Biometrija kao metoda zaštite podataka

Kudelić, Gabrijel

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2020/2021.

Gabrijel Kudelić

Biometrija kao metoda zaštite podataka

Završni rad

Mentor: Dr.sc. Vjera Lopina

Zagreb, svibanj 2021.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Sadržaj

1. UVOD

Tek nakon odslušanog kolegija "zaštita podataka" u meni su počela nicati pitanja i uvidi na temu privatnosti pojedinca, te koliko je ta privatnost (ne)zaštićena. Postalo je jasno koliko na svakodnevnoj bazi baratamo i razmjenjujemo rizične i osjetljive podatke. Većina nije svjesna tih procesa. Mnoge pogodnosti koje nam je tehnološki napredak donio i omogućio uzimamo zdravo za gotovo. Najčešće se uviđaju pogodne strane tog napretka, ali je važno osvijestiti mnoge ranjivosti i rizike koji dolaze s njim. "Uz veliku moć dolazi i velika odgovornost". No da bismo njome mogli ovladaiti, potrebno je kroz vlastitu edukaciju razviti razumijevanje spram dobrih i loših strana koje ona donosi za sobom, kako bismo mogli zaštititi sebe i druge. Stoga mi se biometrija učinila kao pogodna tema, biometrija i njene tehnike su danas sveprisutne, te gotovo neprimjetne čovjeku današnjice.

2. BIOMETRIJA

2.1. Pojam biometrije

Biometrija je tehnika za autentifikaciju jedinstvene fizičke karakteristike čovjeka. Utvrđivanje identiteta bazira se na fizičkim, biokemijskim ili bihevioralnim atributima osobe. Uloga biometrije u modernom društvu dobiva na značenju zbog povećane potrebe svakodnevne identifikacije i zaštite čovjeka. Funkcionalnost takvih sustava oslanja se na ispravno utvrđivanje identiteta jedinstvene osobe u odnosu na ostale osobe koje se prijavljuju u sustav. Primjeri takvih sustava su dijeljenje mrežnih resursa, odobravanje pristupa strogo čuvanim ustanovama, izvršavanje financijskih transakcija ili ukrcavanje na let avionom. Krajnji zadatak sustava upravljanja identitetom je utvrđivanje ili verifikacija identiteta osobe.

2.2. Pojam biometrijskog sustava

Biometrijski sustavi bez obzira na metode kojima se koriste, u svojoj srži sastoje se od četiri elementa kojim se vrši identifikacija. Prvi je ulazna jedinica tj. senzor koji služi za stvaranje virtualnog prikaza tj. skeniranje biometrijskog obilježja nekog pojedinca. Drugi element je ekstraktor, njegova je svrha prepoznati i izdvojiti samo ono potrebno tj. izdvojiti objekt od pozadine, izoštriti prikaz, podesiti svjetlinu itd. Zatim iz skeniranog biometrijskog obilježja generira geometrijski predložak te prepoznaje ono što ga čini jedinstvenim i individualnim. Treći element jest baza biometrijskog sustava unutar koje se stvara svojevrsni dosje prvotno zabilježenog biometrijskog obilježja. Zadnji element biometrijskog sustava je jedinica za verifikaciju i komparaciju. Funkcija tog elementa je da usporedbom provjeri podudarnost ili moguću nepodudarnost autentifikatora sa uzorcima iz baze tj. verifikatorima, te donese odluku. Biometrijski sustavi uglavnom koriste algoritam koji uspoređuje koliko se autentifikator i verifikator poklapaju te procjenjuje postotak njihove podudarnosti i iskazuje je u obliku brojčane vrijednosti. Sustav provjerava preklapanje vektora dobivenih iz generiranih geometrijskih uzoraka.

Postoje dvije vrste pogreški koje se mogu dogoditi. Prva je pogrešna potvrda, ta pogreška se javlja kada autentifikator i verifikator izbace dovoljnu visoku vrijednost unutar sustava te se neovlaštenoj osobi ustupi pristup. Takva vrsta pogreške uvrštava se u FAR (False Acceptance Rate), što bi u doslovnom prijevodu značilo omjer lažno prihvaćenih uzoraka. Druga vrsta

pogreške koja se pojavljuje je pogrešno odbijanje to je pogreška koja se javlja kada odgovarajući autentifikator i verifikator ne izbacuju dovoljno visoku vrijednost, te ovlaštenoj osobi pristup bude odbijen. Ovaj tip pogreške uvrštava se u FRR (False Rejection Rate). Kako bi biometrijski sustav radio u skladu sa svojim karakteristikama i ograničenjima, potrebno je pratiti statistiku FAR-a i FRR-a. FAR i FRR su proporcionalne suprotnosti, ako nam je potrebna veća sigurnost, sustav ćemo ugoditi tako da ima veću pojavnost FRR-a te će se za jednako toliko smanjiti broj pojava FRR-a i obrnuto. Kod odluke o odnosima FAR-a i FRR-a potrebno je promišljati o svrsi biometrijskog sustava i proporcionalno tome stvoriti balans između lakoće uporabe i sigurnosti sustava. CER (Crossover error rate) je mjerna jedinica kojom se procjenjuje pouzdanost, točnost i preciznost biometrijskih uređaja i sustava. Što je CER manji to je biometrijski sustav bolji.

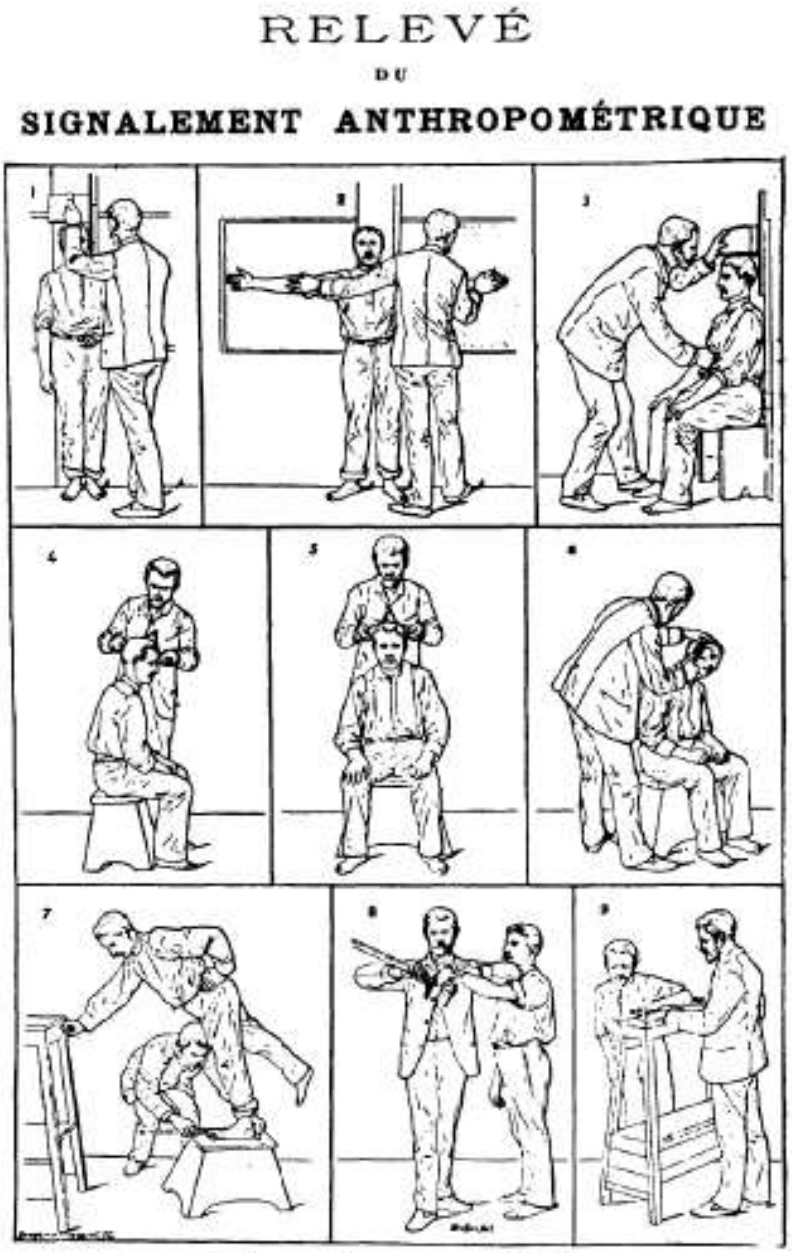
2.3. Povijest biometrije

Pitanje svih mogućih aspekata razlikovanja, prepoznavanja i identifikacije javlja se još u dalekoj povijesti**.** U plemenskom sustavu prvobitne zajednice, nepoćudne članove plemena koji su se ogriješili o plemenska pravila uz progon kao mjeru s vrlo izvjesnom smrtnošću (nije se moglo preživjeti sam, bez vatre, hrane i lovačke opreme), određivalo se i označavanje istih sakaćenjem, ožiljcima ili žigosanjem, kako bi svi znali da se radi o prognaniku, pa ga obično, nakon što je prepoznat kao takav, nije prihvaćalo niti drugo pleme.

Poznati su slični načini označavanja ubojica, lopova i nemoralnih u srednjovjekovnoj Europi, ali i diljem svijeta. Pojedine metode identifikacije koristile su se i u *humanije* svrhe, pa je poznato da su prije četiri tisućljeća u pisanim dokumentima Asiraca i Babilonaca kao znak pisca i dokaz autorstva na dokument otiskivani otisci papilarnih linija prsta (tzv. Supur), a još stari Kinezi daktiloskopirali su novorođenčad kako bi izbjegli zamjenu djece.

U novom dobu, a posebno razvojem humanističkih i prirodnih znanosti došlo je do procvata brojnih metoda koje su trebale pridonijeti identifikaciji, prepoznavanju i razlikovanju određenih osoba. Prije svega radi se o apliciranju medicinskih znanosti u području kriminalističke identifikacije osoba i o traseološkoj identifikaciji.

Slika 1. Mjerenje glave 1913. godine



Slika 2. Apometrijski sustav Bertilloange 1883. god

3. PODJELA BIOMETRIJSKIH METODA

Svaki pojedinac ima više individualnih obilježja veće ili manje invarijantnosti. U to pripadaju otisak prsta, šarenica oka, hod, karakteristike lica, oblik usne školjke, raspodjela krvnih žila…

Podjela biometrijskih podataka:

- Otisak prsta
- Biometrija dlana
- Biometrija lica
- Biometrija oka
- Biometrija potpisa
- Biometrija glasa
- Termograf lica i tijela
- DNK
- Ostale biometrijske metode

3.1. Biometrija otisaka prsta

Najpoznatije, najraširenije i najprisutnije biometrijsko obilježje u našoj svakodnevici je informacija sakrivena na vršcima prstiju.

Uzorak otiska prsta uvjetovan je već u embrijskom stadiju razvoja osobe, te se vjeruje da je uzorak prsta u potpunosti jedinstven za svakog pojedinca. Uzimajući u obzir da osoba stari, te da postoji mogućnost ozljede, proces skeniranja neće biti proveden sto postotno. Zbog visoke razine jedinstvenosti naglasak se stavlja samo na glavne karakteristike i obilježja, te su ona dovoljna za veću podudarnost između skeniranog uzorka i već postojećeg uzorka u bazi podataka.

Kada se to biometrijsko obilježje digitalizira, postaje izuzetno pouzdano oruđe i metoda za izvršavanje identifikacije. Koristi se na svakodnevnoj bazi u gotovo svim aspektima života. Na primjer koristi se za otvaranje ulaznih vrata, korištenje dizala, otključavanje automobila, otključavanje mobilnog uređaja, može se čak naći na kućanskim uređajima kao što su hladnjaci, perilice rublja te i ostalim uređajima za koje ne bi bilo pogodno da su korišteni od strane djece.

Slika 3. Obilježja otiska prsta

Kod biometrijskog obilježja otiska prsta koristi se nekoliko metoda i to:

- Optička metoda se vrši tako da prst položimo na površinu skenera, a linije na vršcima prstiju poznate kao papilarne linije snimaju se pomoću optičkih čipova zadovoljavajuće rezolucije i brzine prijenosa. Npr. CMOS senzori omogućuju čitanje podataka sa svih fotoosjetljivih elemenata odjednom, te tako na mjestima tj. udubljenih dijelova otiska prsta gdje svjetlo ne dopire skener ih zapisuje kao „nepostojeće“ piksele a izbočene dijelove kao crne tj. „postojeće“. Na taj način skener prikazuje samo izbočene linije, te tako tvori točan prikaz. Na isti način funkcionira CCD matrica, ali za razliku od CMOS-a CCD matrica čita informacije iz svake ćelije uzastopno te je samim time brzina prijenosa znatno sporija. Nerijetko skeneri ovog tipa sadrže ugrađeni izvor svijetlosti, kako bi sken bio veće kvalitete. Uglavnom se koristi LED svjetleća dioda poradi izrazito niske emisije toplinske energije, i niske potrošnje. Slabost ove metode je „sjena“ sačinjena od prirodnih ulja i masti iz kože, koja ostaje na površini skenera te se potencijalno može zlorabiti.

- Kapacitivna metoda skeniranja otiska prsta vrši se istoimenim kapacitivnim skenerom. Kapacitivni skener se sastoji od mikro kondenzatora smještenih unutar silikonske smole koji su ravnomjerno raspoređeni njenom cijelom površinom, u obliku kvadratne ili pravokutne matrice. Uglavnom je ta vrsta skenera kvadratnog ili pravokutnog oblika. No smatra se da pravokutni oblik bolje prati ergonomiju prsta. Proces skeniranja funkcionira tako da sustav tvori sliku pomoću različitih stanja svake pojedine točke na polju. Kondenzatori koji su ostali nabijeni nisu prepoznati kao pikseli, a one koji su prilikom kontakta sa kožom ispraznili svoj naboj sustav prepoznaje kao piksel. Ovakva

metoda skeniranja funkcionira zbog razlika u elevaciji na površini jagodice. Prosječna širina između izbočenih linija tj. papilarnih linija je 450 mikrona. Što je podosta kada usporedimo sa međusobnom udaljenošću kondenzatnih modula koja iznosi samo 50 mikrona tj. udaljenost među modulima iznosi samo 25 μm^2.

- Kada prst položimo na površinu skenera, ultrazvučni odašiljač mjeri vrijeme koje je potrebno da odaslani zvučni val iz ultrazvučnog odašiljača stigne do kože i vrati se nazad do ultrazvučnog resivera. Zbog razlika u elevaciji vrijeme slanja i zaprimanja se razlikuje, te je na taj način stvoren 3D prikaz pupilarnih linija. Pozitivna strana i najveća prednost ove tehnike je ta što bez obzira na to je li prst mokar ili mastan ultrazvučni valovi prodiru čak i do četiri milimetra ispod kože i vrše gotovo besprijekoran sken. No mana ove metode je visoka cijena pošto je najnovija na tržištu.

3.2. Biometrija dlana

U pravilu se ovo biometrijsko obilježje koristi na mjestima gdje je velika protočnost korisnika. Ova vrsta biometrijske tehnologije uzima relativno grube informacije, te zbog vrlo jednostavnog prikaza koje ovo biometrijsko obilježje potrebuje moguće je spremiti velike baze sa puno uzoraka na jako malo zapremnog prostora.

Nedostatak ove tehnike je što i najsitniji detalji poput nakita ili deformacija nakon povrede imaju pozamašan utjecaj na preciznost verifikacije. Sustav uzima mjere čak trideset geometrijskih obilježja dlana. Mjeri površinu, duljinu, širinu, opseg i polumjer svakog prsta zasebno, zatim površinu, duljinu, širinu, opseg i polumjer dlana kao zasebnog objekta te nakraju opseg i geometrijski oblik dlana kao cjeline. Od skeniranih obilježja tvori specifični obrazac.

Neki tipovi ovog sustava koriste dvije kamere koje vrše skeniranje s gornje i donje strane dlana te tako zadobivaju novu mjernu dimenziju koju možemo nazivati obujmom. Dok drugi sustavi mnogo jednostavnije prirode koriste samo siluetu dlana kako bi izvršili proces. No svi sustavi koriste metalne dijelove znane kao spejsere na površini za skeniranje kojim je svrha razdvojiti prste i postaviti dlan u najidealniji položaj za izvršavanje procesa. Naravno svaki od sustava se razlikuje po stupnjevima FAR-a, CRR-a i CER-a, no izbor sustava ovisi o potrebi i svrsi u koju se koristi.

Tehnologija za prepoznavanje slanosti ljudskog tkiva je zapravo nadogradnja i dodatak tehnologiji koja prepoznaje biometrijska obilježja dlana te samim time podiže sigurnost i

preciznost tog sustava mijenjajući CER (Crossover error rate) dimenziju ovog sustava. Ono što dovodi do kratkog spoja nakon kontakta nekog hardvera sa vodom zapravo nije voda nego minerali koji omogućuju vodi da bude vodič.

Način na koji funkcionira provjera slanosti je sličan kao i navedeni fenomen. Sustav projicira niskofrekventni električni naboj na površinu koju koristi kao senzor, te ovisno o količini minerala u znoju znanih kao elektroliti sustav zaprima više ili niže razine frekvencije, tj. veću ili manju provodljivost.

3.3. Biometrija lica

Sakupljanje fotografija i skenova lica je jedna od najmanje nametljivih i gotovo nezamjetnih procesa.

Proces se sastoji od dva glavna dijela, lociranja lica i prepoznavanja specifičnih obilježja. Za lociranje lica potrebna je kamera više rezolucije. Proces lociranja ne predstavlja problem, pošto je lako izvršiti diferencijaciju između lica i pozadine. Proces prepoznavanja specifičnih obilježja lica isto tako je moguće postići digitalnom kamerom, ali sa znatno manjom pouzdanošću.

Da bi se taj proces visoko kvalitetno obavio, koriste se specijalizirani uređaji, kao što su infracrvena kamera, reflektor infracrvene svjetlosti, senzor udaljenosti tj. dubine i reflektor točaka. Ti se uređaji koriste u tandemu kako bi se dobio potpuni sken lica i njegovih specifičnih obilježja potrebnih za autentikaciju, odnosno identifikaciju pojedinca.

Slika 4. Slikoviti prikaz biometrije lica mobilnim uređajem

Slika 5. Hardware za biometriju lica

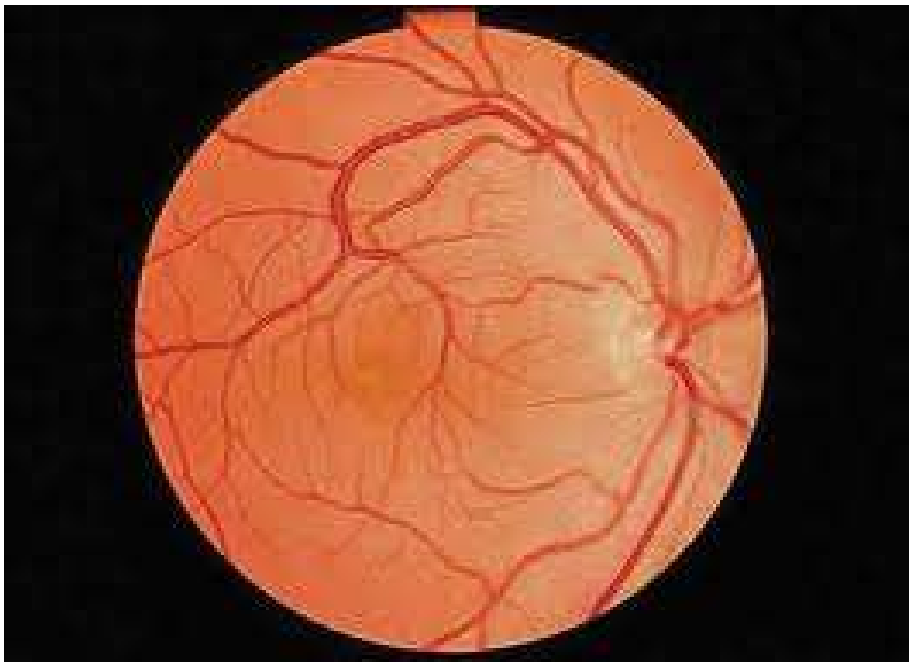
3.4. Biometrija oka

MREŽNICA

Sken mrežnice je jedno od najsigurnijih biometrijskih identifikacijskih obilježja. Mrežnicu tj. unutarnju strukturu oka nije moguće promijeniti ili replicirati, niti se ona mijenja tijekom čitavog života osobe, a mrežnica toliko brzo propada da nije moguće izvršiti sken mrtve osobe.

Za uspješno skeniranje mrežnice, oko je potrebno približiti okularu skenera, te fokusirati pogled na određenu točku. Proces skeniranja traje između 10 i 15 sekundi. Za vrijeme skeniranja na oko se projicira niskoenergetski snop infracrvene svjetlosti, koju očne kapilare i krvne žile apsorbiraju više od ostatka oka. Time nastaje razlika u refleksiji te je jasno vidljiva putanja i debljina kapilara, koja tvori specifičan uzorak korišten za identifikaciju pojedinca.

Ono što ovu biometrijsku metodu čini nepraktičnom je njena nametljivost, i neugodnost samog procesa. Prednost ove metode je što osoba mora biti veoma blizu skenera, te je iz tog razloga nemoguće izvesti krađu tj. sken mrežnice bez znanja osobe.



Slika 6. Sken mrežnice

ŠARENICA

Šarenica je univerzalno, trajno i nepromjenjivo biometrijsko obilježje. Prepoznavanje osoba skeniranjem šarenice (iridologija) jedna je od najpouzdanijih biometrijskih metoda, ponajviše zbog prirodnih karakteristika šarenice.

Šarenica je obojeni dio oka koji svoj izgled poprima u najranijem djetinjstvu i ne mijenja se tijekom vremena. Izgleda poput prstena koji okružuje zjenicu. Načinjena je od vlaknastog mišića, kojim obično prevladava singularna dominantna boja. No na dominantnoj boji vidljive su brazde i pjege u različitim nijansama iste, ili potpuno različite boje. Te brazde i pjege čine jedinstveni nepromjenjiv kompleks, kojim je moguće definirati oko 200 identifikacijskih karakteristika i obilježja. Definirana obilježja su jedinstvena za svakog pojedinca, te pogodna za njegovu identifikaciju.

Većina sustava za skeniranje šarenice ima veoma visok stupanj sigurnosti. Ne mogu se prevariti slikom očiju, lećama, sintetičkom replikom oka, niti okom odstranjenim s mrtve osobe. Šarenicu je nemoguće mijenjati zahvatima estetske kirurgije bez maksimalnog rizika od gubitka vida. Većina sustava ima sistem za prepoznavanje leća. Sustav isto tako može uz pomoć sistema za prepoznavanje mišićnog rada tj. kontrakcije i širenja šarenice prepoznati je li riječ o slici, sintetičkoj replici ili mrtvom organu. Ova tehnika identifikacije vrlo je jednostavna, pouzdana i nenametljiva. U procesu skeniranja nije potreban fizički kontakt osobe sa skenerom. Skeniranje šarenice oka se vrši se infracrvenom kamerom s udaljenosti od 12cm do 45cm.

Slika 7. Primjer dviju različitih šarenica

3.5. Biometrija potpisa

Čovjek od ranih godina počinje učiti čitati i pisati. Za pisanje, potrebno je puno vježbe i ispisanog teksta. Uz toliko prakse i vježbe, počinje se razvijati poseban način pisanja slova, riječi i rečenica koje može postati prepoznatljiv, te se može koristiti kao biometrijska karakteristika pojedine osobe. Na temelju te biometrijske karakteristike može se izvršiti identifikacija ili verifikacija određene osobe. Kod plaćanja računa kreditnom karticom, potpisivanju ugovora ili davanju izjava, potreban je potpis. Potpisom osoba garantira za napisane stavke na dokumentu i da će, ako dođe do nesuglasica, pravno odgovarati. Verifikacija potpisa vrši se tako da se identificira način na koji osoba potpisuje svoje ime. Način pisanja kao što su brzina, pritisak pisala, oblik slova oblikuju jedinstvenost potpisa.

Od davnih vremena poznata je identifikacijska vrijednost rukopisa i potpisa. Činjenica da svaka osoba ima jedinstven rukopis, a potpis je neka vrsta otiska prsta, otvara mogućnost koja se može iskoristiti u identifikaciji osoba. U klasičnoj identifikaciji rukopisa i potpisa provodi se grafološka analiza koja se uglavnom temelji na grafičkim, ali i nekim psihološkim i bihevioristićkim premisama skriptora, odnosno osobe kojoj pripada rukopis ili potpis. Grafologija se može definirati kao disciplina namijenjena otkrivanju i definiranju širokog spektra osobina i sposobnosti. Katkad se naziva i psihologija rukopisa. Grafologijom se u širem smislu može smatrati i analiza rukopisa kao vrsta ekspertize kojom se utvrđuje identitet osobe.

Kad je riječ o biometrijskoj metodi analize potpisa i rukopisa, treba kazati da je prihvatljiva iako postoji mogućnost krivotvorenja (još uvijek vlada mišljenje da je za mjerodavnu analizu potrebno tumačenje eksperta – subjektivno mišljenje temeljeno na objektivnom nalazu). Ipak, određena obilježja rukopisa, odnosno potpisa mogu se grafički determinirati i klasificirati, jer ostaju nepromijenjena unatoč pokušajima namjernog iskrivljavanja načina pisanja, pa postoji prostor za automatsku klasifikaciju i identifikaciju.

Svaki rukopis ima svoja opća i posebna obilježja. Opća obilježja su opći izgled rukopisa, stupanj ispisanosti, raspored teksta, odnos prema liniji pisanja, veličina rukopisa, razmaci, vezanost i nevezanost slova, rastavljanje riječi, brzina pisanja, pritisak na papir, nagib rukopisa, ukrašavanje i dr.

Posebna obilježja se za razliku od općih ne mogu u potpunosti definirati, jer su individualna od osobe do osobe, ali se baziraju na mjerenju nagiba, brzine, jačine pritiska, duljine poteza ruke. Upravo na ovim obilježjima temelji se biometrijska identifikacija skriptora.

Osoba započinje proces učenja prepoznavanja i repliciranja simbola alfabeta najkasnije sa 6 god. Pet godina kasnije tj. u 11. godini života počinju se javljati prvi znaci individualnosti u rukopisu. U tom periodu u rukopisu mlade osobe moguće je uočiti poseban način pisanja određenih slova, riječi i rečenica. Kako osoba stari tj. sazrijeva, rukopis pojedinca ne doživljava neke znatne promjene, ali postaje vidljivo da se specifične karakteristike počinju javljati učestalije i konzistentnije. Zbog same konzistentnosti i prepoznatljivosti specifičnih uzoraka rukopisa, potpis postaje mjerljiva biometrijska karakteristika za identifikaciju pojedinca.

Ova biometrijska metoda temelji se na bihevioralnim karakteristikama vidljivim u rukopisu pojedinca. Mjerljiva obilježja koja oblikuju jedinstvenost potpisa su brzina, nagib potpisa, nagib i jačina pritiska pisala, duljina poteza, oblik slova, ukrašavanje i drugo. Velika prednost ovakvog tipa identifikacije je njena jednostavnost i niska cijena instrumenata potrebnih za njeno provođenje.

Dva glavna pristupa verifikaciji potpisa su statička metoda i dinamička metoda. Kod statičkog verificiranja potpisa, sustav stavlja fokus na njegov oblik i njegove geometrijske karakteristike. Sustav normalizira veličinu potpisa, te naglasak stavlja na njegove sastavne dijelove kao što je preklapanje linija, zavijutci, točke, nagib i dužina linija koje su sastavni dio određenih simbola.

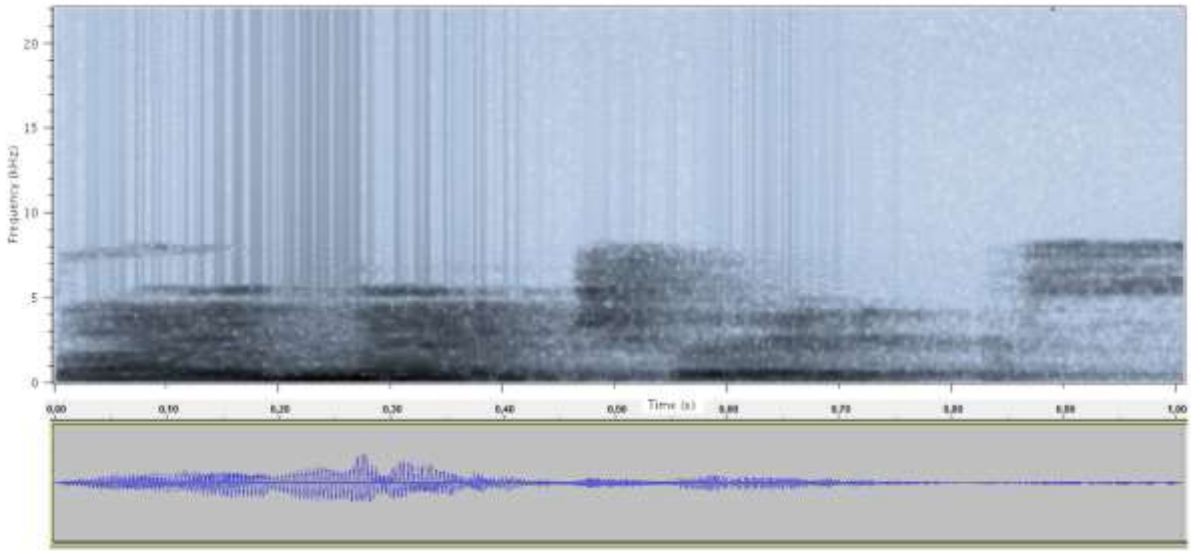
Dinamička verifikacija potpisa naglasak stavlja na vrijeme koje je potrebno za njegovu egzekuciju, brzinu poteza i putanju toka potpisa. Kod dinamičkog pristupa sustav analizira sve navedene atribute u stvarnom vremenu.

Nova tehnologija koja koristi stilos i tablet stopila je oba pristupa u jedan, i povećala sigurnost. Stoga krivotvoritelj potpisa mora replicirati sve od navedenih atributa i karakteristika. Možemo zaključiti da krivotvorenje potpisa postalo gotovo nemoguće, te da je iznimno teško kod svih nabrojenih faktora izvesti podudarnost.

Slika 8. Stilos i tablet

3.6. Biometrija glasa

Svakodnevno raspoznajemo sugovornike pomoću njihova glasa, no ipak se radi o subjektivnom doživljaju koji je temeljen na subjektivnim karakteristikama slušatelja pa ovakva metoda nije potpuno kvalitetna. Glas pojedinca također ima jedinstvene karakteristike, pa se zbog toga može smatrati biometrijskim obilježjem. Vrlo se lako može zabilježiti, odnosno stvoriti kontrolne uzorke. Kada je riječ o identifikaciji putem analize ljudskog glasa, radi se o obilježjima kao što su boja glasa, modulacija, frekvencija, govorne mane i sl., a to područje identifikacije naziva se fonoskopska identifikacija. Zbog pojave novih tehnologija za mimikriju i manipulaciju zvučnih uzoraka glasa, korištenje ove biometrijske metode je u potpunosti zastarjelo. Sigurnost ovakvog načina identifikacije nije više na zadovoljavajućoj razini.



Slika 9. Biometrijska obilježja glasa

3.7. Termograf lica i tijela

Ljudska bića su toplokrvna, unutar svog organizma sadrže krvožilni sustav koji se kao i živčani sustav prožima kroz cijelo tijelo. Svaki organ ljudskog organizma je ispunjen krvlju kao i najveći organ ljudskog tijela koji služi kao barijera koja odvaja unutarnji svijet od vanjskog, a organ o kojem je riječ je koža, iz tog razloga možemo uz pomoću termografskih kamera uočiti uzorke sačinjene od termičkih razlika na površini kože.

Neki dijelovi tijela su zbog razlike u razini prokrvljenosti veće ili manje temperature. Najtopliji dio ljudskog organizma je trup zatim ga slijede prepone, pazusi, glava i lice. Najhladniji dijelovi tijela su laktovi, koljena, šake i stopala.

Za proces prikupljanja termografskog biometrijskog obilježja potrebna nam je prije svega kamera za termalni imidžing. Kamera tog tipa ima posebnu leću koja dopušta infracrvenoj svjetlosti da prolazi kroz nju, zatim fokusirano infracrveno svijetlo koje dolazi do senzora koji skenira informaciju i sakuplja ju od nekoliko tisuća točki koje dobiva iz vidokruga.

Kroz taj proces dobivamo složeni uzorak sačinjen od temperaturnih razlika. Dobivena slika poznata nam je kao termogram. Za stvaranje slike potrebna je samo jedna tridesetina sekunde. Termogram se tada pretvara u električne impulse koji su zatim usmjereni u jedinicu za procesuiranje signala koja prevodi informaciju u vizualne podatke. Dobivena slika se prikazuje na sučelju u raznovrsnim bojama koje koreliraju spram količine infracrvene energije koja je odaslana iz svijeta u senzor. Kombinacija navedenih elemenata koja generira sliku nam dopušta da svijet promatramo kao prikaz toplinske radijacije.

Razlike u prokrvljenosti dereme, hipoderme i epiderme čine termogram biometrijskim obilježjem. Termogram lica i tijela ispunjava sve uvjete da bi bio biometrijsko obilježje, univerzalan je, individualan i konstantan. Prednost ove biometrijske metode je to što ga je moguće obaviti u uvjetima gotovo nemogućima za klasičnu kameru.

Skeniranje termoograma u svrhu prepoznavanja i identifikacije se može obaviti i bez voljnog pristanka pojedinca. Iz tog razloga se dovodi u pitanje etičnosti ovog biometrijskog postupka.

3.8. Biometrija DNK

Analiza DNK je jedna od najznačajnijih i najpouzdanijih metoda biometrijske identifikacije.
Koristi se u mnogim područjima istraživanja, a nama najzanimljivija primjena je u području gdje se analiza DNK koristi za utvrđivanje identiteta osobe, dokazivanje roditeljstva, posmrtnu identifikaciju ostataka mrtvog tijela, određivanje spola osoba itd.

Razvojem prirodnih znanosti, a prije svega molekularne biologije, došlo se do spoznaje o genetskoj uvjetovanosti brojnih ljudskih psiho-tjelesnih karakteristika, ali i o individualnosti i neponovljivosti ljudske stanice tj. jedinstvenosti građe molekule DNK.
DNK ili deoksiribonukleinska kiselina je molekula građena u obliku dvostruke spiralne zavojnice koja je međusobno povezana parovima baza. Svaka molekula sadrži oko tri milijuna takvih parova baza. Molekula DNK nalazi se u svakoj stanici ljudskog organizma i njena struktura predstavlja genetsku šifru kao osnovu nasljeđivanja. Oko 99,5% DNK molekule je zajedničko svim ljudima i to područje DNK naziva se nekodirajuće područje, dok preostalih 0,5% predstavlja kodirajuća područja koja su visoko varijabilna (polimorfna), te čine svaku osobu jedinstvenom, a iznimka su jednojajčani blizanci kojima je i DNK isti. Na proučavanju kodirajućih područja temelji se obilježje korišteno u svrhu biometrijske identifikacije.
Genetičke odrednice nalaze se u 23 para kromosoma, odnosno u 46 kromosoma koji se nalaze u jezgri svake tjelesne stanice. Unutar kromosoma na točno određenim mjestima nalazi se približno 30 000 do 40 000 gena, koji određuju sva svojstva jednog organizma. Polovica od ukupno 46 kromosoma, odnosno 23 kromosoma nasljeđuju se od majke, a 23 od oca. Jedan od tih parova čine spolni kromosomi (X, Y), koji određuju spol osobe.
Preostala 22 kromosomska para, koji se nazivaju autosomi, prenose nasljedna svojstva. To je osnova za određivanje spola temeljem analize DNK.

U primjeni analize DNK za svrhe biometrijske identifikacije koriste se unaprijed određeni lokusi, za koje je poznato da sadrže određene parove baza koji se uzastopno ponavljaju, a istodobno pokrivaju veliku varijabilnost u ljudskoj populaciji, odnosno koji sadrže VNTR. VNTR ili varijabilni (polimorfni) ponavljajući sljedovi. (engl. *Variable number tandem repeats*) su visoko polimorfni sljedovi i određeni su brojem ponavljajućih DNK sekvenci. Većina DNK sljedova odnosno sekvenci ne sadrži gene, već služi isključivo kao pomoćni genetički materijal. Kratke sekvence parova baza koji se učestalo ponavljaju, nazivaju se kratki ponavljajući sljedovi ili STR (*short tandem repeats*). Iako se ove sekvence pojavljuju u DNK

svake osobe, broj ponavljanja sekvenci jako se razlikuje od osobe do osobe. Upravo se na utvrđivanju broja i dužine ponavljanja tih sekvenci temelji identifikacija osoba metodama analize DNK.

Svaka stanica građena je od jezgre kao središnjeg dijela i citoplazme koja okružuje jezgru, a koja je s vanjske strane obavijena membranom koja stanicu odvaja od drugih stanica. U jezgri se nalaze kromosomi koji su nositelji osnovnog nasljednog materijala. U kromosomima je smještena jezgrina ili nukleusna DNK, dok se u citoplazmi nalaze brojne stanične strukture među kojima i mitohondriji, u kojima se nalazi mitohondrijska DNK. Stoga se razvila i druga mogućnost identifikacije, analizom mitohondrijske DNK koja je s mnogim drugim staničnim strukturama sastavni dio citoplazme. Iako je po strukturi slična jezgrinoj DNK, mitohondrijska DNK se od jezgrine razlikuje po tome što je znatno manja i u svojoj strukturi ima oko 10.000 puta manje parova baza, ali zato ima više stotina kopija od jezgrine. Također bitna razlika u odnosu na jezgrinu DNK je u načinu nasljeđivanja. Mitohondrijska DNK nasljeđuje se isključivo po majci tako da sva braća i sestre imaju slijed nukleotida mitohondrijske DNK identičan majčinom. Razlog tome leži u činjenici što jajna stanica ima nekoliko tisuća mitohondrija i stotine tisuća kopija mitohondrijske DNK, a spermij svega nekoliko mitohondrija. Budući da je način nasljeđivanja samo po majčinoj liniji, prilikom identifikacije primjenom analize mitohondrijske DNK moguće je koristiti nesporne uzorke pribavljene od srodnika koji su u obiteljskom stablu relativno daleko od sporne osobe, bilo vodoravno ili okomito u načinu nasljeđivanja. Prednost mitohondrijske pred jezgrinom DNK je upravo u činjenici da svaka stanica sadrži više stotina kopija mitohondrijske DNK, zbog čega je lako izdvojiti dovoljnu količinu DNK potrebnu za analizu, čak i u slučaju malo biološkog materijala. Nedostaci DNA metode se ogledaju u tome što je to dugotrajan i skup proces analize koji uključuje stručno osposobljene osobe, DNA uzorci su osjetljivi, lako se onečiste.

3.9. Ostale biometrijske metode

Vrijedno je spomenuti i ostale oblike biometrijske identifikacije kao što su oblik ušne školjke, miris tijela, raspored krvnih žila, dinamika tipkanja, pulsiranje krvotoka i prepoznavanje hoda itd. Njih nećemo pobliže opisivati jer nisu u toliko širokom doticaju s "običnim" korisnicima.

4. ZAŠTITA PODATAKA

4.1. Zakonodavni okvir

Zaštita osobnih podataka uređena je sljedećim propisima:

- Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija (Narodne novine broj 68/18)
- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)
- Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine broj 42/18)

4.2. Zaštita podataka i pravo na zaštitu podataka

Zaštita podataka je niz mjera i postupaka koji se poduzimaju kako bi se osigurao integritet podataka koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

Primjeri osobnih podataka:

- ime i prezime
- kućna adresa
- e-adresa (ime.prezime@poduzeće.com)
- broj identifikacijske isprave
- podaci o lokaciji, na primjer funkcija za podatke o lokaciji na mobilnom telefonu
- adresa internetskog protokola (IP adresa)
- identifikacijska oznaka kolačića
- identifikacijska oznaka oglašavanja vašeg telefona
- podaci u posjedu bolnice ili liječnika, koji mogu na jedinstven način identificirati osobu.

Pravo na zaštitu osobnih podataka ustavna je kategorija, budući da je člankom 37.1. Ustava Republike Hrvatske (NN 85/10 -pročišćeni tekst) svakoj osobi zajamčena sigurnost i tajnost osobnih podataka. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi.

4.3. Zaštita podataka u EU

U Povelji EU-a o temeljnim pravima navodi se da svaka osoba u EU-u ima pravo na:

- zaštitu osobnih podataka koji se na nju odnose
- pristup prikupljenim podacima koji se na nju odnose i pravo na njihovo ispravljanje

Od svibnja 2018., stupanjem na snagu Opće uredbe o zaštiti podataka (GDPR), postoji jedan skup pravila o zaštiti podataka za sva poduzeća koja posluju u EU-u, neovisno o njihovu poslovnom nastanu.

Uredba je stupila na snagu 24. svibnja 2016., a primjenjuje se od 25. svibnja 2018. Zahvaljujući strožim pravilima uvedenima Općom uredbom o zaštiti podataka:

- građani i građanke imaju veću kontrolu nad svojim osobnim podacima
- poduzeća ostvaruju korist od jednakih uvjeta.

Paket za reformu zaštite podataka, koji je EU donio 2016., uključuje i Direktivu o zaštiti osobnih podataka koji se obrađuju za potrebe izvršavanja zakonodavstva u području kaznenog prava. Objedinjeno i ažurirano zakonodavstvo o zaštiti podataka ključno je kako bi se zajamčila temeljna prava pojedinaca na zaštitu njihovih osobnih podataka, omogućio razvoj digitalnoga gospodarstva i pojačala borba protiv kriminala i terorizma.

Slika 10. Plakat Vjeća Europske unije

5. POVREDA OSOBNIH PODATAKA

Povreda osobnih podataka, sukladno Općoj uredbi o zaštiti podataka, predstavlja kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Opća Uredba o zaštiti podataka pojašnjava i uvodi određena nova prava za ispitanike te osigurava, osim u iznimnim situacijama, jednaku razinu zaštite svakom pojedincu iz Europske unije.

Prema Općoj uredbi o zaštiti podataka imate pravo:

- biti obaviješteni o obradi vaših podataka - tko ih obrađuje i koristi, u koju svrhu i na temelju koje pravne osnove.
- ostvariti pravo pristupa osobnim podacima.
- zatražiti ispravak i brisanje osobnih podataka od voditelja obrade zatražiti ograničenje obrade osobnih podataka.
- ostvariti pravo na prenosivost (pravo da zaprimite podatke koji se na vas odnose te pravo da prenesete podatke drugom voditelju obrade).
- uložiti prigovor na obradu osobnih podataka
- zahtijevati da se na vas ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi osobnih podataka, uključujući izradu profila.

5.1. Tijelo nadležno za provedbu Opće uredbe o zaštiti podataka

Agencija za zaštitu osobnih podataka nadležna je za provedbu Opće uredbe o zaštiti podataka. Agencija za zaštitu osobnih podataka (u daljnjem tekstu: Agencija) je samostalno i neovisno tijelo koje nadzire provedbu Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27.04.2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka (Opće uredbe o zaštiti podataka) i obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18) kojim se osigurava provedba.

5.2. Opće uredbe o zaštiti podataka.

Sukladno Općoj uredbi Agencija ima savjetodavne, korektivne i istražne ovlasti. Agencija kontinuirano ulaže napore da primjerena zaštita privatnosti (zaštita osobnih podataka) kao jedno od temeljnih ljudskih prava postane opće prihvaćeno načelo rada svih koji prikupljaju, obrađuju i prenose osobne podatke. Svatko tko smatra da mu je povrijeđeno pravo na zaštitu osobnih podataka, može se Agenciji obratiti zahtjevom za zaštitu prava, o čemu Agencija odlučuje rješenjem.

Obrada osobnih podataka je zakonita kad se temelji na barem jednom od pravnih temelja:

- ako je ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha.
    - 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.
- obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
- obrada je nužna radi poštovanja pravnih obveza voditelja obrade
    - Fizička ili pravna osoba, tijelo javne vlasti, društvo, organizacija, poduzeće ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka.
- obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe; obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade
- obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Izvršitelj obrade Fizička ili pravna osoba, tijelo javne vlasti, društvo, organizacija, poduzeće ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom.

5.3. "Osjetljivi podaci"

Posebne kategorije osobnih podataka su takozvani „osjetljivi podaci", tj. podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje, ili podataka o spolnom životu ili o seksualnoj orijentaciji pojedinca.

Ti se podaci mogu prikupljati i obrađivati pod sljedećim uvjetima:

- dali ste izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha
- ako je obrada nužna za potrebe izvršavanja obveza i ostvarivanja prava voditelja obrade ili vaših prava na području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti
- ako je obrada nužna za zaštitu vaših životno važnih interesa ili životno važnih interesa drugog pojedinca ako fizički ili pravno niste u mogućnosti dati privolu
- ako se obrada provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te pod uvjetom da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s takvim tijelom u vezi s njegovim svrhama i da osobni podaci nisu priopćeni nikome izvan tog tijela bez vaše privole
- ako se obrada odnosi na osobne podatke za koje je očito da ste ih vi objavili
- ako obrada nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad sudovi djeluju u sudbenom svojstvu
- ako je obrada nužna za potrebe značajnog javnog interesa
- ako je obrada nužna u svrhu preventivne medicine ili medicine rada, procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama
- ako je obrada nužna u svrhu javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanja visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda
- ako je obrada nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.

5.4. Zlouporaba podataka

Zlouporabu tuđih osobnih podataka netko čini u svrhu nanošenja drugom štete (povreda ugleda i časti, povreda privatnosti)

Primjer 1: osoba A otvori lažni Facebook profil osobe B, objavi pri tom fotografiju osobe B, njene osobne podatke kojima raspolaže, ime, prezime, dob itd. i potom objavljuje neadekvatan i/ili vulgaran sadržaj na FB profilu koji osobu B prikazuje u negativnom svjetlu.
Osobni podaci mogu se zloupotrijebiti u svrhu počinjenja nekih kaznenih djela, npr. prijevare ili netko iskoristi tuđe osobne podatke u svrhu pribavljanja protupravne koristi, npr. korištenje tuđih osobnih podataka u svrhu sklapanja lažnih ugovora (tzv. krađa identiteta).

Primjer 2: osoba A koristi osobne podatke osobe B u svrhu sklapanja "lažnog" ugovora s nekim teleoperaterom, predstavljajući se kao osoba B, sklopi u njeno ime, a u svoju korist ugovor o pribavljanju broja i mobilnog uređaja, napravi račun koji ne podmiruje, a teret dugovanja padne na osobu B koja sa spomenutim ugovorom nema nikakve veze budući da je isti lažno sklopljen korištenjem njenih osobnih podataka.

Pojedince se može navesti da dostave svoje osobne podatke npr. lažno ih se uvjerava da su osvojili veliko nasljedstvo ili da su osvojili nagradu na nagradnoj igri, a sve u svrhu stjecanja protupravne koristi.

Primjer 3: osoba je na društvenoj mreži dobila obavijest od organizatora nagradne igre da je dobitnik na nagradnoj igri. Kako bi mogla preuzeti nagradu, mora dostaviti presliku prednje i stražnje strane svoje osobne iskaznice. Preslika osobne iskaznica je potom zloupotrebljena za sklapanje lažnog pretplatničkog ugovora na daljinu.

Savjetuje se da s osobnim podacima postupate s osobitom pažnjom, odgovorno i kritički te da iste ne prosljeđujete nepoznatim kao i nedovoljno poznatim osobama ako nemate pouzdane informacije o njihovom identitetu, a naročito ne putem interneta.

Isto tako, ukazujemo da što je veći opseg osobnih podataka koje netko od Vas traži putem interneta (primjerice potpuna preslika osobne iskaznice) to su veće mogućnosti nezakonite objave osobnih podataka, krađe identiteta i drugih zlouporaba osobnih podataka. Imajte na umu da osobnu iskaznicu i podatke sadržane u osobnoj iskaznici imaju pravo i ovlast tražiti samo nadležna tijela i pravne osobe sukladno posebnim propisima i uvjetima poslovanja, tj. policija te davatelji usluga, banke i operatori telekomunikacijskih usluga, a u svrhu nedvojbene identifikacije građana/klijenata (uvid trgovaca kod prodaje alkohola i duhanskih

proizvoda, prijavljivanje kod usluga smještaja, rent-a-car usluge i dr.) Osim toga, osobnu iskaznicu radnika može tražiti i poslodavac pod zakonom propisanim uvjetima.

Također, povrede prava na zaštitu osobnih podataka često se odnose na: objavu osobnih podataka u medijima, objavu osobnih podataka na oglasnoj ploči stambene zgrade, dostave medicinske dokumentacije neovlaštenim osobama, obradu osobnih podataka postavljanjem videonadzornog sustava u zajedničkim prostorijama višestambenih zgrada bez valjanog pravnog temelja, obradu osobnih podataka videonadzornim kamerama u poslovnim prostorijama poslodavaca netočno vođenje osobnih podataka o korisnicima usluga u ovršnim postupcima u svrhu naplate usluga tj. obrada tuđeg OIB-a ili broja identifikacijskog dokumenta kod osoba istog imena i prezimena koji dovodi do netočne identifikacije dužnika i zamjene identiteta osoba, davanje na korištenje osobnih podataka drugim korisnicima bez pravne osnove kao što je primjerice dostava OIB-a suvlasnika potencijalnim upraviteljima zgrade, nepoduzimanje odgovarajućih mjera zaštite osobnih podataka koje banke vode o svojim klijentima od neovlaštenog pristupa i uporabe itd.

Nadzorno tijelo morate obavijestiti o svakoj povredi podataka. Premda je većina propisa u GDPR-u dosta stroga, ponegdje postoje male iznimke. Pada se često vjeruje da je svaku povredu podataka potrebno prijaviti nadzornom tijelu, to nije točno.

Obvezi obavještavanja ne podliježu povrede podataka za koje procijenite da ne nose značajan rizik za slobode i prava oštećenih ispitanika. U praksi to znači da ne morate prijaviti povrede kod kojih gubitak podataka kod osoba za posljedicu može imati samo minornu smetnju. Ako im ne bi značajno smetalo da se ti podaci nađu u 'krivim' rukama, onda se ta povreda smatra beznačajnom. S druge strane, ako možete zamisliti situaciju u kojoj bi se podaci mogli zlorabiti, recimo za krađu identiteta, potrebno je bez odlaganja reagirati i stupiti u kontakt s nadzornim tijelom.

Naravno, ako niste sigurni u važnost oštećenih podataka, kao što pretpostavljamo da će biti slučaj kod malih tvrtki, najbolje bi bilo svejedno prijaviti povredu. Zakonodavci će prije nego GDPR stupi na snagu objaviti konkretne smjernice za određivanje ozbiljnosti povrede. Problem je što su kazne jako velike, pa vas svaka greška može skupo koštati. S druge strane, i u interesu nadzornih tijela je da ih se ne zatrpava podacima o bezazlenim povredama.

Bilo kako bilo, nadzorna tijela o povredama morate obavijestiti odmah, a najkasnije u roku od 72 sata. Za ikakva kašnjenja morate imati dobar razlog te isti potkrijepiti dokazima.

Morate obavijestiti sve osobe čiji su podaci izloženi riziku, u čl.34. st.1. propisuje se da je potrebno obavijestiti sve osobe čiji su podaci izloženi ako bi ta povreda za posljedicu imala veliki rizik po prava i slobode fizičkih osoba, a obavijest morate dati bez odlaganja. Nadalje, obavijest se mora sročiti na jednostavan i lako razumljiv način. Izbjegavajte previše zakonskih pojmova, i nemojte pokušati 'uljepšavati' činjenicu da je došlo do povrede i da postoje rizici. Nadzorna tijela na to zasigurno neće gledati blagonaklono.

Iz gorenavedenog se može iščitati da obavještavanje osoba nije potrebno ako je povreda niskog ili malog rizika po slobode i prava osoba, ali postoje još neke olakotne okolnosti čak i ako ste obvezni obavještavati. Ako povreda podataka obuhvaća velik broj osoba, i ako bi iz tog razloga bilo vrlo nepraktično ili nemoguće obratiti se svakome ponaosob, dovoljnim se smatra i priopćenje putem medija. To može biti izjava za javnost ili obavijest na mrežnoj stranici tvrtke koju će korisnici vidjeti kad se prijave. Pobrinite se da vijest dopre do većine oštećenih osoba. Za tvrtku je osobito važan nastup direktora u javnosti. Imajte na umu da je prag za obavještavanje osoba viši od praga za izvještavanje nadzornog tijela. Kod nekih povreda tako je potrebno obavijestiti nadzorno tijelo, ali ne i osobe. Ako ste koristili adekvatne mjere enkripcije ili pseudonimizacije, onda uopće ne morate obavještavati osobe jer se smatra da su podaci dovoljno osigurani.

Pojam povrede podataka ne odnosi se samo na hakiranje. Pojam 'povreda podataka' zvuči pomalo konfuzno svima koji ga po prvi put čuju jer navodi na dojam da se sve ovo odnosi samo na slučajeve kad hakeri 'upadaju' u sustave i kradu podatke za svoju korist. Međutim, termin se odnosi na „kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani (čl. 4. st. 12.). To znači da se i neodgovorno rukovanje podacima od strane zaposlenika smatra povredom podataka, kao i krađa laptopa, mobitela i sl. koji pripadaju tvrtki. Nepropisno brisanje podataka također u nekim okolnostima može predstavljati povredu (odlaganje nedovoljno uništenih tvrdih diskova i ostalih medija).

Neozbiljno je olako shvaćati problematiku povrede podataka, nastale posljedice je izuzetno kompleskno a nekada i nemoguće riješiti. Teža povreda može ugroziti samu opstojnost tvrtke. Šteta po reputaciju može biti ogromna, čak kao i financijski gubici, odlazak klijenata i gubitak povjerenja. U nekim slučajevima mogu vas i tužiti. Ako na vrijeme ne obavijestite nadzorno tijelo, možete dobiti kaznu od 10 milijuna eura ili 2 % ukupnog godišnjeg prihoda tvrtke, štogod je veće. Kod ozbiljnih prekršaja koji se tiču obrade i zaštite podataka kazne mogu biti i dvostruko veće.

6. ZAKLJUČAK

Zbog velike izloženosti osobnih podataka i nas samih korisnika u virtualnom svijetu, možemo zahvaliti biometriji i biometrijskim tehnologiji koja prepoznaje identifikacijska obilježja našeg tijela na tome da npr. nije više dovoljno posjedovati osobnu kartu i znati osobni identifikacijski broj, već treba i biti osoba kojoj taj dokument pripada. Ta nam tehnologija dodaje još jedan sigurnosni sloj koji kao i sve ostalo ima svoje prednosti i mane. Toliko koliko se ulaže u napredak tehnologije, ona zauzvrat postaje brža i pouzdanija.

Smatram da bi podjednako toliko ako ne i više trebalo ulagati u zaštitu pojedinca, te rigoroznije tj. preciznije postaviti zakonske okvire kao zaštitu od zlouporabe. Štititi korisnike od drugih korisnika je relativno lako, ali ne smijemo zaboraviti štititi masu korisnika od tvrtki i kompanija koje koriste svoje baze biometrijskih obilježja u ponekad ne toliko dobronamjerne svrhe.

Na kraju krajeva ne mogu nam pomoći agencije, nadležna tijela niti zakonske regulative ako se neodgovorno ophodimo sa svojim podacima, i ako se na taj način bespotrebno izlažemo rizicima.

7. Literatura

URL poveznice:

https://mup.gov.hr
https://www.consilium.europa.eu/hr/policies/data-protection-reform/
https://www.youtube.com/watch?v=thd534hJNt0
https://www.youtube.com/watch?v=g4m6StzUcOw
http://spvp.zesoi.fer.hr/seminari/2007/seminari/IgorVasiljevic_Biometrija.pdf
https://urn.nsk.hr/urn:nbn:hr:211:304056
https://policijska-akademija.gov.hr/UserDocsImages/onkd/3_4_2008/radmilovic.pdf
http://biochem.mefos.hr/biokemija
https://www.paymentssource.com/list/6-new-innovations-in-biometric-authentication
http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf
http://www.gradimo.hr/clanak/tehnoloski-noviteti-u-biometriji/37599
http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2006-09-167.pdf
https://www.fer.unizg.hr/_download/repository/Identifikacija_osoba_iz_infracrvenih_fotografija_sarenice_oka%5B1%5D.pdf
https://www.fer.unizg.hr/_download/repository/KDI,_Marija_Marcetic.pdf
http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=107598&lang=en
https://www.millenniumsecurity.co.uk/2020/02/03/innovations-security-technology
https://www.thalesgroup.com/en/markets/digital-identity-andsecurity/government/biometrics/trends-in-biometrics
https://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html

Knjige:

Arjun Singh, 25.12.2019., The Most Iconic Biometric Innovations of 2019

Boban, Marija, „Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu“

Bulatov Y, Jambawalikar S, Kumar P, Sethia S : Hand recognition using geomatric classifi - ers, 1st International Conference on Biometric Authentication (ICBA), Hong Kong, China, July 15-17, 2004. Editors: David Zhang and Anil K. Jain. LNCS 3072, pages 753-759. Springer

Fratrić, Ivan (2011) Biometrijska verifikacija osoba temeljena na značajkama dlana i lica dobivenim iz video sekvenci

Jucheng, Yang (2011) Biometrics

Woodward, D John; Orlans, M Nicholas; Higgins T Peter (2003) Biometrics

Zakoni:

Zakon o zaštiti osobnih podataka (NN br. 103/03, 118/06, 41/08, 130/11, 106/12)

Popis slika

Biometrija kao metoda zaštite podataka

Sažetak

Rad na temu "Biometrija kao metoda zaštite podataka", započinjem pojašnjavanjem pojma biometrije i biometrijskog sustava te kaoko je biometrija napredovala kroz povijest. Nakon toga slijedi raščlamba teme po metodama biometrije i njihovo pojašnjavanje. Potom pojašnjavam zaštitu podataka, zakonodavni okvir te te pravo na zaštitu podataka i kako je ona regulirana u EU. Kao zadnju temu spominjem povredu osobnih podataka, tijelo koje je nadležno za provedbu Opće uredbe o zaštiti podataka, opće uredbe o zaštiti podataka, pojam „osjetljivi podatci“ te zlouporaba podataka, cijeli rad završavam zaključkom.

Ključne riječi: Biometrija, biometrijske metode, biometrijski podaci, GDPR, sigurnost podataka, zaštita podataka, zlouporaba podataka, nadležna tijela, privatnost, povreda privatnosti.

Biometrics as a method of data protection

Summary

The paper on "Biometrics as a method of data protection" begins with an explanation of the concept of biometrics and the biometric system, and how biometrics has progressed throughout history. This is followed by an analysis of the biometric methods and their explanation. Then I explain data protection, the legislative framework and the right to data protection and how it is regulated in the EU. As a final topic, I mention personal data breaches, the body responsible for proof of the General Data Protection Regulation, the General Data Protection Regulation, the notion of "sensitive data" and data misuse, whole paper finishes off with a conclusion.

Key words: Biometrics, biometric methods, biometric data, GDPR, data security, data protection, data misuse, authorities, privacy, privacy breach.