedno od drugog. Ponekad se razlikuju tako očito da je jednostavno identificirati osobu ili objekt, ali postoje slučajevi kada su razlike toliko male da se ne mogu identificirati bez pomoći određenih metoda.[16] Identifikacija osobe je utvrđivanje istovjetnosti nepoznatog s otprije poznatim, na temelju određenih identifikacijskih obilježja. To je postupak usporedbe određenog broja identifikacijskih obilježja, pri čemu se ustanovljava podudarnost ili različitost između objekata koji se uspoređuju.[17] Biometrijska identifikacija u suvremenom svijetu se temelji na ponašanju i fiziološkim osobinama određene osobe, odnosno na prepoznavanju određenih biometrijskih karakteristika i njihovom usporedbom s uzorkom pohranjenim u bazi podataka pojedinog sustava. U mnogim državnim i privatnim sektorima biometrijska identifikacija se promovira kao tehnologija koja može pomoći u razotkrivanju terorista, tehnologija koja osigurava bolju kontrolu pristupa financijskim računima, fizičkim prostorima te tehnologija koja povećava učinkovitost i pouzdanost pristupa raznim uslugama. Biometrijska identifikacija korisna je kod identificiranja kriminalaca, kod personalizacije socijalnih usluga i praćenja medicinskih informacija o bolesnicima.[18]

[16] Usp. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 161.
[17] Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 161.
[18] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 33-42 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)

2.3 Biometrijski sustav

Biometrijski sustav je sustav klasifikacije uzoraka koji koristi jednu vrstu naprednog sustava za obradu i specifičnu usporedbu biometrijskih podataka.[19] Takav sustav identificira pojedinca na temelju vektora koji je izveden iz specifične karakteristike koju osoba posjeduje. Biometrijski sustavi obično rade u verifikacijskom ili identifikacijskom načinu rada. U verifikacijskom načinu rada sustav potvrđuje identitet osobe usporedbom pohranjenih biometrijskih karakteristika s biometrijskim predloškom pojedinca. Verifikacija se obično koristi za tzv. pozitivna prepoznavanja kojima je cilj spriječiti da se više ljudi koristi istim identitetom. To obično podrazumijeva identificiranje putem osobnog identifikacijskog broja (PIN-a), login imena i sl. gdje sustav provodi usporedbu jedan na jedan kako bi utvrdio je li tvrdnja istinita točnije je li taj čovjek onaj kojim se predstavlja. Drugi način rada je identifikacijski gdje sustav prepoznaje pojedinca pretraživanjem predložaka u bazi podataka u potrazi za podudaranjem. U ovom slučaju sustav provodi pretraživanje jedan prema više kako bi utvrdio identitet osobe. Sustav utvrđuje je li osoba ona koja tvrdi da je. Cilj identifikacije je da se spriječi jednu osobu od korištenja više identiteta.[20]

Biometrijski sustavi sastoje se od četiri osnovna dijela. Prvi dio je ulazna jedinica koja služi za mjerenje i registriranje biometrijskih karakteristika. Drugi dio je ekstraktor koji izdvaja određenu karakteristiku iz cjeline. Treći dio su baze gdje su pohranjeni dokazi identifikacijskih karakteristika i četvrti dio su jedinice za verifikaciju i usporedbu. Jedinice za verifikaciju ispituju kvalitetu i kvantitetu biometrijskih karakteristika te ih uspoređuju s onima koje su ranije pohranjene u bazi.[21]

Postoje i biometrijske pogreške u sustavu. Biometrijske pogreške odnose se na dva uzorka od iste biometrijske karakteristike od iste osobe npr. dva otiska lijevog palca nisu u potpunosti jednaka zbog nesavršenosti uvjeta (kao što su npr. znojne ruke) ili zbog promjena u ponašanju korisnika kao što su posjekotine ili modrice na prstu, zbog uvjeta okoline (temperatura, vlažnost) ili interakcije korisnika sa senzorom (položaj prsta).[22] Kao što je već spomenuto, biometrijski sustavi mogu raditi u verifikacijskom ili identifikacijskom načinu rada. Biometrijski sustav

[19]Usp. Biometrics Security and Privacy Protection. // IEEE Signal Processing Magazine, 2015. str 17. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7192815 (2016-06-25)
[20]Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 33-34 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
[21] Usp. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 164.
[22] Isto. str 34.

verifikacije može napraviti dvije vrste pogrešaka, a to su: pogrešno biometrijsko mjerenje karakteristika dviju različitih osoba, a da izgleda kao da su biometrijske karakteristike od iste osobe i provođenja mjerenja biometrijskih karakteristika iste osobe, a da izgleda kao da su karakteristike od dvije različite osobe.[23] Tri su načina na koji biometrijski sustavi mogu biti ugroženi, a to su: zaobilaženje sustava, prevare u području verifikacije i prevare u području upisa. Zaobilaženje sustava podrazumijeva korištenja sustava na način suprotan od propisanog. Sustav se može koristi na suprotan način zbog administrativnih razloga, za osiguravanje lakšeg pristupa. Takav način također omogućuje hakerima olakšano iskorištavanje sustava zbog njegove ranjivosti. Prevare verifikacije podrazumijevaju pokušaje zaobilaženja sustava tijekom procesa verifikacije, npr. prisiljavanje pojedinca da verificira svoj identitet kako bi ostvario pristup. Prevare upisa se odnose na osnovna pitanja kao što su „jesi li ti onaj koji kažeš da jesi?“[24]

3. Biometrija u službi sigurnosti i zaštite

Biometrijska identifikacija ili verifikacija prvenstveno je namijenjena poboljšanju sigurnosti i privatnosti.[25] Biometrijske tehnologije nude zaposlenicima sposobnost ograničavanja pristupa određenim sobama/laboratorijima koji mogu sadržavati privatne/povjerljive informacije koje mogu vidjeti samo nekoliko odabranih ljudi. Ovakav način zaštite uglavnom je razvijen u specifičnim područjima radnih mjesta koja su privatna ili nesigurna za korištenje. Biometrija je znanost koja je podigla razinu sigurnosti u poslovnim područjima u nekoliko zadnjih godina.[26]

No, budući da je poznato da su biometrijski podaci ljudi osjetljivi i osobni, pitanja i problemi vezani uz biometriju i zaštitu sigurnosti i privatnosti su u porastu. Najčešći problemi vezani uz sigurnost i privatnost osoba su podvale, gdje se osoba predstavlja sustavu s krivotvorenim biometrijskim karakteristikama s namjerom da oponaša drugu osobu. Idući problem veže se uz osobe koje pokušavaju promijeniti svoje biometrijske karakteristike kako bi izbjegli prepoznavanje od strane sustava. Veliki je problem i ako se pohranjeni biometrijski podaci iskorištavaju u nezakonite svrhe te ako se na bilo koji način želi uništiti integritet biometrijskog

[23] Isto.
[24] Usp. Wayne, Penny. Biometrics: A Double Edge Sword - Security and Privacy, 2002. str 2-13. URL: https://www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edged-sword-security-privacy-137 (2016-06-20)
[25] Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. Str. 1-16. URL: https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf (2016-06-25)
[26] Usp. Parke, Conor. Biometrics in the Workplace. Str. 1-6. URL: http://www.academia.edu/11950137/The_use_of_Biometrics_in_the_Workplace (2016-06-10)

sustava. Sve je veća potreba za dodatnom sigurnošću kako biometrijske tehnologije tako i podataka pohranjenih u njoj.[27] Potrebno je zaštititi biometrijske podatke od otuđenja i od korištenja u druge svrhe izvan onih za koje su namijenjeni. S razvojem sustava za identifikaciju i udruživanjem identiteta osoba s osobnim i drugim ponašanjima i karakteristikama zabrinutosti oko mogućnosti da se te informacije koriste za kršenje prava pojedinaca i za uskraćivanje njihovog prava na anonimnost sve više rastu.[28] Sigurnosni zahtjevi o povjerljivosti, autentičnosti, dostupnosti i integritetu su potrebni kako bi bilo koji sustav bio umrežen pa tako i biometrijski.[29]

3.1 Biometrija i privatnost

Privatnost je sposobnost samostalnog vođenja života i kontroliranje pristupa vlastitim informacijama. Kod biometrije postoje tri glavna problema privatnosti. Prvi problem je to što su biometrijske karakteristike biološkog podrijetla te bi ljudi koji prikupljaju te podatke mogli prikupljati i dodatne osobne podatke iz biometrijskih mjerenja. Npr. drugačije oblikovan prst može se statistički povezati s određenim genetskim poremećajem i sl. Takve informacije mogu biti temelj za diskriminaciju. Drugi problem privatnosti je što su neke metode biometrijske identifikacije poput otiska prstiju dovoljno jake da omogućuju i neželjenu identifikaciju. Npr. ukoliko osoba ima drugo ili tajno ime iz sigurnosnih razloga ona može ipak biti identificirana prema svom otisku prsta. Na taj način moguće je povezivati informacije o ljudima s njihovim ponašanjem. I treći problem privatnosti je što biometrijske karakteristike ljudi nisu tajne te je često moguće dobiti biometrijski uzorak osobe bez znanja te osobe. Što bi značilo da osoba ne može biti anonimna.[30] Također, kontrolu nad biometrijskim podacima ima sustav, točnije ti su podaci dostupni samo ovlaštenim korisnicima kao što su vlasnici i administratori.[31]

Od 2012. godine pa sve do danas predlagane su razne sigurnosne mjere i strategije koje se baziraju na pretpostavkama koje uključuju korisnika, subjekta koji vrši identifikaciju i

[27] Usp. Biometrics Security and Privacy Protection. // IEEE Signal Processing Magazine, 2015. Str 17. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7192815 (2016-06-25)
[28] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. Str 33. URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
[29] Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. Str. 1-16. URL: https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf (2016-06-25)
[30] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. Str 33-41 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
[31] Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. Str. 1-16. URL: https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf (2016-06-25)

komunikacijskog kanala za prijenos poruka između pošiljatelja i primatelja. Kako bi se biometrijski podaci sigurno pohranili u bazu podataka u takvom obliku da ih je gotovo nemoguće dobiti u originalu iz predloška provodi se transformacija. Kako bi se podaci zaštitili u slučaju da baza više nije sigurna koriste se razne tehnike pohrane iskrivljenih podataka što znači da parametri neće biti dostupni, te transformirani elementi neće odati originalni podatak iz predloška. Za zaštitu podataka koristi se i opozvana biometrija i obnovljivost te kripto-biometrija. Indukcija opoziva i otkazivanje u biometrijskim sustavima ima cilj zaštite podataka nakon krađe. Funkcionira sastavljanjem neupotrebljivih navoda na biometrijskih predložak s čime se podiže razina privatnosti. Također, postoji mogućnost da se ljudske karakteristike promijene tijekom vremena ili ozljedama. U tom slučaju, potencijalno ne prepoznavanje, koje će biti lažno, će povećati s korisnikove strane prethodni proces autentifikacije te ostali podaci neće moći biti duplicirani. Zbog navedenih razloga važna je mogućnost zamijene biometrijskih podataka zbog održavanja ažurnosti. [32]

Kripto-biometrija je jedna od najpoznatijih tehnika za zaštitu biometrijskih podataka koja se bazira na ključevima, a koristi kriptografske algoritme za šifriranje i dešifriranje. U šifriranoj domeni ključevi za biometriju mogu biti digitalni, što znači da PIN, lozinke i alfanumeričke veze će biti potvrđene samo ako je točan biometrijski uzorak, koji se naravno nakon svakog završenog procesa uništava. Kripto-biometrija omogućava kreiranje više ključeva za istu biometriju točnije za isti fizički identitet osobe, što uvelike pomaže jer omogućuje interakciju između različitih aplikacija bez ikakvih kompromisa. Prednosti ove metode su manje zadržavanje biometrijske slike ili pohranjenog predloška, mogućnost korištenja anonimnih modela baze podataka te veća usklađenost sa zakonima o privatnosti. No, nedostaci kripto-biometrije su što je nizak postotak točnosti za korištene algoritme te što postoji opasnost od povećanih napada na biometrijski predložak ili sam komunikacijskih kanal.[33]

[32] Isto.
[33] Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. Str. 1-16. URL: https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf (2016-06-25)

3.2 Biometrija u različitim sektorima

Biometrijske aplikacije se sastoje od tri glavne skupine, a to su komercijalne aplikacije (elektronička sigurnost podataka, računalne, mrežne prijave, fizička kontrola pristupa, pristup internetu, bankomatu, kreditnim karticama, upravljanje medicinskim zapisima i sl.), vladine aplikacije (osobna iskaznica, vozačka dozvola, socijalna sigurnost i socijalna skrb, granična kontrola, kontrola putovnica i sl.) i forenzične aplikacije (identifikacija umrlih, kriminalne istrage, određivanje roditeljstva, nestala djeca i sl.)[34]

U mnogim državama diljem svijeta, različite razine vlasti u potrazi su za mjerama prikladno dizajniranim za efektivnu borbu protiv prevara u njihovim programima. Jedan primjer prevare u vladinim programima su beneficije koje pojedinac ostvaruje pod višestrukim identitetima. Primjer je Toronto koji je razmišljao o uvođenju biometrijskih mjera kako bi kontrolirao socijalnu prevaru. Nadzorna agencija privatnosti u Ontariju surađivala je s gradom i ministarstvom u sastavljaju pravnog standarda za zaštitu. Vlada u Ontariju, ali i brojne druge vlade zalažu se da prikupljeni biometrijski podaci moraju biti kodirani te da se oni ne mogu koristi kao jedinstveni identifikatori koji mogu olakšati drugim stranama pristup biometrijskim podacima. Šifrirani biometrijski podaci mogu biti pohranjeni ili se prenositi u šifriranom obliku, a zatim uništiti na propisan način. Također, zakon uključuje da ni administratori ili ovlaštene osobe ne mogu implementirati sustav koji može obnoviti ili zadržati izvorni biometrijski uzorak. Drugim riječima, biometrijske tehnologije ne smiju imati mogućnost rekreiranja originalnog biometrijskog uzorka iz šifriranih biometrija. Pristup drugoj ili trećoj strani kodiranim podacima omogućit će se jedino kroz sudski nalog. Prikupljanje biometrijskih podataka, naravno, provodi se izravno kao što je propisano standardima. Biometrijski podaci koji se prikupljaju od pojedine osobe bit će dostupni i otvoreni toj osobi.

Biometrija je primijenjena metoda identifikacije i u području policije i zakona. Već je poznato da su otisci prstiju korišteni za identifikaciju žrtava i potencijalnih osumnjičenika više od sto godina. Brojne druge biometrijske metode identifikacije koriste se za osiguranje zatvora, zakonom zaštićenih područja i sl. Metoda DNK koristi se kao pomoć u rješavanju zločina. DNK se koristi kako bi se utvrdio krivac i razlikovao od nevinih u području kriminalistike. U te svrhe mnoge države su uspostavile ili razmatraju uspostavu DNK baza podataka. Biometrija uvelike smanjuje

[34] Usp. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 35 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)

policijske napore, ali biometrijski podaci moraju biti prepoznatljivi i jasno vidljivi što otvara brojna druga pitanja privatnosti. Što ako se DNK koristi izvan identifikacijskih svrha, npr. u svrhu prikupljanja informacija o zdravstvenim predispozicijama ili informacije o etničkom podrijetlu? Kako bi se spriječile potencijalne opasnosti korištenje, biometrija se treba regulirati zakonom. No, smatra se da bi policija mogla imati ključnu ulogu u utjecanju na pozitivno korištenje biometrije u zajednici i da bi mogla obučiti druge ustanove, tvrtke, organizacije pravilnom korištenju biometrijske tehnologije.

Zadnje područje gdje je Nadzorna agencija za privatnost ispitivala i proučavala korištenje biometrije je zasigurno područje poslovnih aplikacija. Godine 1997. Bill Gates je predvidio da će biometrijske tehnologije biti jedne od najpotrebnijih inovacija u narednih nekoliko godina. Komercijalna uporaba biometrije sve se više širi i postaje značajna u svijetu. U mnogim bankomatima diljem svijeta uključeno je prepoznavanje lica i šarenice oka, brojne financijske ustanove koriste otiske prsta za identificiranje svojih klijenata. Zanimljivo je da se geometrija prsta, dlana ili ruke koristi za kontrolu pristupa brojnim tematskim parkovima u svijetu. Kod poslovnih aplikacija koje su usmjerene na potrošače svakako treba razmotriti mogućnost da one budu dizajnirane tako da vlasnici biometrijskih podataka ujedno imaju i kontrolu nad njima. Također, smatra se da je poraslo javno prihvaćanje i razumijevanje biometrije. Jedna Američka anketa pokazala je da 87% ispitanika smatra uzimanje otiska prsta legitimnom identifikacijom te 91% ispitanika smatra da je opravdano koristi otisak prsta za kontrolu ulaska u visoko sigurnosna područja. No, u ovom području zasigurno nedostaje više propisa koji određuju uporabu biometrijskih podataka te korisnici trebaju zastupati vlastite interese u pogledu privatnost. [35]

3.3 Učinkovita procjena privatnosti

Kako bi se osigurala privatnost biometrijskih podataka, samih biometrijskih sustava te na taj način privatnost krajnjih korisnika prvo je neophodna zaštita biometrijski podataka. Također, dizajn i način korištenja biometrijskih sustava uvijek trebaju poštivati strogo propisane smjernice. Kako bi se ostvarila privatnost moraju se zadovoljiti četiri glavne smjernice, a to su: opseg i sposobnost biometrijskog sustava, zaštita podataka, korisnička kontrola osobnih podataka te objavljivanje, revizija i odgovornost biometrijskih sustava. Prva točka se odnosi na opseg i

[35] Usp. Cavouklan, Ann. Privacy and Biometrics. Ontario: Information and Privacy Commissioner, 1999. str 1-14. URL: https://www.ipc.on.ca/images/resources/pri-biom.pdf (2016-06-25)

sposobnosti sustava. Opseg i funkcionalnost sustava ne bi trebali biti prošireni bez izričitog dopuštenja i obavještavanja svih korisnika. Sposobnost zadržavanja biometrijskih podataka mora biti minimalna, što znači da se verifikacijski podaci trebaju uvijek brisati, a biometrijski predlošci čuvati. Također, korisnik treba biti obavješten o brisanju verifikacijskih podataka. Zaštita podataka je druga točka osiguravanja privatnosti. Prije svega vrlo je važna uporaba odgovarajućih tehnologija za zaštitu podataka. Biometrijski sustavi trebaju se koristiti u kontroliranim i sigurnim uvjetima. Također, važno je istaknuti da samo ograničen broj operatera treba imati pristup biometrijskim podacima. Kontrola osobnih podataka korisnika označava da korisnik mora zadržati kontrolu nad svojim biometrijskim podacima, da korisnici biometrijski sustav moraju koristi dobrovoljno i nikako drugačije te da korisnik ima mogućnost mijenjanja i brisanja svojih osobnih podataka. Zadnja točka je područje vezano uz odgovornost za biometrijske podatke. Svaki operater mora biti upoznat sa svrhom biometrijskog sustava. Važno je znati kada se koristi biometrijski sustav pogotovo kada se provodi verifikacijska ili identifikacijska faza. Operateri moraju preuzeti odgovornost za eventualno počinjene pogreške tijekom provođenja neke od biometrijskih faza. [36]

4. Zaštita informacijskih sustava i informacijska sigurnost

Informacijski sustav je strukturirani sustav u kojem se međusobno povezani softver, hardver i telekomunikacijske mreže. Informacijske sustave grade ljudi u svrhu prikupljanja, upravljanja i obrade podataka. Informacijski sustavi su ključni elementi svakog poslovanja. Informacijska sigurnost je važan dio sigurnosti informacijskih sustava. Informacijska sigurnost je stanje povjerenja, cjelovitosti i raspoloživosti podataka. Takvo stanje postiže se primjenom zakonom propisanih standarada i mjera za informacijsku sigurnost. Pod tim pojmom smatra se zaštita informacijskih sustava od prijetnji, kako se ne bi narušio poslovni kontinuitet te da se razina rizika od prijetnji što više smanji. Prijetnje su sve akcije koje ugrožavaju sigurnost informacijskog sustava odnosno informacija pohranjenih u njemu. Prijetnja informacijskom sustavu mogu biti ljudi odnosno njihovo namjerno i nenamjerno djelovanje, mehanička i sl. oštećenja opreme i elementarne nepogode. Brojne organizacije susreću se s velikim brojem prijetnji kao što su računalne prevare, špijunaže, hakiranja ali i s potresima, poplavama i brojnim drugim prirodnim nepogodama koje također uništavaju važne podatke. Informacijska sigurnost se postiže implementacijom odgovarajućih mjera zaštite. Informacijsku sigurnost čine pet područja, a to su:

[36] Usp. Privacy in Biometrics, 2009. str 1-24.

fizička sigurnost, sigurnost podataka, sigurnost poslovne suradnje, sigurnosna provjera i sigurnost informacijskog sustava. Fizička sigurnost je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere zaštite objekata, uređaja i prostora u kojem se nalaze podaci. Sigurnost podataka je drugo područje informacijske sigurnost koje se odnosi na otkrivanje i otklanjanje štete nastale od gubitka podataka ili od neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka. Sigurnosna provjera je područje informacijske sigurnosti unutar kojeg se primjenjuju mjere zaštite na osobe koje imaju pristup klasificiranim podacima. Sigurnost poslovne suradnje odnosi se na obveze pravnih i fizičkih osoba koje imaju pristup ili se koriste klasificiranim i neklasificiranim podacima. Sigurnost informacijskog sustava je zadnje područje informacijske sigurnosti koji je zapravo dokument za vlasnika informacijskog sustava. Tim dokumentom definiraju se odgovornosti, mjere i standardi unutar informacijskog sustava. [37]

5. Korisnička percepcija o biometriji

Stavovi i mišljenja o biometriji su podvojena. Brojni korisnici su izrazili interes za ovakvu vrstu tehnologije te su prepoznali prednost biometrije zbog njezine sigurnosti i pouzdanosti. No, s druge strane korisnici biometrijske sustave doživljavaju kao prijetnju njihovoj privatnosti. Mnogi misle da je točnost identifikacije u biometrijskim sustavima 100% te da su biometrijski uzorci pohranjeni, poslani na mrežu ili na neki drugi način izloženi javnosti što kod mnogi izaziva zabrinutost. Naravno, poznato je da se prikupljeni biometrijski podaci ne mogu koristi u svrhe izvan namijenjenih iako postoje situacije gdje to nije tako. Brojni korisnici strahuju i od mogućnosti da ih se prati u svim aktivnostima i mjestima. Korisnici strahuju da ih superiorna osoba pomoću biometrijskog sustava promatra i zna sve o njihovim aktivnostima. Mali dio populacije smatra korištenje biometrijskih sustava neugodnim ili opasnim po zdravlje budući da su npr. senzori otiska prsta prethodno korišteni od strane druge osobe, a nisu prikladno očišćeni. Također, neki korisnici strahuju od mogućnosti oštećenja očiju prilikom laserskog skeniranja šarenice. Kao što je već spomenuto, mnoge se biometrijske karakteristike mogu koristiti za dobivanje osobnih podataka korisnika kao što su informacije o povijesti bolesti i sl. Npr. uzorak mrežnice oka može otkriti vrijedne informacije o prisutnosti dijabetesa, hipertenzije i brojnih drugih bolesti što korisnici smatraju vrlo neugodnim. [38]

[37] Usp. Boban, Marija; Perišić, Mirjana. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. str. 118-119. URL: http://hrcak.srce.hr/142285 (2016-06-10)
[38] Usp. Privacy in Biometrics, 2009. str 1-24.

CTA istraživanje o biometrijskim tehnologijama i njihovoj prihvaćenosti od strane korisnika provedeno je u SAD-u 2016. godine. Ono je pokazalo je da manje od polovine odraslih osoba prihvatilo ili koristilo neku od vrsta biometrijske tehnologije. Otisak prsta i prepoznavanje glasa dvije su najviše korištene i prihvaćene biometrijske metode identifikacije. Većina ispitanika osjeća se sigurno s biometrijskim tehnologijama na mjestima koja su visoko zaštićena ili koja trebaju veću zaštitu. Više od polovine (63%) odraslih ispitanika su otvoreni i spremni na korištenje biometrijskih tehnologija za vlastite potrebe kao što su npr. medicinska istraživanja (58%). No, ispitanici smatraju da organizacije trebaju educirati korisnike o prednostima biometrije i njihove uporabe. Samo 28% ispitanika se ne osjeća ugodno pri pomisli na korištenje biometrijske tehnologije.[39] GIGYA istraživanje provedeno 2015. godine pokazalo je da 41 % stanovnika USA-a ima veliku razinu povjerenja u prijavljivanje na web stranice i mobilne aplikacije koristeći svoje otiske prstiju. No, više od 90% USA i UK korisnika su na neki način zabrinuti za privatnost njihovih podataka i na način koji ustanove koriste njihove podatke.[40] Treće istraživanje provedeno 2014. godine među stanovnicima Ujedinjenog Kraljevstva dokazalo je da 79% ispitanika i ujedno korisnika biometrijskih tehnologija je spremno odbaciti lozinke i zamijeniti ih skenerima otisaka prstiju, a 53% ispitanika bi voljeli kada bi njihove banke implementirale skenere za otiske prstiju u svoje digitalne usluge.[41]

Istraživanje provedeno 2015. godine u razdoblju od travnja do lipnja obuhvaćalo je područje biometrijske identifikacije u uređajima najbližim krajnjem korisniku kao što su pametni telefoni. Istraživanjem se htjelo uvidjeti kakva je korisnička percepcija o sigurnosti biometrijske identifikacije na pametnim telefonima, kako oni percipiraju korisnost i pouzdanost identificiranja šarenice oka te se htjelo vidjeti utječu li demografski čimbenici kao što je dob na percepcije korisnika. Anketa je bila u online obliku i sastojala od dva dijela, prvi dio se odnosio na percepciju korisnika o sigurnost i privatnosti biometrijske identifikacije na pametnim telefonima, a drugi dio se odnosio na percepciju korisnika o korištenju identifikacije putem šarenice oka na pametnim telefonima. Većina ispitanika koja je sudjelovala u istraživanju je bila u dobi između 25 i 44 godine. Ispitanici se slažu s potrebom zaštite podataka i sigurnosti na njihovim pametnim telefonima (šifriranje podataka, zaštita telefona od krađe, zloupotrebljavanja, hakiranja i sl.). Vrlo važnim smatraju i zaštitu svojih osobnih podataka kao što su ime, prezime, lokacija, zanimanje i sl. Kod starijih ispitanika važnost zaštite i sigurnost informacija na pametnim telefonima bila je veća nego kod mlađih ispitanika. 85% ispitanika u dobi između 25 i 44 godine iskazali su visok

[39] Usp. IBA. Recent Opinion Surveys on Public Perceptions of Biometrics, str 1
[40] Isto, str 3-4.
[41] Isto, str 4.

značaj zaštite njihovih informacija na pametnim telefonima, a samo 67% u dobi između 15 i 24 godine složilo se s istim. Istraživanjem je i dokazano da ispitanici više preferiraju moderne tehnologije te su pokazali veliku zainteresiranost za identifikaciju putem šarenice oka. Najveći broj ispitanika za idealnu kombinaciju za zaštitu i dodatnu sigurnost izabralo je lozinku i otisak prsta, a njih 21% odgovorilo je da im nije bitno sve ukoliko nije kompliciranо. Zaključeno je da ispitanici smatraju da je sigurnost podataka i privatnost na pametnim telefonima jako važna. Ispitanici ne vjeruju tehnologijama koje nisu toliko popularne i dovoljno promovirane kao što su prepoznavanje lica i ušiju. Kada se radi o prepoznavanju šarenice oka mnogim korisnicima nije problem prilagoditi se ograničenjima poput toga da se tijekom identifikacije oko ne smije micati kao ni telefon te da se moraju skinuti dioptrijske naočale, no neki ispitanici su izrazili nezadovoljstvo što su trebali pronaći savršeno osvjetljenje kako bi identifikacija bila moguća. Vrlo je važno istaknuti da se 90% ispitanika znalo služiti svim biometrijskim metodama identifikacije dovoljno dobro da bi se osigurao biometrijski uzorak koji zadovoljava njihove kriterije kvalitete. [42]

6. Zaključak

Budući da je biometrija relativno mlada disciplina, tek je u novije doba doživjela svoj procvat i prihvaćanje. Razlog njezinog prihvaćanja može se povezati s ubrzanim razvojem moderne tehnologije i povećanom uporabom iste. Biometrija i njezin spektar mogućnosti prelazi granice poznatog i zbog toga mnogi ljudi i dalje strahuju od njezine svakodnevne uporabe bilo u privatnom ili državnom području ili u poslove svrhe. Biometrijske tehnologije gotovo nepogrešivo provode mjerenja tjelesnih obilježja, ali i obilježja ponašanja. Dok jedni to percipiraju kao prednost, drugi strahuju od sigurnosti njihovih osobnih podataka, a samim time i njih samih. No, može li se biometrija smatrati prijateljem u zaštiti privatnosti i održavanju sigurnost ili pak neprijateljem najviše ovisi način na koji je sustav dizajniran. Ukoliko se sustav precizno i pravilno dizajnira i informacijski vodi on je zasigurno velika pomoć u očuvanju sigurnosti. Tehnologije omogućavaju

[42] Usp. Zirjawi, Nedaa; Kurtanović, Zijad; Maalej, Walid. A Survey about User Requirements for Biometric Authentication on Smartphones// IEEE, 2015. str 1-6. . URL: https://mobis.informatik.uni-hamburg.de/wp-content/uploads/2015/07/2015_BiometrySurvey_PrePrint.pdf (2016-06-25)

zaštitu privatnosti i očuvanje sigurnosti ukoliko su i dizajnirane s tim ciljem. Prije samo malo više od deset godina mnogi ljudi nisu se znali služiti niti su posjedovali tehnologiju koja je danas opće prihvaćena i neizostavna poput računala i mobilnih telefona. S istom sudbinom se može i trebala bi se suočiti biometrija i njezine tehnologije. Biometrija je daleko pouzdanija i učinkovitija od tradicionalnih metoda prepoznavanja, lakša je i brža za korištenje te zahtjeva minimalan napor korisnika biometrijskih tehnologija. S podizanjem svijesti u zajednici i u društvu općenito, biometrijske tehnologije u skorije vrijeme mogle bi pronaći svoje mjesto u svakoj državnoj ili privatnoj ustanovi, industriji, organizaciji i svakom drugom neizostavnom području ljudskoga života.

Literatura

1. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. Str. 1-16. URL: https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf (2016-06-25)
2. Biometric Recognition: Security and Privacy Concerns. // IEEE Security & Privacy, 2003. str 33-42 URL: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf (2016-06-20)
3. Biometrics Security and Privacy Protection. // IEEE Signal Processing Magazine, 2015. str 17-18. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7192815 (2016-06-25)
4. Boban, Marija; Perišić, Mirjana. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. str. 115-148. URL: http://hrcak.srce.hr/142285 (2016-06-10)
5. Cavoukian, Ann. Privacy and Biometrics. Ontario: Information and Privacy Commissioner, 1999. str 1-14. URL: https://www.ipc.on.ca/images/resources/pri-biom.pdf (2016-06-25)
6. Parke, Conor. Biometrics in the Workplace. str. 1-6. URL: http://www.academia.edu/11950137/The_use_of_Biometrics_in_the_Workplace (2016-06-10)
7. Pato, Joseph N; Millett, Lynette I. Biometric Recognition: Challenges and opportunities. Washington: The national academies press, 2010. str 1-183 URL: http://dataprivacylab.org/TIP/2011sept/Biometric.pdf (2016-06-25)
8. Privacy in Biometrics, 2009. str 1-24.
9. Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008), str. 159-180.
10. IBA. Recent Opinion Surveys on Public Perceptions of Biometrics
11. Uddin, Jasmin. Matrix of Biometrics// Biometrics, 2016. str 1-3. URL: https://www.researchgate.net/publication/301542522_Matrix_of_Biometrics (2016-06-25)
12. Zirjawi, Nedaa; Kurtanović, Zijad; Maalej, Walid. A Survey about User Requirements for Biometric Authentication on Smartphones// IEEE, 2015. str 1-6. URL: https://mobis.informatik.uni-hamburg.de/wp-content/uploads/2015/07/2015_BiometrySurvey_PrePrint.pdf (2016-06-25)

13. Wayne, Penny. Biometrics: A Double Edged Sword - Security and Privacy, 2002. str 2-13. URL: https://www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edged-sword-security-privacy-137 (2016-06-20)