Nove tehnologije u nacionalnoj sigurnosti

Radelić, Samanta

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department for Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:695227

Rights / Prava: Attribution-NonCommercial-NoDerivs 3.0 Unported/Imenovanje-Nekomercijalno-Bez prerada 3.0

Download date / Datum preuzimanja: **2024-03-29**

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

Repository / Repozitorij:

Repository of University Department for Forensic Sciences

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNA SIGURNOST

DIPLOMSKI RAD

NOVE TEHNOLOGIJE U NACIONALNOJ SIGURNOSTI

SAMANTA RADELIĆ

Split, rujan, 2020. godine

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNA SIGURNOST

DIPLOMSKI RAD

NOVE TEHNOLOGIJE U NACIONALNOJ SIGURNOSTI

MENTOR: izv. prof. dr. sc. Marija Boban

SAMANTA RADELIĆ

MATIČNI BROJ STUDENTA: 414/2017

Split, rujan,2020. godine

Rad je izrađen na Sveučilišnom odjelu za forenzične znanosti uz pomoć izv. prof. dr. sc. Marije Boban u ulozi mentorice i komentorice u razdoblju od travnja 2020. godine do srpnja 2020. godine.

Datum predaje diplomskog rada: 17. rujan 2020. godine

Datum prihvaćanja diplomskog rada: 21. rujan 2020. godine

Datum usmenog polaganja: 28. rujan 2020. godine

Povjerenstvo:

1. Prof dr. sc. Jozo Čizmić
2. Doc.dr. sc. Marina Carić
3. Izv.prof. dr. sc. Marija Boban

SADRŽAJ

1.UVOD 1

2. NACIONALNA SIGURNOST 2

2.1 Strategija nacionalne sigurnost Republike Hrvatske 4

3.BIOMETRIJA 6

3.1 Biometrijska identifikacija 8

3.2 Biometrijske karakteristike 9

3.2.1. Otisak prsta 9

3.2.2. Lice 12

3.2.3. Glas 13

3.2.4.Šarenica i mrežnica oka 14

3.2.5. Potpis 15

3.3 Biometrija u sustavu nacionalne sigurnosti 17

3.4. Biometrija i zaštita privatnosti 20

4.GDPR I VIDEONADZOR 22

5.RAZVOJ SUSTAVA VIDEONADZORA 26

6. UČINKOVITOST VIDEONADZORA U SMANJENJU KRIMINALITETA 28

7. ISTRAŽIVANJE O PRIMJENI NOVIH TEHNOLOGIJA U SIGURNOSTI RH 31

8.ZAKLJUČAK 39

9.SAŽETAK 40

10.SUMMARY 41

11.LITERATURA 42

12.ŽIVOTOPIS 46

13. IZJAVA O AKADEMSKOJ ČESTITOSTI 47

1.UVOD

U prvom djelu rada pisat će se općenito o nacionalnoj sigurnosti, njenoj definiciji i shvaćanju samog pojma kroz povijest. Naime, pojam nacionalna sigurnost često se poistovjećuje s pojmom nacionalnih interesa. Iako im definicija nije ista pojmovi nacionalna sigurnost i nacionalni interesi u odnosu su međuovisnosti. Nacionalna sigurnost je djelatnost koja se uvijek zasniva na nacionalnim interesima te zaštiti nacionalnih interesa svake države.

Drugi dio rada posvećen je biometriji i njenoj implementaciji u sustav nacionalne sigurnosti.

Pišući o sustavu videonadzora i uvjetima pod kojim se navedeni može koristiti ne možemo se ne dotaknuti Opće uredbe o zaštiti osobnih podataka, odnosno GDPR-a.

Osim razvoja sustava videonadzora na kraju rada daje se uvid učinka videonadzora na svijest potencijalnog počinitelja kaznenog djela.

Za kraj rada provedena je online anketa na uzorku 106 ispitanika svih dobi dobi kako bi se dobio uvid u stavove ljudi o videonadzoru, biometriji, korištenju biometrijskih podataka i njihovoj distribuciji te korištenju biometrijskih podataka pri pristupu aplikacijama.

2. NACIONALNA SIGURNOST

Pri određivanju definicije pojma nacionalne sigurnosti često se susrećemo s problemom definiranja istog. Pojam nacionalna sigurnost nerijetko se poistovjećuje sa pojmom državne sigurnosti u smislu održavanja ustavnog poretka te s nacionalnom obranom.

Shvaćanje navedenog pojma razlikuje se od autora do autora. Povijesno određenje pojma nacionalne sigurnosti uvijek je bilo povezano sa sukobima i rivalitetom između država. Neki navode kako shvaćanje pojma ovisi od pojedinca, njegovom stanju i svijesti. Drugi navode kako je nemoguće definirati pojam, dok postoje autori koji pojam nacionalne sigurnosti određuju obuhvaćajući vrijednosti poput političke samostalnosti, opstanka, teritorijalne cjelovitosti, kvalitete života, obuhvaćajući time sve vrijednosti koje su sadržane u pojmu nacionalne sigurnosti.

Tako, Arnold Wolfers govori o problematici definiranja pojma nacionalne sigurnosti navodeći kako se isti ne smije promatrati samo sa vojnog gledišta, te je nacionalna sigurnost za njega neodređeni simbol koji može a i ne mora imati značenje.

Michael H.H. Louw drži da osim obrambene politike države treba voditi računa i o njenim nevojnim djelatnostima.

Penelope Hartland-Thunberg navodi definiciju nacionalne sigurnosti kao sposobnosti nacije da uspješno provodi vlastite interese.

Amin Hewedy nacionalnu sigurnost definira kao djelatnost nacionalnih država, koje sukladno vlastitim društvenim mogućnostima, a uz poštivanje globalnih promjena i razvitka, štite vlastiti identitet, opstanak i interese.

Božidar Javorović kaže da "nacionalna sigurnost podrazumijeva unutarnju i vanjsku sigurnost države, odnosno sigurnost države u odnosu na vanjske i unutarnje opasnosti i ugroženosti."[1]

Mario Nobilo piše o pojmu nacionalne sigurnosti kao složenoj interakciji ekonomskih, političkih, vojnih, pravnih, ideoloških, socijalnih te drugih unutrašnjih i vanjskih faktora kroz koje države nastoje različitim instrumentima osigurati prihvatljive uvijete očuvanja

[1] Darko Lacković, Poteškoće u definiranju pojma nacionalne sigurnosti, Stručni rad, 1. rujna 2000. godine, str. 199

suvereniteta, teritorijalnog integriteta, fizičkog opstanka stanovništva, političku nezavisnost te mogućnost za ravnopravan, skladan i brz društveni razvoj.[2]

Uz ovaj kratak pregled definicija (gdje naravno, nisu navedeni svi autori i slučajevi definiranja pojma nacionalne sigurnosti), dolazimo do zaključka kako se nacionalna sigurnost uvijek zasniva na nacionalnim interesima te zaštiti nacionalnih interesa svake države.

Nacionalni interesi se određuju unutar svake države donošenjem Strategije nacionalne sigurnosti. Kriteriji po kojima se nacionalni interesi oblikuju jesu:

- Ekonomski
- Ideološki
- Vojni
- Kriterij sile, morala i legaliteta
- Kulturni
- Rasni kriterij i dr.[3]

Prilikom određivanja nacionalnih interesa uvijek treba voditi računa o nacionalnim mogućnostima potrebnim za ostvarenje istih kako ne bi došlo do kraha. Također, pri određivanju nacionalnih interesa valja voditi računa i o određenim čimbenicima:

- Unutarnja situacija u državi,
- Struktura međunarodnog sustava,
- Interesi različitih društvenih slojeva,
- Percepcija i interesi političke elite i dr.[4]

Iz navedenog možemo razlučiti kako su nacionalni interesi i nacionalna sigurnost u uskoj vezi. Nacionalni interesi su, kao vrijednosti i ciljevi, usmjereni ka razvoju nacionalne

[2]Darko Lacković, Poteškoće u definiranju pojma nacionalne sigurnosti, Stručni rad, 1.rujna 2000.godine, str. 198-199
[3]Vlatko Cvrtila, Nacionalni intersei i nacionalna sigurnost, Pregledni članak, 1995. godina, str. 63
[4]Vlatko Cvrtila, Nacionalni intersei i nacionalna sigurnost, Pregledni članak, 1995. godina, str. 65

zajednice dok je s druge strane nacionalna sigurnost djelatnost koja je organizirana kako bi zaštitila te interese i mehanizme koji su potrebni da bi se oni ostvarili.

2.1 Strategija nacionalne sigurnost Republike Hrvatske

Svrha Strategije nacionalne sigurnosti je jasno definiranje i određivanje temeljnih nacionalnih interesa zemlje. Unazad tri godine u Republici Hrvatskoj na snazi je bila Strategija nacionalne sigurnosti iz 2002.godine. S obzirom na ciljeve koji su u njoj bili navedeni (zbrinjavanje izbjeglica iz Domovinskog rata, ulazak u EU, ulazak u Nato itd.) jasno je bilo kako je Republici Hrvatskoj trebala nova Strategija. Naravno, nova Strategija nacionalne sigurnosti je bila potrebna ne samo zbog ostvarenja ciljeva iz stare Strategije već i zbog pojave novih ugroza za nacionalnu sigurnost Republike Hrvatske.

U srpnju 2017.godine Republika Hrvatska dobila je novu Strategiju nacionalne sigurnosti te je ista objavljena u Narodnim novinama 26.srpnja 2017.godine. (NN73/2017).

Strategija predviđa četiri nacionalna interesa i devet strateških ciljeva.

Nacionalni interesi su:

- dobrobit i prosperitet,

- sigurnost,

- nacionalni identitet,

- međunarodni utjecaj i ugled te ravnopravan položaj,

- suverenitet,

- opstanak.

Neki od strateških ciljeva su:

- dostizanje najvišeg stupnja sigurnosti i zaštite stanovništva te kritičnih infrastruktura,

- razvoj i održavanje snažne i aktivne obrane,

- uspostava razvoja sustava domovinske sigurnosti,

- ekološka Hrvatska,

- razvoj snažnog i održivog gospodarstva.

Novom Strategijom također se naglašava kako je njen razvoj trajan proces unutar kojeg će svaka Vlada, u suradnji sa Predsjednikom, na početku mandata predlagati novu ili izmjenu postojeće Strategije.

Strategija nacionalne sigurnosti Republike Hrvatske obvezuje sva državna tijela da donesu svoje strateške i druge dokumente kojima će, u okvirima svojih nadležnosti, određivati konkretne ciljeve, mjere, postupke i sposobnosti zaštite nacionalne sigurnosti.[5]

[5]Republika Hrvatska, Ured vijeća za nacionalnu sigurnost, Strategija nacionalne sigurnosti Republike Hrvatske, Dostupno na : https://www.uvns.hr/hr, Preuzeto: (15.02.2020)

3.BIOMETRIJA

Kada govorimo o razvoju i pojmu biometrije vraćamo se na sam početak ljudskog postojanja. Tada su ljudi koristili karakteristike tijela poput lica, glasa, hoda kako bi prepoznali jedni druge.

U 3. stoljeću prije Krista u Kini su se otisci prstiju koristili kao potpisi. Kako bi spriječili zamjenu novorođenčadi, Kinezi su također koristili daktiloskopiju. Asirci i Babilonci su koristili neke od metoda identifikacije utiskivanjem otisaka papilarnih linija kao dokaz autorstva nad dokumentima.

U 18. stoljeću opće je poznato kako se može upravljati identitetom pomoću jedinstvenih fizičkih karakteristika ljudi. Alphonse Bertillon u 19. stoljeću u Parizu, razvio je ideju korištenja fizičkih mjera kao što su dužina ruku, stopala i prstiju, visina u svrhu lakše identifikacije kriminalaca. Ova ideja postaje sve zastupljenija ali otkrićem otisaka prstiju postaje potisnuta. Zbog jedinstvenosti otisaka prstiju mnogi zakonski i pravni odjeli podupiru ideju uzimanja otisaka prstiju od kriminalaca te stvaranja baze podataka. Nedugo nakon toga policija razvija način uzimanja fragmenata otisaka prstiju s mjesta zločina, koji kasnije može usporediti s onima koji se nalaze u bazi podataka.

2005.godine RTE vijesti obavijestile su kako se biometrijske tehnologije sve više razvijaju te usvajaju na radnim mjestima u Irskoj. Tada su sindikati i radnici strahovali od gubitka privatnosti nad osjetljivim podacima. Sukladno tome pojavljuju se brojna pitanja i etičke rasprave vezane za biometriju.

Kao što možemo primijetiti iz ovog kratkog pregleda biometrije kroz povijest ona se prvo koristila u forenzičke i pravne svrhe dok se danas sve više koristi od strane privatnih i državnih organizacija.

Tri bitne stvari promijenile su se kod biometrije kroz povijest:

a) Tehnološka transformacija

- vrste i oblici biometrijskih informacija, metode i upravljanje biometrijskim podacima te pouzdanost tih podataka zbog razvoja tehnologije doveli su do toga da je danas biometrijski sustav gotovo nepogrešiv.

b) Značaj biometrijskih karakteristika

- npr. Otisak prsta koji se upotrebljavao kao osobni potpis a do danas je prerastao iz pravnog u pretraživački i identifikacijski alat.

c) Vlasništvo 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. [6] Na brojna pitanja još se uvijek traži odgovor.

Sumirajući povijesni razvoj biometrije (grčki bios = život i metrikos = mjera) uviđamo kako je biometrija 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.[7]

U svrhu identifikacije osobe biometrija koristi njene fizičke i biološke karakteristike. Biometrija se ne oslanja na ono što osoba zna (npr. lozinka) ili ono što osoba posjeduje (npr. osobna iskaznica) već se u potpunosti oslanja na činjenicu tko je osoba i što ona radi. Prednost biometrije je u tome što ona može nadopuniti ili u potpunosti zamijeniti postojeću tehnologiju. Biometrija je u nekim tehnologijama jedini održivi pristup osobnom identificiranju.

Biometrija ima prednost pred tradicionalnim oblicima prepoznavanja koje se temelje na znanju korisnika (lozinka, pin) ili na onome što korisnik fizički posjeduje (kartica, ključ).

[6]Mihaela Konjevod, Biometrija i zaštita privatnosti, završni rad, Osijek 2016. godine, str. 3

[7]Ibidem

Jedna od glavnih prednosti biometrije je ta što korisnik ne mora pamtiti lozinke, brinuti o njihovom mijenjanju i složenosti te ne mora sa sobom nositi kartice ili ključeve. Biometrija je lakša i brža za korištenje te zahtjeva minimalan korisnikov napor. Također, biometrija je teža za napasti a razina sigurnosti u biometrijskom sustavu je za sve ista.

3.1 Biometrijska identifikacija

Svaka osoba, predmet ili životinja razlikuje se od drugih. Ponekad je tu razliku, zbog sličnosti između vrsta, teško utvrditi bez primjene određenih metoda. Spomenutim metodama u postupku identifikacije detektirat će se detalji u kojima se objekti razlikuju.

Identitet predstavlja ukupnost nepromjenjivih obilježja koja čine određenu osobu ili predmet, a prema kojima se ona/ono može razlikovati od svih drugih[8]

Biometrijska identifikacija temelji se na prepoznavanju obrasca ponašanja te usporedbe istog s uzorkom koji je otprije pohranjen u bazi podataka u podatkovnom obliku.

Biometrijski sustav sastoji se od:

a) ulaznih jedinica
   - one služe za registriranje i mjerenje određenog biometrijskog obilježja.
b) ekstraktora
   - jedinica koja služi za izdvajanje nekog obilježja iz cjeline.
c) baze podataka
d) jedinice za verifikaciju komparacije
   - provjerava kvalitetu i kvantitetu spornih obilježja te ih nakon toga uspoređuje s ranije pohranjenim obilježjima.

[8] Želimir Radmilović, Biometrijska identifikacija, Stručni članak, kolovoz 2018. godine, str. 161

Metode tjelesne biometrije, koje se temelje na nepromijenjenosti i individualnosti pojedinih dijelova ljudskog tijela, koriste brojni sigurnosni sustavi kako bi utvrdili je li osoba ta za koju se predstavlja. Važno je napomenuti kako takva identifikacijska provjera ne smije zadirati u tjelesni integritet osobe te može biti brza, jeftina i pouzdana

3.2 Biometrijske karakteristike

3.2.1. Otisak prsta

Kada spominjemo otisak prsta govorimo o najstarijoj metodi provjere identiteta. Kao službena metoda provjere identiteta u zakonodavnom sudu prihvaćen je u ranom 20-tom stoljeću. Deset tjedana nakon začeća on se formira kod čovjeka te ostaje nepromijenjen do kraja života. Izuzetak su slučajevi porezotina, opeklina ili kemijskih oštećenja gdje se otisak prsta može promijeniti. Otisak prsta jedinstven je za svaku osobu.

Otisak prsta uzima se na dva načina:

a) Skeniranje utiska prsta od tinte na papiru

b) Uređaj za trenutačno skeniranje otiska prsta[9]

Otisak koji ostavlja struktura brazdi na jagodici prstiju, odnosno struktura papilarnih linija, je ustvari otisak prsta. Papilarne linije mogu se također pronaći i na dlanovima te na stopalima. Neke životinje (gotovo svi sisavci) također imaju papilarne linije na rukama i nogama kao što je slučaj kod majmuna. Zanimljivo je npr. slučaj kod krava gdje se njihove papilarne linije nalaze na njušci.

Napretkom tehnologije otisci prstiju više se ne uspoređuju ručno kao nekad, već to rade različiti računalni sustavi koji omogućuju automatizirano prepoznavanje. Biometrija

[9]Tarek Saghir, Problem sigurnosti i privatnosti u biometrijskoj identifikaciji, diplomski rad, Varaždin 2018. godine , str. 9

raspoznavanja otisaka prsta u cijelosti se zasniva na daktiloskopiji.[10] Karakteristike otisaka prsta su:

a) Trajnost – od rođenja do raspadanje kože oblik papilarnih linija je trajan.

b) Stalnost – dermatoglifi u principu imaju stalan oblik kroz čitav čovjekov život, osim u slučaju traumatoloških oštećenja gdje se mogu promijeniti.

c) Individualnost – na svijetu ne postoje osobe s identičnim otiscima prstiju.



Slika 1. Otisak prsta

Dostupno na: Genius Croatia, http://en.genius-croatia.com/, Preuzeto: (04.02.2020)

Iz perspektive računala otisci prstiju jesu digitalne slike. Sustav za automatizirano procesuiranje otisaka prstiju sastoji se od 3 podsustava:

1). Podsustav za pred procesuiranje

[10] Otisak prsta, Ivan Drakić, Bača, Miroslav; Schatten, Markus; Kišasondi, Tonimir: Prstom otključaj vrata, ZAŠTITA, Časopis o zaštiti i sigurnosti osoba i imovine, broj 2, godina II, Zagreb, 2006.

- prije samog prepoznavanja otiska izvodi se pred procesuiranje,

- zadaća ovog podsustava je da normalizira sliku po veličini, osvjetljenju, kontrastu, rotaciji otiska te neutralizacija pozadine.

2.) Podsustav za detekciju otiska

- zadaća ovog sustava je odrediti sadrže li predstavljeni podaci jedan ili više otisaka te gdje se oni točno nalaze na slici.

3.) Podsustav za prepoznavanje otisaka

- zadaća ovog podsustava je utvrđivanje identiteta osobe.

Uz navedene podsustave tu je još i baza podataka gdje se vrši prepoznavanje a u kojoj su pohranjeni otisci prstiju. Uklanjanje suvišnih informacija, određivanje glavnih obilježja i usporedba s uzorkom iz baze podataka su koraci koji vrše u obradi podataka.

Utjecaji kojima su podložni prsti (npr. voda, prljavština) moraju se otkloniti kako bi papilarne linije bile dobro vidljive i čiste. Takozvani filtri zalihnosti koriste se kako bi se sa slike odbacile sve linije koje nisu u smjeru papilarnih linija. Posljednja faza je stanjivanje kojim se širina papilarne linije reducira na jedan piksel. Stanjivanjem se smanjuje višak informacija a bez mijenjanja karakteristika otiska prsta.

Nadalje, dolazimo do faze određivanja karakterističnih točaka gdje se određuju grananja linija (minuciji) te njihovi završeci.

Izrada grafa karakterističnih točaka zadnja je faza. Raspon od 10 do 100 točaka je broj u kojem se kreće broj karakterističnih točaka.

U današnje vrijeme nekoliko različitih tehnologija koristi se za prepoznavanje otisaka prstiju a najpoznatije od njih su: optički senzori, termo-električni senzori, senzori elektroničkog polja, kapacitivni senzori, senzori bez dodira, senzori osjetljivi na pritisak.

3.2.2. Lice

Kao jedna od uobičajenih metoda identifikacije pri ljudskoj vizualnoj interakciji smatra se lice. Lice je jedna od najprihvatljivijih biometrijskih karakteristika. Ona se izvršava tako da se uspoređuje kontrolirani, statički, cijeli portret lica s prednje strane.

Dva glavna zadatka kod prepoznavanja lica jesu:

a) lokacija lica

b) prepoznavanje lica[11]

Lokacija lica ne predstavlja problem budući da je pozadina kontrolirana. Prepoznavanje lica zahtjevnije je od lokacije lica jer se kod prepoznavanja lica pronalaze sličnosti lociranog lica sa spremljenim predlošcima kako bi se uspješno utvrdio identitet.

Aplikacija koja prepoznaje lica radi tako da analizira karakteristike lica pa je stoga potrebna digitalna kamera kako bi se razvila digitalna slika korisnika za identifikaciju.



Slika 2. Biometrijske karakteristike lica

Dostupno na: https://www.iotworldtoday.com/, Preuzeto: (13.03.2020)

[11] Ibidem

Prepoznavanje lica kao biometrijska karakteristika postaje sve popularnije u današnje vrijeme. Kamere na pametnim mobilnim uređajima, kamere, sigurnosni video nadzori svugdje su oko nas. Za navedene uređaje postoje softveri ili aplikacije koje omogućuju prepoznavanje lica. Facebook je društvena mreža koja je među prvima počela koristiti prepoznavanje lica u komercijalne svrhe. Mjesta od sigurnosne važnosti npr. zračne luke koriste sustav prepoznavanja lica. Analiza strukture lica vrši se na cjelokupnoj strukturi lica i to funkcionira u blizini ali kako se korisnik udaljuje dolazi do progresivnog gubljenja točnosti analize.

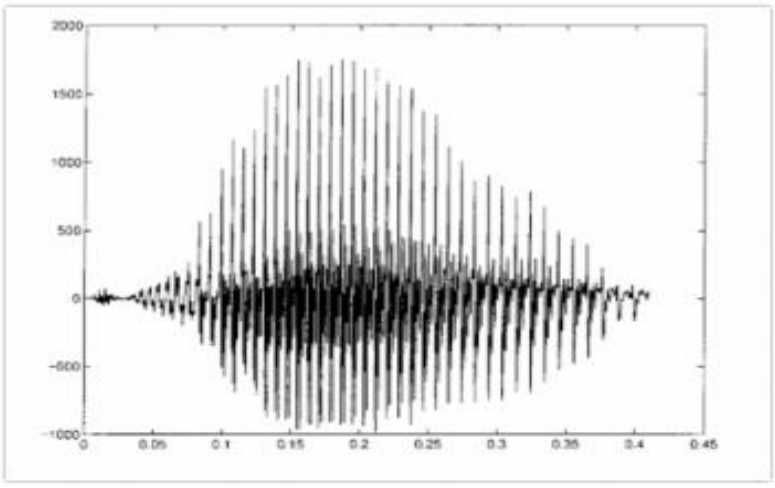
3.2.3. Glas

Govoreći o identifikaciji osobe na temelju glasa zapravo govorimo o identifikaciji glasa temeljenoj na karakteristikama glasa poput: boje glasa, frekvencije, modulacije, govornim manama, specifičnosti izgovora određenih glasova i slično. Iako je glas individualna karakteristika svake osobe ne smatra se dovoljno jedinstvenim za izvršenje stopostotne identifikacije korisnika.

Glas za identifikaciju uvelike ovisi o uvjetima poput kvalitete mikrofona kojim se snima, komunikacijskom kanalu te digitalizatoru karakteristika.

Autentifikacija glasa, odnosno prepoznavanje glasa nije samo bazirana na prepoznavanju glasa osobe već i na pretvorbi zvuka u tekst. Pretvorba zvuka u tekst vrši se pomoću kompleksne tehnologije.

Promatrajući razvoj tehnologije, trendova u tehnologiji i umjetnoj inteligenciji možemo zaključiti kako postoji sve veća vjerojatnost da će verifikacija osobe preko glasa zamijeniti ili postati dodatak lozinkama, pinovima i korisničkim računima.



Slika 3. Signal glasa

Dostupno na: Tarek Saghir, Problem sigurnosti i privatnosti u biometrijskoj identifikaciji, diplomski rad, srpanj 2018. godine, str. 13, Preuzeto: (13.03.2020)

3.2.4.Šarenica i mrežnica oka

Ljudsko oko sadrži veliki broj individualnih karakteristika te je zbog toga izuzetno povoljno za postupak identifikacije. Jedinstvenost oka čini njegova šarenica (iris) te je ona zajedno sa mrežnicom (retina) oka posebno pogodna karakteristika za identifikaciju.

U optičkom smislu šarenica oka služi za zatvaranje i otvaranje zjenice kako bi propustila svjetlo. Njenu fleksibilnost omogućuje skup mišića koji je čine. Šarenica se sastoji od pjega, prstena i brazdi u različitim bojama koje čine jedinstveni kompleks šara i boja svakog pojedinca. Oko 200 karakteristika koje su pogodne za identifikaciju definirano je na šarenici.

Sustav za identifikaciju koji se koristi šarenicom oka ne mogu korisnici prevariti staklenim okom, lećama ili okom koje je odstranjeno s mrtve osobe. U slučaju staklenog oka ili oka koje je odstranjeno s mrtve osobe neće doći do kontrakcije tj. širenja zjenice pri obasjavanju oka a za detekciju leća postoje algoritmi koji ih registriraju.

Pri ovoj tehnici nije potreban fizički kontakt korisnika sa skenerom već se snimanje šarenice oka može obaviti i s običnom kamerom na udaljenosti do pola metra. Ova tehnika identifikacije vrlo je pouzdana i jednostavna.



Slika 4. Identifikacija putem šarenice

Dostupno na : https://mobitrgovina.com/, Preuzeto: (14.03.2020)

Mrežnica oka je splet krvni žila, tanki sloj stanica koji se nalazi u stražnjem dijelu oka. Struktura mrežnice je jedinstvena, individualna karakteristika svake osobe. Identifikacija mrežnicom oka jedna je od najpouzdanijih metoda jer se unutarnja struktura oka ne mijenja tijekom života a nemoguće ju je replicirati ili promijeniti. Za vrijeme skeniranja, koje traje između 10 i 15 sekundi, oko će se osvijetliti blagom svjetlosti te se zbog toga ova metoda smatra jednom od neugodnijih biometrijskih metoda.

3.2.5. Potpis

Pisanje iziskuje puno vježbe i ispisanog teksta. Zbog toga osobe počinju razvijati poseban način pisanja slova, rečenica i riječi što se može koristiti kao biometrijska karakteristika pojedine osobe. Kod davanja izjava, potpisivanja ugovora ili plaćanja kreditnom karticom potreban je potpis kojim osoba garantira za napisane stavke u dokumentu te garantira da će pravno odgovarati ako dođe do nesuglasica.

Verifikacija se vrši tako da se identificira način na koji se osoba potpisuje. Jedinstvenost potpisa oblikuje:

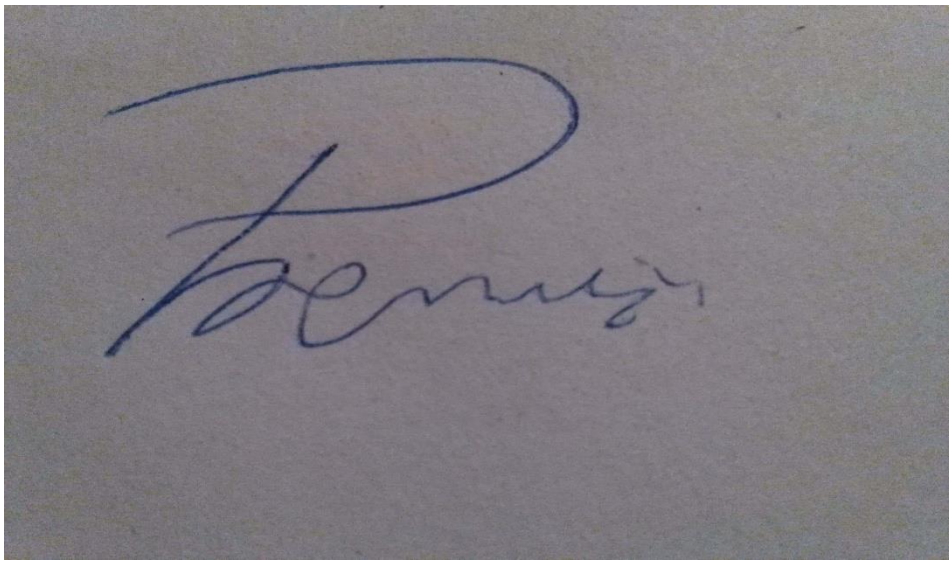
a) oblik slova

b) pritisak pisala

c) brzina pisanja

Dva su pristupa kod verifikacije potpisa: statički i dinamički. Oblik i geometrija potpisa uzimaju se kod statičke verifikacije dok se kod dinamičke verifikacije uzima u obzir brzina poteza, brzina pisanja i putanja profila potpisa.

Kada popis promatramo u kategoriji biometrijskih karakteristika tada se on analizira u sustavu tj. programskom algoritmu koji će provjeriti gore navedene atribute. U slučaju krivotvorenja potpisa, krivotvoritelj mora znati brzinu pisanja, putanju potpisa, oblik slova te tiskanje pisala.



Slika 5. Primjer vlastoručnog potpisa

Dostupno na : Divljak, https://divljak01.wordpress.com/, Preuzeto: (05.02.2020)

U radu nisu navedene sve biometrijske karakteristike u biometrijskoj verifikaciji. Naime, fokus je bio stavljen na one biometrijske karakteristike koje se najčešće koriste u komercijalne svrhe te one o kojima najviše ovisi sigurnost i privatnost korisnika.

3.3 Biometrija u sustavu nacionalne sigurnosti

Globalizacijom i razvojem tehnologije brišu se granice, povećava se mobilnost ljudi, protok kapitala i roba te druge gospodarske aktivnosti. Stvaraju se nove mogućnosti ali i novi rizici. Živimo u vremenima kada je razvoj tehnologije i prisutnost Interneta normalna pojava, pa ponekad nismo svjesni utjecaja istog. Povezanost infrastruktura prometnih, zdravstvenih, energentskih i drugih područja s informacijskim tehnologijama ima kao negativnu posljedicu otvaranje vrata novim oblicima kriminala. Razvojem tehnologije raste i potreba za sigurnosnim okruženjem, pouzdanim sustavima za osiguranje osoba i imovine. Identifikacija osobe je značajan čimbenik pri postizanju sigurnosti. Provjera identiteta pomoću zaporki, pinova, potpisa i slično polako zastarijeva te njeno mjesto preuzima biometrija kao sve češći i sigurniji oblik autentifikacije.

Zaključujući iz prethodnog dijela o biometrijskim karakteristikama, vidljivo je kako svaka od njih ima svoje prednosti i mane, te da ne postoji savršena metoda. Biometrija je samo jedan od alata koji se može koristiti pri identifikaciji. Sigurnost i distribucija podataka koji su pohranjeni biometrijskim metodama, njihovo čuvanje te pravo na pristup pitanja su na koja odgovor trebaju dati čelnici država unije.

Sigurnost i tehnologija prate se u korak. Nakon što napredak neke industrijske ili tehnološke grane dođe do kritične točke gdje razina sigurnosti padne tada se daljnji napori ulažu u povećanje razine pouzdanosti i sigurnosti.

Analizirajući sigurnost i nadzor informacijskih sustava te ulogu biometrije dolazimo do pojma informacijski sustav te informacijska sigurnost. Biometrija i informacijska sigurnost su usko povezani. Information System ili informacijski sustav definiramo kao strukturirani sustav u kojem su međusobno povezani hardveri, softveri, telekomunikacijske mreže, a ljudi ih grade i njima upravljaju u svrhu prikupljanja podataka, njihove pohrana, obrade i daljnje distribucije, te da isti budu dostupni ovlaštenim korisnicima.[12] Informacijska sigurnost postiže se propisanom sigurnosnom politikom koja obuhvaća niz mjera i metoda koje su implementirane u obliku tehničkih i organizacijskih kontrola u poslovne procese, određena državna tijela ili

[12] Marija Boban; Mirjana Perišić, Biometrija u sustavu sigurnosti , zaštite i nadzora informacijskih sustava, Pregledni rad, str. 116

pravne osobe. Ona je bitna za očuvanje anonimnosti podataka. Cjelovitost, povjerljivost i raspoloživost podataka uzimaju se kao definicija informacijske sigurnosti.

Područja informacijske sigurnosti:

a) sigurnosna provjera
   - utvrđuju se mjere i standardi koji će se primjenjivati na osobe koje imaju pristup klasificiranim podacima (vrlo tajno, tajno, povjerljivo i ograničeno) .

b) fizička sigurnost
   - utvrđuju se standardi i mjere za zaštitu objekata, uređaja i prostora gdje se nalaze klasificirani podaci.

c) sigurnost podataka
   - mjere i standardi koji će se primjenjivati u postupanju s klasificiranim i neklasificiranim podacima kao zaštitne mjere za prevenciju, otklanjanje i otkrivanje štete od gubitka ili neovlaštenog otkrivanja navedenih podataka

d) sigurnosna dokumentacija informacijskog sustava
   - obvezujući dokument kojim se definiraju mjere informacijske odgovornosti i sigurnosti unutar informacijskog sustava.

e) sigurnost poslovne suradnje
   - primjenjuju se za provedbu ugovora ili natječaja s klasificiranom dokumentacijom.

Razvojem tehnologije, posebno računalne klasične biometrijske metode doživljavaju punu afirmaciju.[13] Prepoznavanje određenih biometrijskih značajki te njihovo uspoređivanje s uzorkom koji je pohranjen u bazi podataka temelj su suvremene biometrijske identifikacije. Digitalizacija u tome ima ključnu ulogu kao najvažniji element pri procesu prepoznavanja. Da bi računalo obradilo podatke dobivene skeniranjem potrebno je prevesti ih u digitalni format.

[13] Marija Boban; Mirjana Perišić, Biometrija u sustavu sigurnosti , zaštite i nadzora informacijskih sustava, Pregledni rad, str. 125

U svibnju 2006. godine, na 15. Kongresu o informacijskoj tehnologiji, raspravljalo se o proširenju definicije sigurnosti kako bi se uspješno obuhvatili novi trendovi globalizacije. Industrijske vođe tada su isto tako zahtijevale više odgovornosti od poduzeća i vlada. Otvara se pitanje kako uspostaviti ravnotežu između novonastalih trendova i zaštite nacionalne sigurnosti, zaštite od terorizma, kriminala, ilegalnih migracija i slično.

Jedno od glavnih pitanja kod korištenja biometrije danas je kako osigurati pozitivnu identifikaciju roba i ljudi uz garanciju sigurnosti njihovih podataka, prava na privatnost, poštivanje ljudskih prava i sloboda i slično. Također, u obzir se moraju uzeti i čimbenici poput razvijenost pojedinih zemalja, različitost zakonske regulative, etničke, vjerske te kulturološke razlike kako bi se postigla sigurnost. Pred vladama zemalja stoji veliki zadatak i odgovornost u osiguranju nacionalne sigurnosti. Poput infrastruktura željeznice, energetskog sustava i slično isto tako i informatička infrastruktura postaje važna te od vitalnog značaja za nacionalnu sigurnost .

Vrlo je važno da pri izgradnji metoda identifikacije vlade zemalja ne krše kulture, etičke i društvene senzibilitete nacije ili religije svijeta.

3.4. Biometrija i zaštita privatnosti

Biometrijska verifikacija tj. identifikacija prvenstveno je namijenjena poboljšanju privatnosti i sigurnosti. Biometrijske tehnologije nude mogućnost ograničenog pristupa zaposlenicima koji rade s povjerljivim podacima. Npr., ograničen pristup određenim sobama ili laboratorijima u kojima se čuvaju povjerljivi podaci koji su dostupni samo nekolicini ljudi. U zadnjih nekoliko godina u poslovnim područjima biometrija je podigla razinu sigurnosti.

Biometrijski podaci ljudi su osjetljivi i osobni. Razvojem biometrije u porastu su i pitanja sigurnosti i privatnosti. Najčešći problemi vezani uz privatnost i sigurnost osoba jesu podvale. Osoba se u ovom slučaju predstavlja sustavu s krivotvorenim biometrijskim karakteristikama s namjerom oponašanja druge osobe. Nadalje, problemi nastaju u situacijama kada osobe pokušavajući promijeniti svoje biometrijske karakteristike nastoje prevariti sustav, navodeći ga na neprepoznavanje. Nezakonito korištenje biometrijskih karakteristika te uništavanje integriteta biometrijskog sustava također su problemi koji se mogu javiti u biometriji.

Javlja se sve veća potreba za dodatnom sigurnošću biometrijske tehnologije i pohranjenih podataka, zaštitom biometrijskih podataka od otuđenja ili korištenja u druge svrhe izvan namijenjenih. Povjerljivost, autentičnost, dostupnost i integritet sigurnosni su zahtjevi koji su potrebni kako bi bilo koji sustav mogao biti umrežen, isto tako i biometrijski.

Kontroliranje pristupa vlastitim informacijama te sposobnost vođenja života definiramo kao privatnost. Tri su glavna problema privatnosti kod biometrije:

a) biometrijske karakteristike su biološkog podrijetla

   - ovo otvara prostora ljudima koji prikupljaju biometrijske podatke da prikupljaju i neke dodatne osobne podatke. Npr., drugačiji oblik prsta može se statistički povezati s nekim genetskim poremećajem što kasnije može biti temelj za diskriminaciju.

b) neželjena identifikacija

   - metode, poput otiska prsta, su toliko jake da mogu omogućiti neželjenu identifikaciju. Npr. , ukoliko osoba ima tajno ime iz sigurnosnih razloga ona opet može biti identificirana na temelju svog otiska prsta.

c) biometrijske karakteristike nisu tajne

- obzirom da biometrijske karakteristike ljudi nisu tajne, često je moguće dobiti biometrijski uzorak osobe bez njenog znanja. Također, sustav ima kontrolu nad biometrijskim podacima, tj. podaci su dostupni samo ovlaštenim korisnicima, odnosno vlasnicima i administratorima.

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. Da 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.[14]

Kripto- biometrija, kao najpoznatija tehnika za zaštitu biometrijskih podataka, bazira se na ključevima koristeći kriptografske algoritme za šifriranje i dešifriranje. U šifriranoj domeni ključevi za biometriju mogu biti digitalni, što znači da će PIN, lozinke i alfanumeričke veze biti potvrđene samo ako je točan biometrijski uzorak, koji se 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[15]. Prednosti kripto-biometrije jesu: mogućnost korištenja anonimnih modela, veća usklađenost sa zakonima o privatnosti te manje zadržavanje pohranjenog predloška tj., biometrijske slike. S druge strane nedostaci bi bili: opasnost od povećanih napada na biometrijski predložak, opasnost od povećanih napada na komunikacijski kanal te nizak postotak točnosti za algoritme koje koristi.

[14] Mihaela Konjevod, Biometrija i zaštita privatnosti, završni rad, Osijek 2016. godine, str.9

[15] Ibidem

4.GDPR I VIDEONADZOR

25. svibnja 2018. godine s primjenom je počela Opća uredba o zaštiti osobnih podataka, odnosno GDPR koja propisuje nove načine postupanja s osobnim podacima. Ovaj datum smatra se prekretnicom u svim automatiziranim obradama podataka koji su imali mogućnost identifikacije pojedinca svojim algoritmima.

Primjenom GDPR-a sve europske Institucije i tvrtke koje se u svojim poslovima dotiču obrade osobnih podataka te tvrtke koje pružaju proizvode i usluge vezane uz obradu osobnih podataka, procesno i dokumentacijski moraju biti usklađene s odredbama GDPR-a.

Svrha ove Uredbe je jačanje prava u upravljanju i kontroli pojedinca nad njegovim osobnim podacima te zaštita privatnosti.

Uredba kaže kako je definicija osobnog podatka svaki podatak koji se odnosi na pojedinca čiji se identitet može utvrditi ili je utvrđen. To su npr. : ime, OIB, fotografija, adresa, e-mail adresa, telefonski broj, video snimke pojedinca, GPS lokacija, IP i MAC adresa, biometrijski podaci, kolačići na web stranicama, podaci o obrazovanju i stručnoj spremi, podaci o kreditnom zaduženju, podaci o plaći, genetski podaci, podaci o zdravlju, podaci o računima u banci te bilo koji drugi podaci na temelju kojeg se može utvrditi identitet pojedinca.

Pojedinci odnosno ispitanici temeljem GDPR-a imaju sljedeća prava:

a) pravo na pristup osobnim podacima i pravo na informiranje o obradi podataka

   - Transparentnost; voditelj obrade podataka je dužan jasno i jednostavnim rječnikom informirati ispitanika o načinu obrade njegovih osobnih podataka.

b) pravo na brisanje podataka

   - koristeći pravo na zaborav ispitanik ima pravo tražiti brisanje svojih osobnih podataka a voditelj obrade ima obavezu, bez nepotrebnog odgađanja, obrisati te podatke.

c) pravo na ispravak

   - ispitanik ima pravo od voditelja obrade tražiti ispravak netočnih podataka ili dopunu nepotpunih osobnih podataka.

d) pravo na ograničenje obrade

- u slučaju kada je obrada ograničena, ti se podaci smiju koristiti samo uz privolu ispitanika.

e) pravo na prigovor

- voditelj obrade podataka mora jasno predočiti ispitaniku kako ima pravo na prigovor te mu omogućiti mogućnost podnošenja istog.
- ispitanik prigovor može priložiti u bilo kojem trenutku a voditelj obrade osobnih podataka mora prestati s korištenjem spornih podataka. Iznimka je slučaj kada voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za nastavak korištenja istih.

f) pravo na prenosivost podataka

- ispitanik ima pravo zaprimiti svoje osobne podatke od voditelja obrade osobnih podataka te ih neometano prenijeti drugom voditelju obrade osobnih podataka.

g) pravo na izuzeće pravnih odluka prilikom automatskog donošena odluka i profiliranja

- ispitanik ima pravo tražiti da se na njega ne odnose odluke koje se temelje isključivo na automatiziranoj obradi (uključujući izradu profila) a koje proizvode pravne učinke koji utječu na njega.

Kako bi do obrade osobnih podataka uopće moglo doći ispitanik mora potpisati privolu. Privola je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.[16] Adekvatna privola mora biti neuvjetovana, partikularna, nedvosmislena, komunicirana jednostavnim jezikom i informirana.

Obaveze voditelja obrade osobnih podataka:

[16] Apicurabi Business Intelligence, Dostupno na: https://apicura.hr/, Preuzeto: (01.03.2020)

- Na temelju načela transparentnosti, koje kaže kako se osobni podaci moraju obrađivati zakonito, pošteno i transparentno, voditelj obrade ispitaniku je dužan precizno objasniti što i kako radi s njegovim osobnim podacima,

- Podaci koji su prikupljani u posebne, zakonske svrhe dalje se ne smiju obrađivati u druge svrhe, npr. profiliranje ispitanika,

- Obrada podataka mora biti primjerena, relevantna i ograničena na ono nužno u odnosu na svrhu zbog koje se obrađuju podaci. To bi značilo kako poduzeća ili kompanije ne smiju prikupljati podatke po principu "za svaki slučaj" te voditelj obrade osobnih podataka obradu mora ograničiti samo na prikupljanje onih podataka koji su mu potrebni za prvotnu svrhu. Također, voditelj obrade mora u svakom trenutku biti u mogućnosti jasno opravdati svrhu prikupljanja podataka te razlog njihove pohrane i korištenja,

- Podaci moraju biti točni i ažurni,

- Podaci se čuvaju u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno da bi se podaci mogli obraditi. Izuzetak je situacija kada se osobni podaci obrađuju u svrhe arhiviranja u javnom interesu, statističke svrhe, svrhe znanstvenog ili povijesnog istraživanja,

- Podaci uzeti za obradu moraju se obrađivati na način kojim se osigurava odgovarajuća sigurnost osobnih podataka uključujući zaštitu od nezakonite ili neovlaštene obrade, zaštitu od slučajnog gubitka, zaštitu od uništenja ili oštećenja primjenom određenih tehničkih ili organizacijskih mjera.

Videonadzor je jedan od učestalih načina prikupljanja, obrade i arhiviranja osobnih podataka.[17] European Data Protection Bord – EDPB tj., Europski odbor za zaštitu podataka u srpnju 2019. godine objavio je Smjernice o obradi osobnih podataka putem video uređaja čija je svrha pojasniti način primjene GDPR-a u odnosu obrade . U njima navodi kako videonadzor nije nužno neophodan ukoliko se zaštita ljudi ili imovine može na neki drugi način osigurati.

[17] Lider media, Dostupno na: https://lider.media/, Preuzeto sa: (01.03.2020)

Uz GDPR i zakon o njegovoj provedbi, obrada i prikupljanje osobnih podataka dodatno su regulirani provedbenim propisima dviju direktiva koje su povezane:

a) tzv. policijska direktiva

   - o zaštiti pojedinaca u slučajevima obrade osobnih podataka od strane nadležnih tijela u različite svrhe : sprječavanje istrage, otkrivanja kaznenog djela, progon kaznenog djela, izvršavanje kaznenih sankcija te o slobodnom kretanju ovakvih podataka.

b) direktiva o upotrebi podataka u zračnom prometu

   - ova direktiva se koristi u svrhu otkrivanja teških kaznenih djela i terorizma.

GDPR i njegove odredbe ne odnose se na obradu osobnih podataka koju provode fizičke osobe tijekom kućnih ili osobnih aktivnosti. Ukoliko se ne radi isključivo o obradi osobnih podataka tijekom kućnih ili osobnih aktivnosti tada je voditelj obrade podataka, koji provodi obradu osobnih putem videonadzora, dužan držati se svih zahtjeva propisanih GDPR-om.

Tijelima javne vlasti, pravnim osobama koje obavljaju pravnu službu i pravnim osobama s javnim ovlastima zakonom je dozvoljeno pokrivanje javnih površina videonadzorom, ukoliko im je to nužno za izvršenje zadaća i poslova javne vlasti ili radi zaštite života i zdravlja ljudi, tj. imovine. (Čl. 32. Zakon o provedbi Opće Uredbe o zaštiti podataka (NN 42/2018))

5.RAZVOJ SUSTAVA VIDEONADZORA

Sustavi za videonadzor danas su vrlo popularni u svijetu te imaju široku primjenu (kod kuće, na radnom mjestu, u javnim ustanovama itd.). Svrha sustava videonadzora je dostizanje visokog stupanja sigurnosti. Napredak tehnologije i masovna proizvodnja sa sobom donose osjećaj nesigurnosti kod javnosti te sve veće zanimanje za sustav videonadzora. Danas je npr. zakonom određeno osiguranje mjenjačnica, banaka i kockarnica uz pomoć sustava videonadzora.

Povijesno gledajući, 1980. godine pojavljuju se prve kamere za snimanje filmova. Thomas Edison i William Dickson udružili su snage i snimili film.

Minijaturna prijenosna kamera pojavljuje se 1939.godine. Ona je radila na navijanje te ju je bilo moguće držati jednom rukom. Novost koje su ove kamere donijele bila je ta da su se po prvi puta u povijesti kamere mogle koristiti bez nadzora nakon što bi se postavile da snimaju.

1942. godine u Njemačkoj zabilježen je prvi slučaj gdje su se kamare koristile za prenošenje video signala, takozvani CCTV videonadzor. Ovi sustavi video nazora uglavnom su koncipirani tako da su nadzorne video kamere razmještene na ključnim mjestima u i oko objekta koji se štiti sustavom video nadzora.. Sve video nadzorne kamere jednoga sustava videonadzora povezuju se u jednu cjelinu putem centralnog uređaja te takva cjelina tvori jedinstven sustav video nadzora ili CCTV (eng. Close Circuit TeleVision). [18]

Prve video kazete izumljene su 1951. godine koje se u kombinaciji s CCTV-om koristi za snimanje materijala koje se kasnije može i pregledati.

Razvojem tehnologije 1960. dolazi do pojave prvih javnih kamera. One su bile osmišljene zbog osiguranja zaštite i sigurnosti povodom posjeta tajlandske kraljevske obitelji u London.

1969. Marie Van Brittan Brown dobiva patent za svoj izum, prvi sustav za videonadzor. Ovaj se sustav sastojao od četiri rupe za cijevi te kamere koja se mogla premještati na te rupe. Kamera je na monitor emitirala sliku. Nakon ovoga banke počinju primjenjivati sustav videonadzora kao mjeru zaštite od krađa.

[18] Videonadzorni sustavi, Dostupno na: https://www.007.hr/videonadzorni-sustavi-videonadzor-cctv/, Preuzeto sa: (13.03.2020)

1976. godine Charge-Coupled Device (CCD) tehnologija dovodi do stvaranja kamera koje se mogu koristiti u slabim svjetlosnim uvjetima. Te kamere prilikom rada koriste mikročipove.[19]

Nakon 1993. i povećanjem svijesti o terorističkim napadima uporaba videonadzora rapidno se širi. Države počinju koristiti sustav videonadzora za praćenje raznih sportskih te sličnih događaja koji bi mogli postati meta teroristima.

1996. godine je proizvedena prva vrsta kamere koja prima i šalje podatke preko računalne mreže, IP kamera. One su potakle razvoj današnjih web kamera.

Nakon 2001. godine i terorističkog napada na Blizance, javnost je sve više zabrinuta za svoju sigurnost. To je rezultiralo izumom kamera s visokom rezolucijom slike, na kojoj se može prepoznati lice. Tehnološki i digitalni napredak postaju prioritet svugdje u svijetu.

[19] Videonadzorni sustavi, Dostupno na: https://www.007.hr/videonadzorni-sustavi-videonadzor-cctv/, Preuzeto sa: (14.03.2020)

6. UČINKOVITOST VIDEONADZORA U SMANJENJU KRIMINALITETA

Britanski filozof Jeremy Bentham (1746.-1832.) u 18. stoljeću osmislio je penalnu instituciju koja je čuvarima u središnjem tornju zatvora omogućavala promatranje zatvorenika bez mogućnosti da oni saznaju tko ih i kada nadzire. Od tu proizlazi zamisao o „sve promatrajućem“ mehanizmu.

Koncept nadzora građana i trend politike suzbijanja kriminaliteta polazi od generalne pretpostavke kako će se ljudi ponašati društveno poželjno i poštenije ako znaju da ih netko promatra. Širenje tehnologije sveprisutnog nadzora osigurava se postupnim, neinvazivnim psihološkim pripremama i osvještavanjem građana najčešće medijskim putem i to promicanjem važnih društvenih pravila i sustava poželjnog, odnosno prihvatljivog ponašanja. U tom smislu potrebno je uvjeriti ljude da nadzor služi ostvarivanju njihove slobode, sigurnosti i, konačno, njihove egzistencije ("sloboda u zamjenu za sigurnost")[20]

Sustav videonadzora koristi se za nadgledavanje javnih prostora poput prometa i prometnih čvorova, graničnih prijelaza, pješačkih zona, središta gradova, kvartova, parkirališta, parkova i slično.

Kada govorimo o učinkovitosti videonadzora u smanjenju kriminaliteta, glavna svrha videonadzora je odvratiti potencijalnog počinitelja od činjenja neke kažnjive radnje pod uvjetom da je potencijalni počinitelj svjestan postojanja videonadzora nad određenim prostorom.

Naravno, činjenica da potencijalni počinitelj zna kako je neki prostor pod videonadzorom nije garancija kako on neće počiniti neku kažnjivu radnju. Sustav videonadzora ne predstavlja fizičku barijeru ali je od iznimne koristi za situacijsku prevenciju kriminaliteta. Prednost videonadzora je u tome što on može biti okidač perceptivnog mehanizma potencijalnog počinitelja koji je usmjeren na njegovu svijest o tome kako može biti uhićen odluči li se za kažnjivu radnju. Ovdje se radi o psihološkom procesu koji se događa kod potencijalnog počinitelja a da bi do njega došlo potrebno je da počinitelj ima saznanja o tome kako je pod

[20] Ksenija Butorac, Irena Cajner Mraović, Hrvoje Filipović: Učinkovitost video nadzora u smanjenju kriminaliteta – pregled istraživanja, Zbornik radova; str. 84

videonadzorom te mora vjerovati da mu postavljene kamere predstavljaju stvarni rizik od uhićenja.

Sustavi videonadzora, s obzirom na ljudski faktor koji je uključen u njega, mogu biti:

a) aktivni – zaposlenik prati i analizira snimke u realnom vremenu,

b) pasivni - pretraživanje snimaka post festum, odnosno nakon nekog događaja.

Hibridni sustavi videonadzora najčešće su u praksi. Koriste se skrivene i vidljive kamere koje se postavljaju u kupole ili zaštitne školjke. U ovakvim situacijama neizostavan je rad operatera koji je najčešće zaštitar ili policijski službenik. On nadzire stanje u prostoru, pregledava snimke, reagira na uočene informacije te o tome obavještava policiju, priprema videozapis (na kojem je zabilježen prekršaj ili kazneno djelo) kao dokaz za sud.

Prednosti videonadzora jesu višedimenzionalne:

- smanjenje straha od kriminaliteta u lokalnoj zajednici; građani se osjećaju sigurnije znajući da je prostor pod videonadzorom,
- pružanje hitne medicinske skrbi; u situaciji kada dođe do ozljeda proizašlih iz kaznenih djela ili u situacijama iznenadnih bolesnih stanja građana koja se događaju na javnim mjestima pokrivenim videonadzorom, operateri će žurno obavijestiti policiju i hitnu medicinsku pomoć,
- upravljanje mjestom događaja; npr. u slučajevima nestanka djece, javnog okupljanja ili prosvjeda,
- prikupljanje informacija; isto tako videonadzorom se nadgleda ponašanje počinitelja koji su od prije poznati (npr. krađa u trgovini) ,
- mogućnost zahvaćanja šireg područja javne površine od zadane, u dosegu kojeg delinkvent nije svjestan.

Nedostatci videonadzora, odnosno neželjene posljedice videonadzora jesu:

- Premještanje kriminaliteta; nerijetko se događa da se umjesto očekivanog smanjenja kriminaliteta, on premjesti u druge dijelove grada za koje potencijalni

počinitelj zna da nisu pod sustavom videonadzora. Doduše, ako do ove posljedice i dođe, riječ je o vrlo malom udjelu,

- negativna reakcija javnosti; kod određenih skupina ljudi često vlada mišljenje kako je videonadzor namijenjen „špijuniranju“ ljudi te to kod njih izaziva strah i nepovjerenje,

- povećan broj kaznenih prijava; sustavom videonadzora povećava se otkrivanje nasilničkog ponašanja, npr. preprodaja droga, grafiti i slično. Potrebno je napomenuti da ovdje nije riječ o stvarnom kriminalitetu, nego isključivo o registriranom (snimljenom) kriminalitetu. U svakom slučaju kamere omogućuju sekundarnu prevenciju kriminaliteta koja vodi u smanjivanje tamne brojke kriminaliteta.[21]

[21] Ksenija Butorac, Irena Cajner Mraović, Hrvoje Filipović: Učinkovitost video nadzora u smanjenju kriminaliteta – pregled istraživanja, Zbornik radova; str. 89

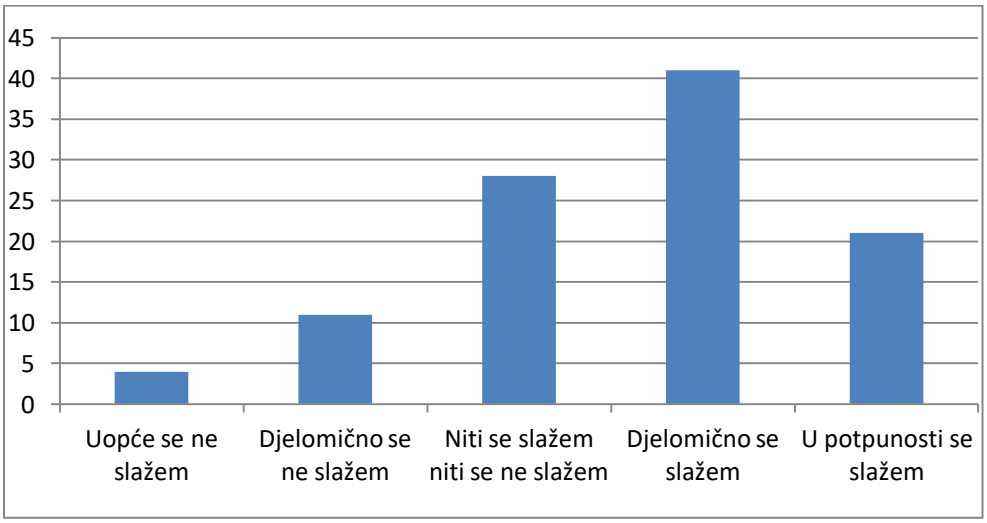
7. ISTRAŽIVANJE O PRIMJENI NOVIH TEHNOLOGIJA U SIGURNOSTI RH

Provedena je online anketa od 10 pitanja na uzorku od 106 ispitanika svih dobi kako bi se dobio uvid u stavove ljudi o videonadzoru, biometriji, korištenju biometrijskih podataka i njihovoj distribuciji te korištenju biometrijskih podataka pri pristupu aplikacijama.

Odgovori su rangirani na način od 1-5 pri čemu je:

1. Uopće se ne slažem
2. Djelomično se ne slažem
3. Niti se slažem niti se ne slažem
4. Djelomično se slažem
5. U potpunosti se slažem

Na pitanje broj jedan „Smatram da se razvojem biometrije i njenom implementacijom u različite sfere ljudskog života podiže i razina opće sigurnosti i zaštite osobnih podataka“ dobiveni su sljedeći rezultati: 4 ispitanika se uopće ne slaže sa navedenom tvrdnjom (4%) , 11 njih se djelomično ne slaže (10 %) , 28 se niti slaže niti ne slaže (27%) , 41 se djelomično slaže (39 %) te se njih 21 u potpunosti slaže (20%).

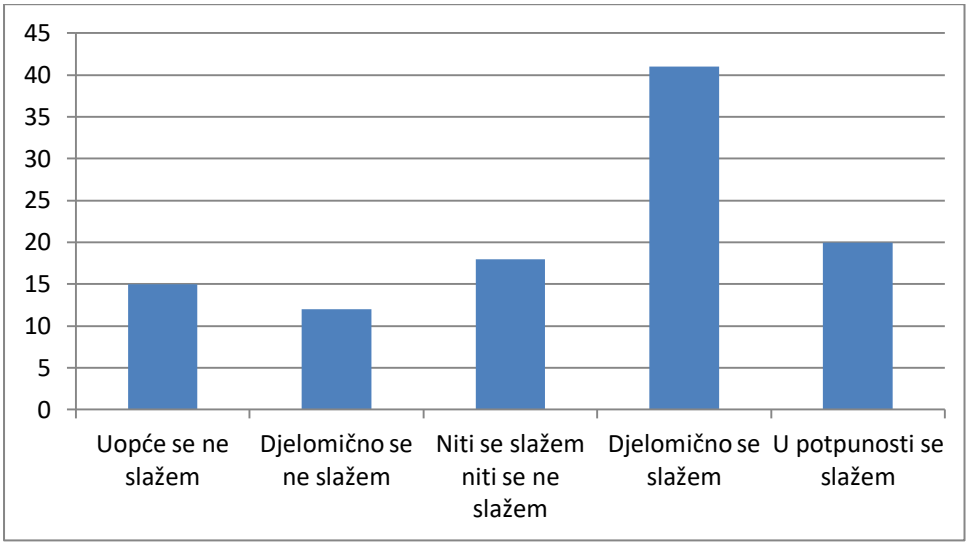


Slika 6. Rezultati online ankete na pitanje „Smatram da se razvojem biometrije i njenom implementacijom u različite sfere ljudskog života podiže i razina opće sigurnosti i zaštite

osobnih podataka.“

Svrha postavljenog pitanja bila je dobiti uvid kakav stav ljudi imaju prema biometriji općenito. Većina ispitanika se djelomično ili u potpunosti slaže kako im biometrija svojim razvojem paralelno osigurava i sigurnost te privatnost osobnih podataka. Obzirom na tehnološki razvoj i zastupljenost upotrebe biometrije u gotovo svim sferama ljudskog života, bilo je za očekivati ovakav postotak.

Pitanje broj dva glasilo je „Osjećam se sigurnije ukoliko znam da je prostor u kojem se nalazim pri obavljanju određenih radnji pokriven videonadzorom“. Rezultati su sljedeći: 15 ispitanika se uopće ne slaže (14%), 12 se djelomično ne slaže (11%) , 18 njih niti se slaže niti se ne slaže (17%) , 41 ispitanik se djelomično slaže (39%) te se 20 ispitanika u potpunosti slaže (19 %).

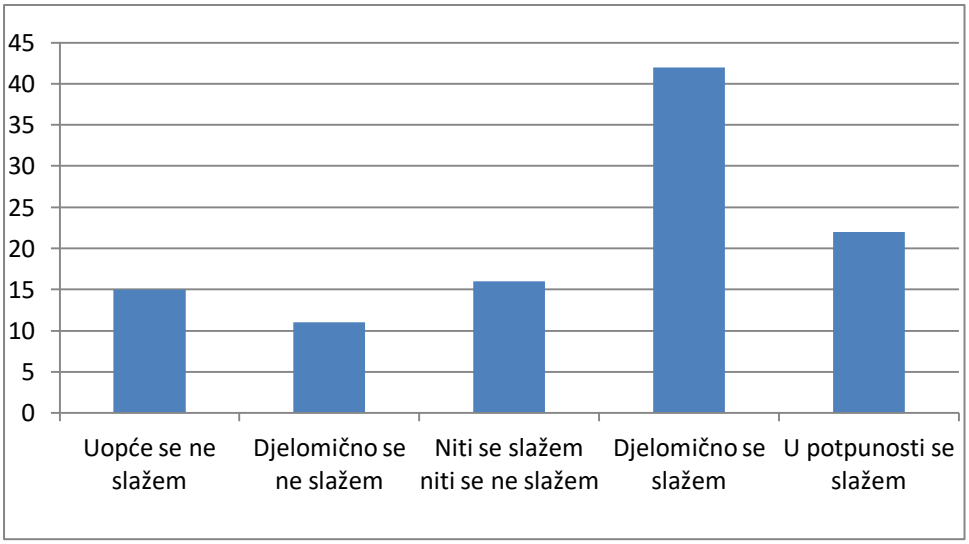


Slika 7. Rezultati online ankete na pitanje „Osjećam se sigurnije ukoliko znam da je prostor u kojem se nalazim pri obavljanju određenih radnji pokriven videonadzorom“

Sustavi za videonadzor danas su vrlo popularni u svijetu te imaju široku primjenu (kod kuće, na radnom mjestu, u javnim ustanovama itd.). Njegova glavna svrha je dostizanje visokog stupanja sigurnosti. Naravno, nerjetki su slučajevi negativnog stava ljudi prema sustavu videonadzora gdje ljudi misle kako ih se „špijunira“ i slično. Dobiveni rezultati upućuju nas

na to kako se ipak velika većina ispitanika (39 %) osjeća sigurnije ukoliko se nalazi u prostoru koji je pokriven sustavom videonadzora. Međutim, iz ankete je vidljivo kako ima i određeni postotak ispitanika koji se uopće ne slažu sa tvrdnjom (14%) ili onih koji se djelomično ne slažu sa navedenim (11%).

Pitanje broj tri bilo je: „ Ukoliko bi sve javne površine grada u kojem živim bile pokrivene sustavom videonadzora osjećao/la bi se sigurnije“. Dobiveni rezultati su: 15 ispitanika se uopće ne slaže (14%), 11 se djelomično ne slaže (10%), 16 se niti slaže niti ne slaže (15%), 42 se djelomično slaže (40 %) te 22 se u potpunosti slaže (21%)

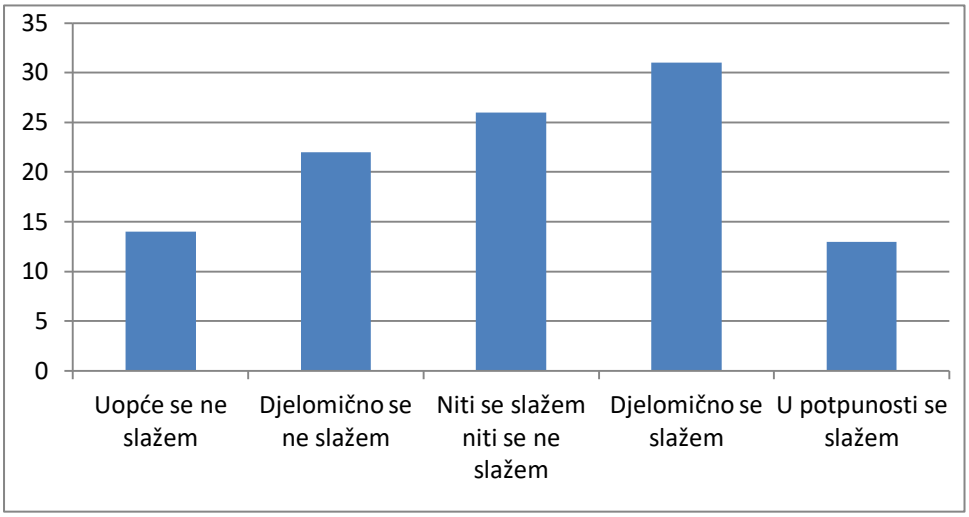


Slika 8. Rezultati online ankete na pitanje „Ukoliko bi sve javne površine grada u kojem živim bile pokrivene sustavom videonadzora osjećao/la bi se sigurnije“

Trećim pitanjem nadovezali smo se na drugo kako bi dobili jasniju sliku stava ljudi o videonadzoru koji je u ovom slučaju proširen na veću površinu. Slično kao i u pitanju pod brojem 2, većina ispitanika se djelomično (40 %) ili u potpunosti slaže (21 %) kako bi se osjećao/la sigurnije ukoliko bi sve javne površine grada u kojem žive bile pokrivene kamerama. Dobivenom postotku jednim djelom možemo pripisati i strah ljudi od novih nacionalnih prijetnji, npr terorizam.

Pod rednim brojem četiri bilo je pitanje: „Smatram kako razvoj biometrije pridonosi boljitku kvalitete ljudskog života te kako on ne ugrožava privatnost i sigurnost ljudi“. Dobiveni

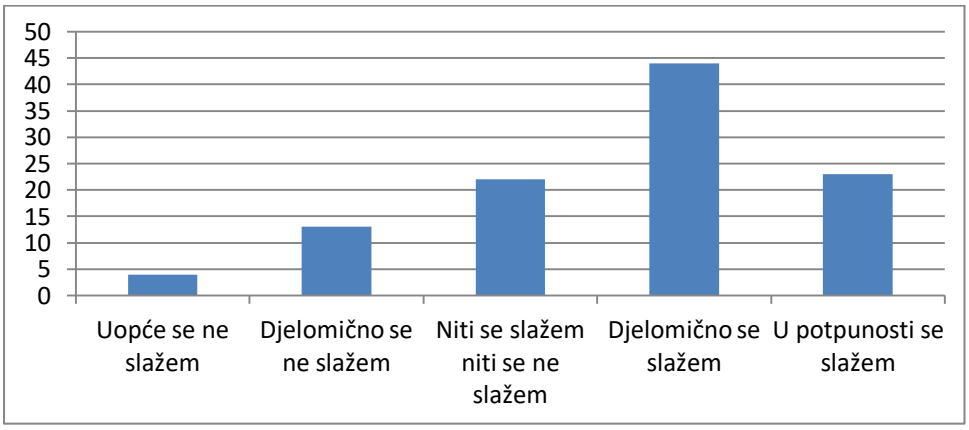
rezultati su: 15 se uopće ne slaže (14%), 22 se djelomično ne slaže (21%), 26 se niti slaže niti ne slaže (24%), 31 se djelomično slaže (29%) i 13 se u potpunosti slaže (12 %).



Slika 9. Rezultati online ankete na pitanje: „Smatram kako razvoj biometrije pridonosi boljitku kvalitete ljudskog života te kako on ne ugrožava privatnost i sigurnost ljudi“

Unatoč postotku koji se niti slaže niti ne slaže sa navedenom tvrdnjom (24%) te relativno malom postotku (12%) koji se u potpunosti slaže sa navedenim, dolazimo do zaključka kako je biometrija danas vrlo popularna te opće prihvatljiva metoda verifikacije korisnika.

Pitanje broj pet „Uspoređujući biometriju sa tradicionalnim metodama verifikacije korisnika (pinovi, lozinke..) smatram kako je biometrija jednostavniji i sigurniji način verifikacije“ rezultiralo je sljedećim: 5 se uopće ne slaže (5%), 13 se djelomično ne slaže (12%), 22 se niti slaže niti ne slaže (21%), 44 se djelomično slaže (41%) te 23 se u potpunosti slaže (21%).

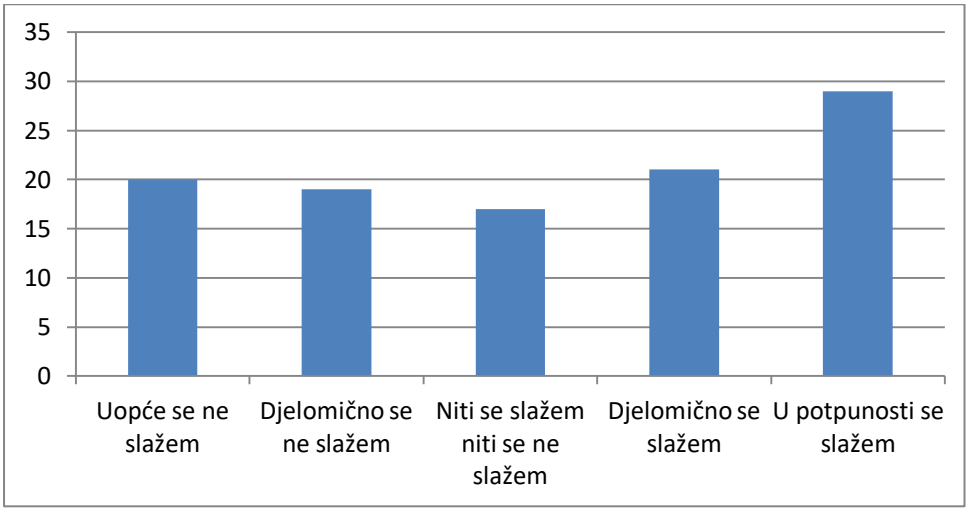


Slika 10. Rezultati online ankete na pitanje „Uspoređujući biometriju sa tradicionalnim metodama verifikacije korisnika (pinovi, lozinke..) smatram kako je biometrija jednostavniji i

sigurniji način verifikacije“

Tehnološkim razvojem i zamjenom tradicionalnih metoda verifikacije korisnika, većina ispitanika (41%) slaže se sa tvrdnjom kako je biometrija jednostavnija i sigurnija za korištenje. Kako se biometrija temelji na identificiranju ponašanja i bioloških karakteristika pojedine osobe, kao što su otisci prstiju, glas, hod, lice, šarenica oka i sl., teža je za napasti a razina sigurnosti u biometrijskom sustavu je za sve ista.

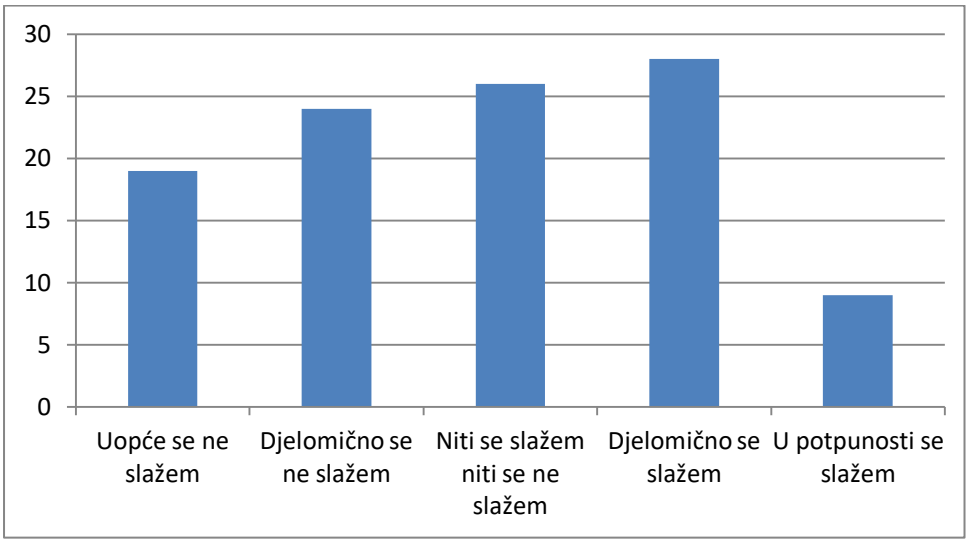
Šesto pitanje „Bez problema pristajem na korištenje biometrije kod pristupa vlastitom mobilnom uređaju“ rezultiralo je: 21 se uopće ne slaže (19%), 19 se djelomično ne slaže (18%), 17 se niti slaže niti ne slaže (16%), 21 se djelomično slaže (20%) a 29 se u potpunosti slaže (27%).



Slika 11. Rezultati online ankete na pitanje „Bez problema pristajem na korištenje biometrije kod pristupa vlastitom mobilnom uređaju“

Odnos postotka ispitanika koji se uopće ne slažu sa navedenim (19 %) i onih koji se u potpunosti slažu (27 %) diskutabilan je. Riječ je o relativno maloj razlici koja nam ukazuje kako ne pristaju baš svi bez razmišljanja na navedeni način pristupa vlastitom mobilnom uređaju.

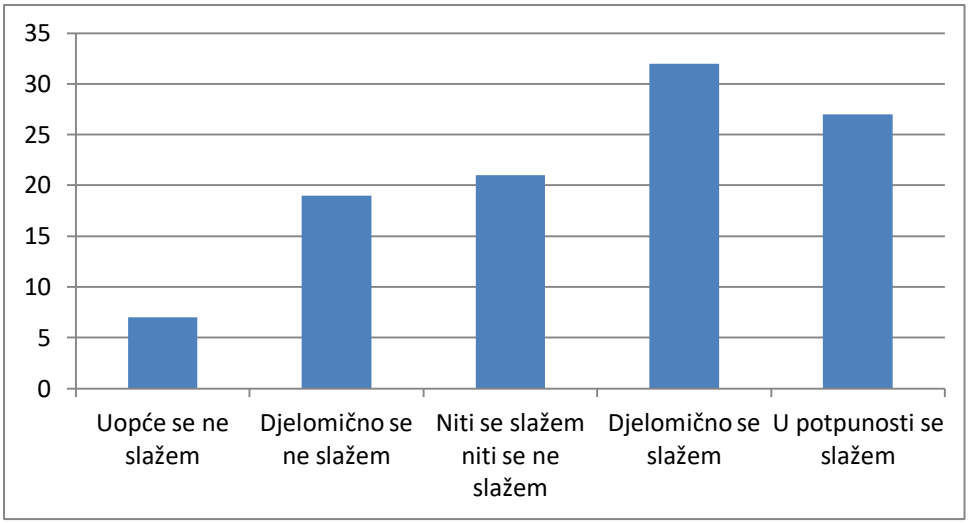
Pitanje broj 7 „Nemam strah ni sumnje u činjenicu da se moji biometrijski podaci, ukoliko se koristim njima kako bi pristupio/la npr. mobitelu, zloupotrebljavaju u druge svrhe“ dalo nam je uvid u rezultate: 20 se uopće ne slaže (19%), 24 se djelomično ne slaže (22%), 26 se niti slaže niti ne slaže (25%), 28 se djelomično slaže (26%) i 9 se u potpunosti slaže (8%).



Slika 12. Rezultati online ankete na pitanje „Nemam strah ni sumnje u činjenicu da se moji biometrijski podaci, ukoliko se koristim njima kako bi pristupio/la npr. mobitelu, zloupotrebljavaju u druge svrhe“

Dobiveni rezultati ukazuju nam kako ipak postoji određeni postotak sumnje u zloupotrebu biometrijskih podataka. S druge strane, 26% ispitanika nema sumnje u zloupotrebu istih što se jednim djelom može povezati sa rastućim trendom uređaja sa senzorima za biometrijsku verifikaciju.

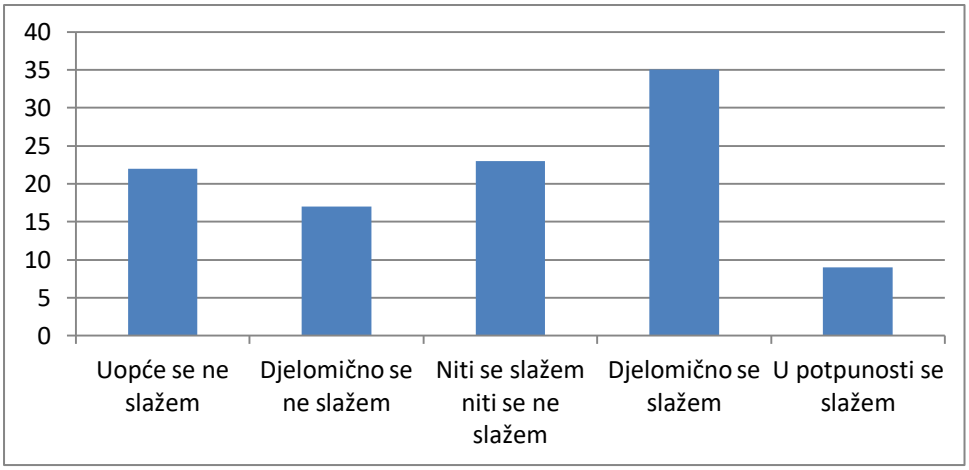
Osmo pitanje bilo je „Razumijem na koji način funkcionira spremanje biometrijskih podataka ukoliko koristim otisak prsta za otključavanje vlastitog mobitela“ dalo nam je sljedeće rezultate: 7 se uopće ne slaže (7%), 19 se djelomično ne slaže ((18%), 22 se niti slaže niti ne slaže (20%), 32 se djelomično slaže (30%) i 27 se u potpunosti slaže (25%).



Slika 13. Rezultati online ankete na pitanje „Razumijem na koji način funkcionira spremanje biometrijskih podataka ukoliko koristim otisak prsta za otključavanje vlastitog mobitela“

30 % ispitanika razumije na koji način funkcionira spremanje biometrijskih podataka ukoliko otiskom prsta otključavaju mobitel. Dakle, većina njih razumije kako se vrši verifikacija korisnika, odnosno kako se biometrijska karakteristika otiska prsta transformira u matematičku, kriptiranu reprezentaciju. Važno je napomenuti kako postoji i postotak ispitanika (7%) koji ne znaju na koji način funkcionira opisani postupak.

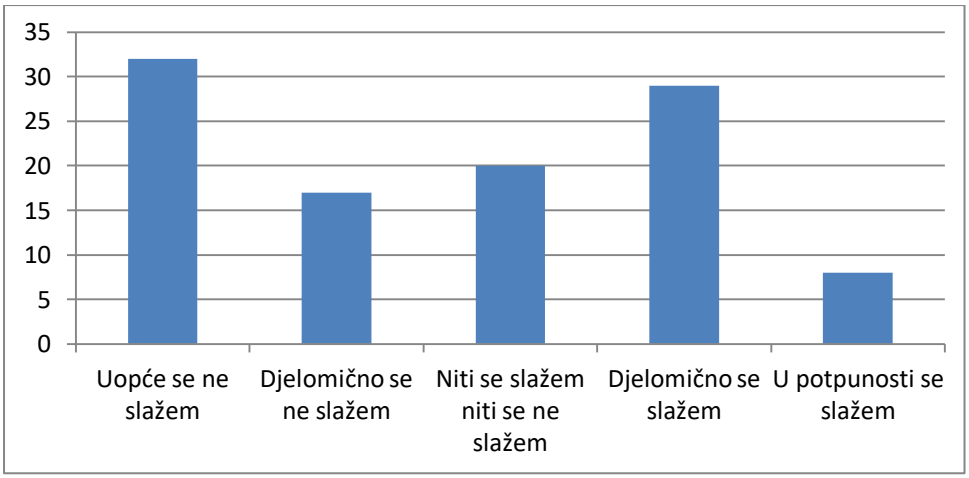
Pod brojem devet pitanje je glasilo: Ukoliko znam da je prostor u kojem se nalazim pokriven sustavom videonadzora i samim time ugrožava moju privatnost ali mi se time jamči sigurnost, pristao/ la bih. Sigurnost u zamjenu za privatnost. Slažete li se?“. 23 se uopće ne slaže (21 %), 17 se djelomično slaže (16%), 23 se niti slaže niti ne slaže (21%), 35 se djelomično slaže (33 %) te se 9 u potpunosti slaže (8%).



Slika 14. Rezultati online ankete na pitanje „Ukoliko znam da je prostor u kojem se nalazim pokriven sustavom videonadzora i samim time ugrožava moju privatnost ali mi se time jamči sigurnost, pristao/ la bih. Sigurnost u zamjenu za privatnost. Slažete li se?“

Iako se u današnje vrijeme redovito stavlja naglasak na privatnost i zaštitu osobnih podataka, većina ispitanika, točnije 33 %, žrtvovalo bi privatnost u zamjenu za sigurnost.

Zadnje, deseto pitanje glasilo je: „Smatram kako je prepoznavanje lica, odnosno biometrija lica u komercijalne svrhe u redu. Npr. slučaj društvene mreže Facebook“. Rezultati koje smo dobili jesu: 33 se uopće ne slažu (31%), 17 se djelomično ne slaže (16%), 20 se niti slaže niti ne slaže (19%), 29 se djelomično slaže (27 %) i 8 njih se u potpunosti slaže (7%).



Slika 15. Rezultati online ankete na pitanje: „Smatram kako je prepoznavanje lica, odnosno biometrija lica u komercijalne svrhe u redu. Npr. slučaj društvene mreže Facebook“

Velik dio ispitanika (31%) ne slaže se sa korištenjem biometrije prepoznavanja lica u komercijalne svrhe.

8.ZAKLJUČAK

Nacionalni interesi određuju se unutar svake države Strategijom nacionalne sigurnosti. Nacionalna sigurnost je pojam koji se odnosi na djelatnost koja je potrebna kako bi se ostvarili nacionalni interesi. Republika Hrvatska zadnju promjenu svoje Strategije nacionalne sigurnosti imala je u srpnju 2017. godine. Nova strategija objavljena je u Narodnim novinama 26.srpnja 2017.godine. (NN73/2017).

Razvojem tehnologije raste i potreba za sigurnosnim okruženjem, pouzdanim sustavima za osiguranje osoba i imovine. Identifikacija osobe je značajan čimbenik pri postizanju sigurnosti. Provjera identiteta pomoću zaporki, pinova, potpisa i slično polako zastarijeva te njeno mjesto preuzima biometrija kao sve češći i sigurniji oblik autentifikacije.

Biometrija se može definirati kao model identifikacije osobe, baziran na fizičkim karakteristikama ili karakteristikama ponašanja, a odnosi se na nešto što osoba posjeduje ili što osoba zna kako bi izvršila osobnu identifikaciju (npr. otisci prstiju, glas, lice, hod, šarenica oka, geometrija šake itd.). U današnje vrijeme sve je veća primjena biometrije u novim uređajima i općenito (npr. slučaj evidencije zaposlenika u tvrtkama). Prema provedenoj anketi može se zaključiti kako korisnici, ukoliko moraju birati između biometrije i tradicionalnih metoda, radije biraju biometriju jer teže jednostavnijoj i lakšoj verifikaciji. Kako bi korisnik biometrije bio što sigurniji od napada ili krađe biometrijskih podataka Europska unije i njene članice postavljaju zakonske regulative u svrhu zaštite svojih građana.

Razvoj sustava videonadzora također se odražava na stanje nacionalne sigurnosti. Globalizacija, napredak tehnologije, masovna proizvodnja sa sobom nose osjećaj nesigurnosti kod građana te bude njihovo sve veće zanimanje za videonadzor.

Tehnološki i digitalni napredak nameću se kao prioritet svugdje u svijetu. Obzirom na realne prijetnje koje se dolaze zajedno sa razvojem i implmentacijom novih tehnologija u sustav nacionalne sigurnbosti (npr. hakiranje putem videokamera, razvijanje terorizma putem suvremenih tehnologija) smatram kako razvoj novih tehnologija ima blistavu budućnost ukoliko će se jednaki napori ulagati u razvoj iste paralelno sa razvojem stupnja sigurnosti.

9.SAŽETAK

Nove tehnologije u nacionalnoj sigurnosti

Nacionalna sigurnost je djelatnost koja je organizirana kako bi zaštitila nacionalne interese i mehanizme koji su potrebni da bi se nacionalni interesi ostvarili. Nacionalni interesi se određuju unutar svake države donošenjem Strategije nacionalne sigurnosti. Gledajući razvoj novih tehnologija i njihov utjecaj na stanje nacionalne sigurnosti dolazimo do pojma biometrije.

Biometrija se može definirati kao model identifikacije osobe, baziran na fizičkim karakteristikama ili karakteristikama ponašanja, a odnosi se na nešto što osoba posjeduje ili što osoba zna kako bi izvršila osobnu identifikaciju. Imamo dvije vrste biometrije: fizičku i biometriju ponašanja. Fizička biometrija je dio biometrije koja se bavi uzorkovanjem fizionomije ljudskoga tijela i njegovim jedinstvenim karakteristikama (čitanje DNK zapisa, skeniranje rožnice i šarenice, prepoznavanje lica, geometrija šake, provjera vena, otisak prsta). Biometrija ponašanja opisuje fizikalne karakteristike (kao kretanje u prostoru, glas, izgled…) čovječjeg tijela koje su dijelom jedinstvene za svaku osobu(glas, rukopis, dinamika tipkanja, dinamika hoda, dinamika mirisa). Danas gotovo da i ne postoji segment društva u kojem se ne pojavljuje biometrija.

Sustavi za videonadzor danas su vrlo popularni u svijetu te imaju široku primjenu (kod kuće, na radnom mjestu, u javnim ustanovama itd.). Svrha sustava videonadzora je dostizanje visokog stupanja sigurnosti. S druge strane, nerado se događa da sustav videonadzora kod ljudi budi strah i sumnju. GDPR-om je uređeno pod kojim uvjetima se smije koristiti isti. Sustav videonadzora koristi se za nadgledavanje javnih prostora poput prometa i prometnih čvorova, graničnih prijelaza, pješačkih zona, središta gradova, kvartova, parkirališta, parkova i slično.

Ključne riječi: nacionalna sigurnost, nacionalni interesi, biometrija, videonadzor, nove tehnologije

10.SUMMARY

New technologies in national security

National security is an activity organized to protect national interests and the mechanisms needed to achieve national interests. National interests are determined within each country by adopting a National Security Strategy. Looking at the development of new technologies and their impact on the state of national security, we come to the concept of biometrics.

Biometrics can be defined as a model of identification of a person, based on physical or behavioral characteristics, and refers to something that a person possesses or what a person knows in order to perform personal identification. There are two types of biometrics: physical and behavioral biometrics. Physical biometrics is a part of biometrics that deals with the sampling of the physiognomy of the human body and its unique characteristics (reading DNA records, scanning the cornea and iris, facial recognition, fist geometry, vein testing, fingerprint). Behavioral biometrics describes the physical characteristics (such as movement in space, voice, appearance and so on) of the human body that are partly unique to each person (voice, handwriting, typing dynamics, dynamic of walking, smell dynamics). Today, there is hardly any segment of society where biometrics do not occur.

Video surveillance systems are very popular in the world today and their usage is widely used (at home, in the workplace, in public institutions, etc.). The purpose of the video surveillance system is to achieve a high degree of security. On the other hand, video surveillance systems are reluctant to cause fear and doubt in people. The GDPR regulates under what conditions the same can be used. The video surveillance system is used to monitor public spaces such as traffic and traffic nodes, border crossings, pedestrian zones, city centers, neighborhoods, parking lots, parks and similar.

Keywords: national security, national interests, biometrics, video surveillance, new technologies

11.LITERATURA

1. Darko Lacković, Poteškoće u definiranju pojma nacionalne sigurnosti, Stručni rad,1.rujna 2000. godine, str. 197-206

2. Kristijan Pukšić i Marinko Žagar, Otpornost autentifikacije biometrijskom metodom otiska prsta na probijanje, 2016. godina , str. 361-362

3. Ksenija Butorac, Irena Cajner Mraović, Hrvoje Filipović: Učinkovitost video nadzora u smanjenju kriminaliteta – pregled istraživanja, Zbornik radova; str. 83- 97.

4. Marija Boban; Mirjana Perišić, Biometrija u sustavu sigurnosti , zaštite i nadzora informacijskih sustava, Pregledni rad, str. 115-148.

5. Marijana Musladin, Utjecaj društvenih mreža na nacionalnu sigurnost, Pregledni rad, 05.svibnja 2012.godine, str. 67-85

6. Mihaela Konjevod, Biometrija i zaštita privatnosti, završni rad, Osijek 2016. godine, str. 2-12

7. Otisak prsta, Ivan Drakić, Bača, Miroslav; Schatten, Markus; Kišasondi, Tonimir: Prstom otključaj vrata, ZAŠTITA, Časopis o zaštiti i sigurnosti osoba i imovine, broj 2, godina II, Zagreb, 2006.

8. Tarek Saghir, Problem sigurnosti i privatnosti u biometrijskoj identifikaciji, diplomski rad, srpanj 2018. godine, str. 9-15

9. Vlatko Cvrtila, Nacionalni interesi i nacionalna sigurnost, Pregledni članak, 1995. godina, str. 62-69

10. Želimir Radmilović, Biometrijska identifikacija, Stručni članak, kolovoz 2018.godine, str. 159-180

Web izvori:

1.Apicurabi Business Intelligence, Dostupno na: https://apicura.hr/, Preuzeto: (01.03.2020)

2. Divljak, Dostupno na:https://divljak01.wordpress.com/, Preuzeto: (05.02.2020)

3. GDPR informer, Dostupno na : https://gdprinformer.com/ ,Preuzeto : (12.02.2020)

4. Genius croatia, Dostupno na:http://en.genius-croatia.com/, Preuzeto: (04.02.2020)

5. IIOT, Dostupno na: https://www.iotworldtoday.com/, Preuzeto: (13.03.2020)

6. Kommdata trgovina, Dostupno na : https://mobitrgovina.com/, Preuzeto: (14.03.2020)

7. Lider media, Dostupno na: https://lider.media/, Preuzeto : (01.03.2020)

8. Novi list, Hrvatska dobila novu Strategiju nacionalne sigurnosti, novilist.hr,14.srpnja 2017.godine, Dostupno na: http://novilist.hr/Vijesti, Preuzeto: (02.02.2020)

9. Pomorac.net, Dostupno na: http://pomorac.net/, Preuzeto : (04.02.2020.)

10. Republika Hrvatska, Ured vijeća za nacionalnu sigurnost, Strategija nacionalne sigurnosti Republike Hrvatske, Dostupno na : https://www.uvns.hr/hr, Preuzeto : (15.02.2020)

11.Terracon Bussines News, Marija Boban, Izbjeglička kriza i nacionalna sigurnost Republike Hrvatske, Dostupno na: http://terraconbusinessnews.com/marija-boban-izbjeglicka-kriza-nacionalna-sigurnost-republike-hrvatske, Preuzeto: (02.02.2020)

12. Videonadzorni sustavi, Dostupno na: https://www.007.hr/videonadzorni-sustavi-videonadzor-cctv/, Preuzeto: (13.03.2020)

13. Walker Beacon Lab, Dostupno na: https://www.walkterbeaconlab.com/face-recognition,Preuzeto: (05.02.2020.)

14. Wikipedija, Dostupno na: https://hr.wikipedia.org/wiki/Video_nadzor, Preuzeto: (13.03.2020)

15. Zakon.hr., Dostupno na: https://www.zakon.hr/, Preuzeto: (02.03.2020)

Popis slika:

Slika 1. Otisak prsta, Dostupno na: Genius Croatia, http://en.genius-croatia.com/, Preuzeto: (04.02.2020).....10

Slika 2. Biometrijske karakteristike lica, Dostupno na: https://www.iotworldtoday.com/, Preuzeto: (13.03.2020).....12

Slika 3. Signal glasa, Preuzeto sa: Tarek Saghir, Problem sigurnosti i privatnosti u biometrijskoj identifikaciji, diplomski rad, srpanj 2018. godine, str. 13.....14

Slika 4. Identifikacija putem šarenice, Dostupno na : https://mobitrgovina.com/, Preuzeto: (14.03.2020).....15

Slika 5. Primjer vlastoručnog potpisa,Dostupno na:Divljak,https://divljak01.wordpress.com/, Preuzeto: (05.02.2020).....16

Slika 6. Rezultati online ankete na pitanje „Smatram da se razvojem biometrije i njenom implementacijom u različite sfere ljudskog života podiže i razina opće sigurnosti i zaštite osobnih podataka.“.....31

Slika 7. Rezultati online ankete na pitanje „Osjećam se sigurnije ukoliko znam da je prostor u kojem se nalazim pri obavljanju određenih radnji pokriven videonadzorom“.....32

Slika 8. Rezultati online ankete na pitanje „Ukoliko bi sve javne površine grada u kojem živim bile pokrivene sustavom videonadzora osjećao/la bi se sigurnije“.....33

Slika 9. Rezultati online ankete na pitanje: „Smatram kako razvoj biometrije pridonosi boljitku kvalitete ljudskog života te kako on ne ugrožava privatnost i sigurnost ljudi“.....34

Slika 10. Rezultati online ankete na pitanje „Uspoređujući biometriju sa tradicionalnim metodama verifikacije korisnika (pinovi, lozinke..) smatram kako je biometrija jednostavniji i sigurniji način verifikacije“.....34

Slika 11. Rezultati online ankete na pitanje „Bez problema pristajem na korištenje biometrije kod pristupa vlastitom mobilnom uređaju“.....35

Slika 12. Rezultati online ankete na pitanje „Nemam strah ni sumnje u činjenicu da se moji

biometrijski podaci, ukoliko se koristim njima kako bi pristupio/la npr. mobitelu, zloupotrebljavaju u druge svrhe“.....36

Slika 13. Rezultati online ankete na pitanje „Razumijem na koji način funkcionira spremanje biometrijskih podataka ukoliko koristim otisak prsta za otključavanje vlastitog mobitela“...37

Slika 14. Rezultati online ankete na pitanje „Ukoliko znam da je prostor u kojem se nalazim pokriven sustavom videonadzora i samim time ugrožava moju privatnost ali mi se time jamči sigurnost, pristao/ la bih. Sigurnost u zamjenu za privatnost. Slažete li se?“.....38

Slika 15. Rezultati online ankete na pitanje: „Smatram kako je prepoznavanje lica, odnosno biometrija lica u komercijalne svrhe u redu. Npr. slučaj društvene mreže Facebook“.....38

12.ŽIVOTOPIS

Osobni podaci:

Ime i Prezime: Samanta Radelić

Datum rođenja: 02.07.1993

Mjesto rođenja: Kozarevac

Adresa: Smokovik, Stoci 3a

Mobitel: 098 954 3861

E-mail: samanta.radelic@gmail.com

Obrazovanje:

2017/2018. – danas, Sveučilišni odjel za forenzične znanosti Split

2013.-2017. Prvostupnik Upravnog prava

Pravni fakultet Split

2008.-2012. Ekonomist

Srednja škola Đurđevac

2004.-2008.- Osnovna škola Kloštar Podravski

2000.-2004.- Područna škola Kozarevac

Radno iskustvo:

Radno iskustvo sam stjecala kroz razne studentske poslove.

SVEUČILIŠTE U SPLITU
Sveučilišni odjel za forenzične
znanosti

13. IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, Samanta Radelić , izjavljujem da je moj diplomski rad pod naslovom „Nove tehnologije u nacionalnoj sigurnosti“ rezultat mog vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovog rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska vrata.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj mog rada u potpunosti odgovara sadržaju obranjenog i nakon obrane uređenog rada.

Split, 4. svibanj, 2020. godine

Potpis studenta: _____