Zaštita osobnih podataka u inteligentnim transportnim sustavima

Martinović, Maroje

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

ZAŠTITA OSOBNIH PODATAKA U INTELIGENTNIM TRANSPORTNIM SUSTAVIMA

THE PROTECTION OF PERSONAL DATA IN INTELLIGENT TRANSPORTATION SYSTEMS

Mentor: dr. sc. Pero Škorput

Student: Maroje Martinović

JMBAG: 0135197583

Zagreb, rujan 2017.

SADRŽAJ

SAŽETAK

Zaštita osobnih podataka podrazumjeva nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka fizičkih osoba. Svrha zaštite osobnih podataka u inteligentnim transportnim sustavima je zaštita privatnog života i ostalih ljudskih prava i temeljenih sloboda u prikupljanju, obradi i korištenju osobnih podataka prilikom korištenja različitih ITS aplikacija. U završnom ovom radu opisani su principi zaštite podataka, kao i načini njihovog prikupljanja u ITS-u. Također opisani su načini obrade i korištenja osobnih podataka u ITS-u te su navedeni primjeri njihove zaštite. Osobne je podatke važno zaštiti u okvirima ITS aplikacija, posebice jer suvremene komunikacijske i informacijske tehnologije otvaraju prostor brojnim zlouporabama, čime se u kritičnoj mjeri ugrožavaju ljudska prava.

KLJUČNE RIJEČI: Zaštita osobnih podataka, biometrija, inteligentni transportni sustav, ITS aplikacije.

SUMMARY:

Personal data protection is based on the oversight over gathering, processing and use of personal data of physical persons. The purpose of personal data protection in intelligent transportation systems is to protect the private life and other basic human rights and freedoms while gathering, process and use personal data for different ITS applications. In this review, the principles of personal data protection are described, as well as the methods they are gathered in ITS. The methods of personal data processing and usage in ITS are also described and several examples of how the data is protected are explained. It is important to protect the personal data within ITS applications, especially because modern communication and information technologies can potentially be misused, critically endangering basic human rights.

KEYWORDS: personal data protection, biometrics, intelligent transportation system, ITS applications.

1. UVOD

U ovom radu je opisana zaštita osobnih podataka u inteligentnim transportnim sustavima. Prema Zakonu o zaštiti podataka osobni podatak je svaka informacija koja se odnosi na fizičku osobu koja je identificirana ili se pomoću takvog podatka može identificirati. Osobni podaci korišteni u identifikaciji mogu biti identifikacijski broj (OIB), ime i prezime i adresa stanovanja, e-mail adresa, podaci o stručnoj kvalifikaciji, radnom mjestu, bankovnim računima, kreditnoj zaduženosti i slično. Pravo na zaštitu osobnih podataka, kao i pravo na privatnost jedno je od najvažnijih ljudskih prava. Ovo temeljno ljudsko pravo, uređeno propisima različitih država koji prate razvoj informacijskih i komunikacijskih tehnologija, dobiva sve više na značaju zbog povećanja učestalosti slučajeva u kojima se krši. Rad je podjeljen šest cjelina:

1. Uvod
2. Zaštita osobnih podataka
3. Inteligentni transportni sustav
4. Biometrija kao primjer zaštite osobnih podataka
5. Aplikacije u ITS-u zasnovane na prikupljanju i doradi osobnih podataka
6. Zaključak.

U drugom poglavlju opisana je važnost zaštite osobnih podataka u okvirima inteligentnog transportnog sustava (eng. Intelligent Transportation Systems, ITS). Kao temeljno ljudsko pravo, zaštita osobnih podataka je uređena nizom različitih zakonskih propisa, a na području Europske Unije (EU) regulirana je odrednicom Europskog parlamenta i Europskog vijeća o zaštiti pojedinaca.

U trećem poglavlju predstavljen je inteligentni sustav. Inteligentni sustav je svaki sustav koji pokazuje sedam osnovnih svojstava. Svojstva govore o sljedećem. Ako neki od pod ciljeva nije ostvariv, inteligentni sustav traži alternativni put prema konačnom cilju sustava. Sustav uči na temelju svojih iskustva, što znači da može prikupljati, prikazivati i upotrebljavati znanje.

Četvrto poglavlje obuhvaća biometriju kao jedan od načina zaštite osobnih podataka. Opisana je obrada i prikupljanje podataka te izdragdnja biometrijskog sustava. Nabrojane su i svaka zasebno opisana biometrijska karakteristika.

U petom poglavlju su prikazane i nabrojane aplikacije u inteligentnom transportnom sustavu. Razina prijetnje i odgovarajuće mjere koje se javljaju za svaku od njih. Također prikazana je analiza ITS aplikacija.

2. ZAŠTITA OSOBNIH PODATAKA

Osobni podatak mora biti zaštićen i osiguran od oštećenja pri prijenosu i od neodobrenog pristupa čime se štiti i javni ili privatni subjekt tog podatka. Inteligentni transportni sustavi u značajnoj mjeri se oslanjaju na prikupljanje i analizu osobnih podataka. Zaštita osobnih podataka u ITS-u jedna je od značajnijih mjera koje treba provoditi od idejne faze pa sve do razgradnje sustava.

Slika 1: Razne aplikacije koje može koristiti vozač u vožnji **Izvor**: www.fleetowner.com

Kako bi na svoje odredište stigli netaknuti i u istom stanju u kojem su poslani, podatke štitimo od oštećenja u prijenosu i neovlaštenih upada ili preusmjeravanja tijekom prijenosa. Također je potrebno zaštiti i podatke koji su spremljeni u našem računalu od neovlaštenih upada treće osobe sa istog ili drugih računala kao i od napada računalnih virusa. Zaštita podataka se ponajviše koristi pri prijenosu podataka osjetljivog sadržaja kao što su npr. vladini dokumenti, bankovni podaci, dokumenti državnih službi, podaci velikih poduzeća itd.

Maskiranje strukturiranih podataka je metoda prikrivanja ili maskiranja određenih podataka u bazama podataka kako bi podaci bili osigurani i korisnikove informacije osjetljivog sadržaja ne bi dospjele izvan ovlaštene okoline. Brisanje podataka je metoda kojom se u potpunosti uništavaju svi elektronski podaci na tvrdom disku ili nekom drugom digitalnom mediju kako bi se osigurali da podaci ili informacije ne procure nakon što se uređaj prestane koristiti. Razvoj pojedinih područja u inteligentnim transportnim sustavima donosi nove i složenije izazove u zaštiti osobnih podataka. Kombiniranjem zaštitnih procesa rizici se mogu smanjiti na minimum. Identifikacija mogućih rizika kojima su osobni podaci

izloženi je prvi korak k rješavanju i sprječavanju potencijalnih problematičnih situacija koje ugrožavaju njihovu sigurnost.

Posebne kategorije osobnih podataka (tzv. „osjetljivi podaci“) koje moraju biti posebno označene i zaštićene odnose se podatke o rasnom ili etničkom podrijetlu, političkim stajalištima, vjerskim ili drugim uvjerenjima, sindikalnom članstvu, zdravlju te spolu i spolnoj aktivnosti. U posebnu kategoriju osobnih podataka spadaju i osobni podaci o kaznenom i prekršajnom postupku.

Ti se podaci mogu prikupljati i obrađivati pod sljedećim uvjetima:

- uz pristanak osobe, te samo u svrhu za koju je osoba dala pristanak
- obrada je određena zakonom, odnosno u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka
- u svrhu zaštite života ili tjelesnog integriteta privatnih osoba
- predmet obrade su podaci koje ste sami objavili
- podatke obrađuje neprofitna organizacija koje je subjekt podatka član
- obrada je potrebna radi uspostave, ostvarenja ili zaštite propisanih zakonom

2.1. Zaštita osobnih podataka u Europskoj uniji (EU)

Razvoj suvremenih informacijskih i komunikacijskih tehnologija doveo je do čitavog niza problema vezanih uz osiguranje zaštite osobnih podataka. Pojava interneta, informacijskih kanala poput YouTubea, razvoj društvenih mreža poput Facebooka, Twittera, on line trgovine omogućili su različite zlouporabe i zadiranja u privatnost pojedinaca. Svaki podatak se moze objaviti i nekontrolirano širiti. Upravo zbog toga je zaštita osobnih podataka globalni problem koji ne može biti reguliran samo propisima nacionalnih zakonodavstava. U tom smislu EU je donijela više različitih propisa. Polazišnu osnovu predstavljaju Povelja o temeljnim pravima Europske Unije iz 2000.g., Konvencija 108. Vijeća Europe iz 1981.g. Europska konvencija o ljudskim pravima (ECHR) iz 1950.g.

Temeljni propis koji regulira zaštitu osobnih podataka u EU je Direktiva Europskog parlamenta i Europskog vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnim protokom takvih podataka (95/46/EZ od 24.10.1995.g).

Ovom direktivom utvrđena su opća pravila o zakonitosti obrade osobnih podataka te određuju prava osoba čiji se podaci obrađuju. Budući da navedena Direktiva uređuje područje koje ima izuzetno dinamičan društveni razvoj, Europska komisija je 2012 predala na raspravu prijedlog Regulacije o zaštiti pojedinaca glede obrade osobnih podataka. Zaštita osobnih podataka obrađenih u okviru policijske i pravosudne suradnje u kaznenim stvarima regulirana je Okvirnom odlukom Vijeća 2008/977/PUP.

Uredba EU 2016/679 Europskog parlamenta i Vijeća od 27.4.2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka stavlja izvan snage Direktive 95/46 EZ .

2.2. Zaštita osobnih podataka u Republici Hrvatskoj (RH)

Zaštita osobnih podataka u RH je ustavna kategorija te je osigurana svakoj fizičkoj osobi u RH bez obzira na državljanstvo i prebivalište, neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili osobinama.

Slika 2: Primjer RH biometrijske putovnice **Izvor:** www.zastita.info

Biometrijska putovnica poznata i e-Putovnica (e-Passport) je vrsta putovnice koja rabi i biometrijske podatke da bi se označio vlasnikov identitet. Podatci se pored zapisa na papiru putovnice zapisuju i u posebnom čipu u kojem se nalaze informacije potrebne radi prepoznavanja geometrije lica, otiska prsta i izgleda mrežnice. Ovu putovnicu je skoro nemoguće krivotvoriti. Iako su se organizacije za zaštitu ljudskih prava odupirale tome da se uvedu biometrijske putovnice, uvelo ih se u većini razvijenih zemalja, ali i u mnogim drugim zemljama. Biometrijska putovnica izdaje se u Republici Hrvatskoj od 1. srpnja 2009. godine.

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

Temeljem ustavne odredbe o zaštiti osobnih podataka donesen je Zakon o zaštiti osobnih podataka (Narodne novine, br. 103/03, 118/06, 41/08, 130/11, 106/12.) kao temeljni akt koji u RH uređuje prikupljanje, obradu, korištenje i zaštitu osobnih podataka te nadzor nad obradom osobnih podataka u RH. Zakon o zaštiti osobnih podataka kao nacionalni standard zaštite osobnih podataka sukladan je najrelevantnijim međunarodnim standardima i načelima zaštite osobnih podataka (Direktiva 95/46/EZ) o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka. Konvencija 108 Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatni protokol uz Konvenciju u vezi nadzornih tijela i međunarodne razmjene podataka. Kao pod zakonski akti u području zaštite osobnih podataka u RH u primjeni su Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (Narodne novine, br. 105/04.) i Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (Narodne novine, br. 139/04.).

2.3. Osobni podatak i svrha zaštite

Osobni podatak je svaka informacija koja se odnosi na fizičku osobu koja je identificirana ili se može identificirati. Osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.

Neki od primjera osobnih podataka su:

- Adresa fizičke osobe;
- Broj telefona;
- E-mail adresa;
- Osobna fotografija;
- Identifikacijski broj/OIB;
- Biometrijski podaci (otisak prsta, snimka šarenice oka);
- Podaci o obrazovanju i stručnoj spremi;

- Podaci o novčanim primanjima;
- Podaci o kreditnom zaduženju;
- Podaci o računima u banci [12].

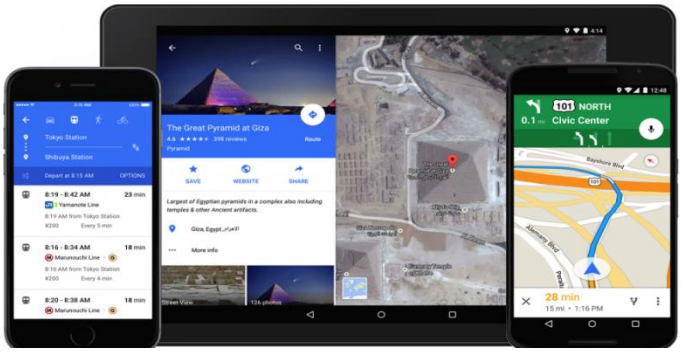
Postoje i posebne kategorije osobnih podataka, takozvani osjetljivi podaci koje se posebno označava i štiti kao npr. rasno podrijetlo, vjerska uvjerenja, podaci o kaznenom postupku. Najčešći oblik zlouporabe privatnosti susreće se na radnom mjestu gdje su granice privatnosti zakonski regulirane. Poslovni prostor u vlasništvu ili u najmu koji služi za rad radnika poslodavac najčešće smatra svojim ograničenim i suverenim prostorom, događa se da propisuje stvara radne uvjete koji direktno negativno utječu na privatnost radnika na radu.

Konvencija za zaštitu pojedinaca pri automatskoj obradi podataka Vijeća Europe iz 1981. u poglavlju II navodi kako će osobni podaci koji prolaze automatsku obradu podataka biti pribavljeni i obrađeni pošteno i u skladu sa zakonom, pohranjeni za određene i zakonite svrhe .Osobni podaci koji otkrivaju rasno podrijetlo, politička mišljenja ili vjerska ili druga uvjerenja, kao i osobni podaci koji se odnose na zdravlje ili spolni život ne mogu se automatski obrađivati, osim ako domaći zakon ne osigura odgovarajuću zaštitu. Isto se odnosi i na osobne podatke koji se tiču kaznene presude (čl. 6 Konvencije).

2.4. Geolokacijske usluge u inteligentnim transportnim sustavima

Postoje usluge temeljene na lokaciji koje više ne rade isključivo sa opcijom da pronađe ljude na zahtjev, ali uključuju aplikacije gdje se oni nalaze. Do njih se dolazi na zahtjev treće strane. Napominjemo da se ljudi mogu locirati čak i ako upotrebljavaju te aplikacije, ali uz uvjet da su povezani na mrežu. Neke od smjernica vezane uz osnovnu zaštitu podataka.

S obzirom na vrlo osjetljivu prirodu obrade podataka o lokaciji, radna će skupina pozvati pružatelje usluga te po potrebi pružiti jasne, potpune i sveobuhvatne informacije o značajkama predloženih usluga.



Slika 3: Primjer aplikacije Google Maps **Izvor:** www.tportal.hr

Google Maps tehnologija besplatnih digitalnih mrežnih karata, koje čine osnovu mnogih servisa i usluga, od pregledavanja satelitskih snimaka, planiranja trase putovanja, lokatora traženih mjesta, itd. opušta jednostavnu implementaciju na različite web stranice, kombiniranje sa drugim aplikacijama. Najkorisnija mogućnost Google Mapsa je skup podataka o cestama i prometnicama sa pripadajućim svojstvima i oznakama, turističkim lokacijama (poput restorana, hotela, parkova), prirodnim i umjetničkim znamenitostima, društvenim lokacijama, geopolitičkim određenjima, itd. Pomoću tih podataka, koji čine digitalno stvoreni sustav karata, može se planirati zamalo bilo što vezano uz putovanje ili transport, od određivanja plana vožnje cestama uz upute o pravcima vožnje, traženja smještaja, određivanja mjesta koja će se posjetiti, najisplativijih pravaca za transport ili pak onih koji pružaju najviše zadovoljstva pri putovanju

Informacije koje su navedene u općim uvjetima i odredbama usluga. Radna skupina preporučuje da davatelj usluga treba dati pojedincima priliku da se savjetuju o informacijama u bilo kojem trenutku i jednostavnom metodom, kao što je putem web stranice ili za vrijeme korištenja usluge.

Suglasnost od strane nositelja podataka treba biti specifična i izričito navedena . U to je uključen pristanak koji se daje kao dio prihvaćanja općih uvjeta i uvjeta pružene usluge elektroničke komunikacije.

Servisi nude uslugu koja zahtijeva automatsko lociranje pojedinca kao npr. mogućnost pozivanja određenog broja za dobivanje informacija o vremenskim uvjetima na određenom mjestu. To je prihvatljivo pod uvjetom da korisnici dobivaju unaprijed sve informacije o obradi podataka o njihovoj lokaciji.

2.5. Prikupljanje osobnih podataka u inteligentnom transportnom sustavu

Osobni podaci mogu se prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom i mogu se dalje obrađivati samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja.

Osobni podaci moraju biti relevantni za postizanje utvrđene svrhe i ne smiju se prikupljati u većem opsegu nego što je to nužno da bi se postigla utvrđena svrha [9].

Pravni temelj za prikupljanje i daljnju obradu osobnih podataka nalazimo u članku 7. ZZOP-a, sukladno kojemu se osobni podaci smiju prikupljati i dalje obrađivati, što podrazumijeva i davanje na korištenje uz dozvolu ispitanika samo u svrhu za koju je ispitanik dao dozvolu ili u slučajevima određenim zakonom ili u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka te u drugim taksativno navedenim slučajevima.

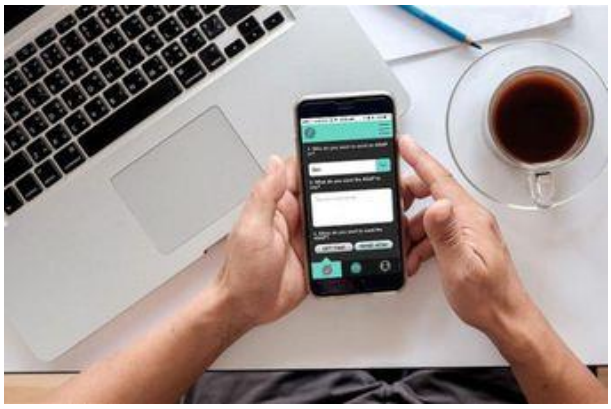
Sukladno članku 11. ZZOP-a, voditelj zbirke osobnih podataka ovlašten je osobne podatke dati na korištenje drugim korisnicima na temelju pisanog zahtjeva korisnika ako je to potrebno radi obavljanja poslova u okviru zakonom utvrđene djelatnosti korisnika. Pisani zahtjev mora sadržavati svrhu i pravni temelj za korištenje osobnih podataka te vrstu osobnih podataka koji se traže.

Zabranjeno je davanje osobnih podataka na korištenje drugim korisnicima za čiju obradu, odnosno korištenje nisu ovlašteni prema odredbama članka 7. ZZOP-a, te ako je svrha za koju se osobni podaci traže na korištenje suprotna prvotnoj svrsi obrade podataka.

Kod obrade osobnih podataka radnika potrebno je uzeti u obzir odredbe posebnih propisa koji uređuju radne odnose u Republici Hrvatskoj, a to je Zakon o radu (Narodne novine, br. 149/09.).

2.5.1. Elektroničko prikupljanje

Voditelj zbirke osobnih podataka obvezan je na svojim internetskim stranicama informirati korisnike/ispitanike čiji se podaci obrađuju o tome da se njihovi podaci koriste u točno određene svrhe i da će se brisati tokom vremena koje je potrebno da bi se ostvarila svrha obrade podataka, osim ako posebnim zakonom nije drukčije određeno.



Slika 4: Elektroničko prikupljanje osobnih podataka **Izvor:** www.zimo.dnevnik.hr

Nije dopušteno slanje elektroničke pošte, u svrhu izravne promidžbe u kojoj se pogrešno prikazuje ili prikriva identitet pošiljatelja ili bez ispravne elektroničke adrese na koju primatelj može, bez naknade, poslati zahtjev za onemogućavanje takvih priopćenja.

2.5.2. Prikupljanje podataka uz privolu

Kako se prikupljanjem osobnih podataka mogu prekršiti temeljne slobode ili privatnost pojedinca Direktivom je propisano kako se ne bi smjeli obrađivati bez izričite suglasnosti pojedinaca na koje se odnose osim kada se podaci koriste za posebne potrebe. Predviđena je mogućnost da države članice ovlaštene, kada za to postoji opravdani javni interes za odstupanje od zabrane obrađivanja osjetljivih kategorija osobnih podataka, posebice u područjima kao sto su javno zdravstvo i socijalna zaštita.

2.5.3. Prikupljanje podataka bez privole

Bez suglasnosti korisnika, osobni podaci smiju se prikupljati i dalje obrađivati u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka. Zatim u svrhu zaštite života ili tjelesnog integriteta korisnika ili druge osobe u slučaju kada ispitanik fizički ili pravno nije u mogućnosti dati svoj pristanak. Osobni podaci se smiju prikupljati bez pristanka i ako je obrada podataka nužna radi ispunjenja zadataka koji se izvršavaju u javnom interesu ili u izvršavanju javnih ovlasti koje ima voditelj zbirke osobnih podataka. Također, podaci se smiju prikupljati ako je korisnik sam objavio svoje podatke.

2.6. Obrada i korištenje osobnih podataka ITS aplikacija

Obrada osobnih podataka je svaka radnja ili skup radnji izvršenih nad osobnim podacima, automatskim sredstvima ili drugim, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima [13].

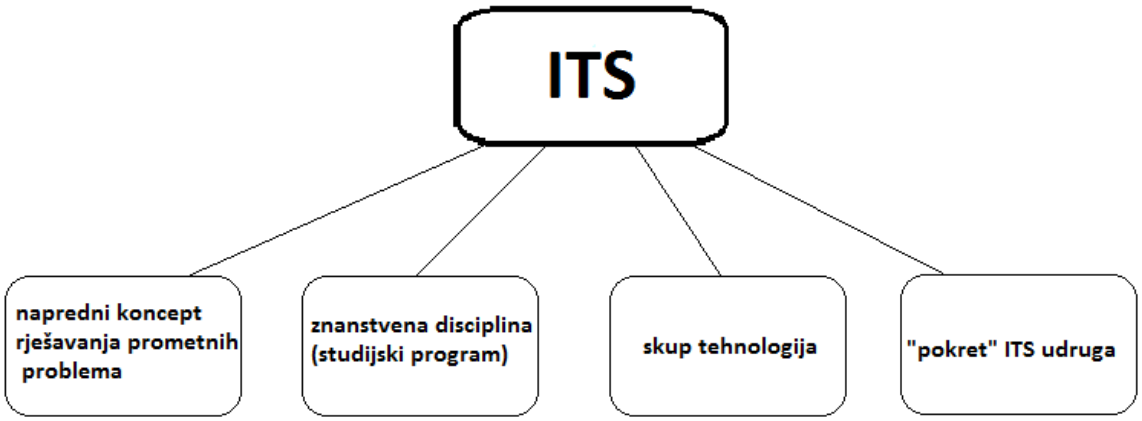
Osobni podaci smiju se prikupljati i dalje obrađivati uz privolu osobe čiji se podaci prikupljaju (prema Zakonu o zaštiti osobnih podataka) ili u slučajevima određenim zakonom. Prikupljanje osobnih podataka predstavlja, primjerice, vođenje evidencija o zaposlenicima, vanjskim suradnicima, klijentima, dobavljačima kao i vođenje drugih sličnih evidencija i popisa fizičkih osoba.

Obrada osobnih podataka najčešće se povjerava izvršitelju obrade osobnih podataka u slučajevima zbirke podataka koje vode primjerice državna i gradska tijela i drugi veliki sustavi kao i u slučajevima iznošenja osobnih podataka iz RH u svrhu njihove obrade u inozemstvu.

3. INTELIGENTNI TRANSPORTNI SUSTAVI

Inteligentni transportni sustavi (ITS) su holistička, upravljačka i informacijsko-komunikacijska nadgradnja klasičnog sustava prometa i transporta kojim se postiže znatno poboljšanje odvijanja prometa, učinkovitiji prijevoz putnika i roba, poboljšanje sigurnosti u prometu, udobnost i zaštita putnika, manje onečišćenje okoliša i slično. Osobne je podatke važno zaštiti u okvirima sustava inteligenih transportnih sustava (ITS), posebice jer suvremene komunikacijske i informacijske tehnologije otvaraju prostor brojnim zlouporabama, čime se u kritičnoj mjeri ugrožavaju ljudska prava. Uz pomoć rješenja ITS aplikacija, koje svakodnevno koristimo u ove svrhe, postiže se bitno veća propusnost, sigurnost, zaštićenost i ekološka prihvatljivost prometnih i transportnih sustava.

Rezultat povećane motorizacije, urbanizacije, porasta broja stanovnika te promjene naseljenosti sela je zagušenje prometa u cijelom svijetu. Zagušenje prometa smanjuje učinkovitost prometne infrastrukture, produžuje vrijeme putovanja, povećava zagađenje zraka i potrošnju goriva. Kako bi se spomenute posljedice mogle izbjeći, sve se više ulaže u područje ITS-a.



Slika 5: Temeljna značenja termina ITS [8]

Inteligentni sustav je svaki sustav koji pokazuje sedam osnovnih svojstava. Svojstva govore o sljedećem. Ako neki od pod ciljeva nije ostvariv, inteligentni sustav traži alternativni put prema konačnom cilju sustava. Sustav uči na temelju svojih iskustva, što znači da može prikupljati, prikazivati i upotrebljavati znanje. Također sustav koristi velike količine znanja jer mora biti slična količini znanja koju posjeduje čovjek, da bi riješio kompleksni problem. Pokazuje svojstava svjesnosti jer ima sposobnost objašnjavanja svojeg ponašanja, nadgledanja

i dijagnoze stanja te oporavka u slučaju pogreške. Čovjek na prijateljski način može komunicirati sa sustavom prirodnim jezikom i govorom. Ono što je od posebne važnosti je to su da sustav tolerira pogreške i nejasnoće u komunikaciji, te odgovara u stvarnom vremenu.

Osim navedenih svojstava inteligentni sustav ima funkcije prikupljanja i obrade informacija, interakcije s vanjskim svijetom, komunikacije s čovjekom i s drugim inteligentnim sustavima, prikupljanja znanja, rukovanja znanjem, obrade znanja i zaključivanja, ali i planiranja.

Cjelokupan životni ciklus ITS-a prikazan na slici 5. počinje od definiranja zahtjeva i specifikacija te operativnog koncepta gdje se zatim funkcionalnom dekompozicijom i fizičkom sintezom izgrađuje sustav koji se nakon toga evaluira i modificira, upotrebljava i održava da bi se na kraju povukao i razgradio.

3.1. Komunikacijska ITS arhitektura

Arhitektura (grč. Architekton, „glavni zidar“, „glavni graditelj“), je temeljna organizacija inteligentnog sustava koja sadrži ključne komponente, njihove odnose i veze prema okolini te načela njihova dizajniranja i razvoja promatrajući cijeli životni ciklus sustava. Komunikacijska arhitektura predstavlja dio fizičke arhitekture ITS-a i služi kao alat za realiziranje postavljenih ciljeva razvoja, kompatibilnosti i interoperabilnosti te omogućava širenje i modernizaciju sustava uz prihvatljive troškove. Ona definira i opisuje načine na koje se razmjenjuju informacije između različitih dijelova sustava i to korištenjem fizičke razmjene podataka koja je određena fizičkom arhitekturom. Generički pristup koji daje okvir za rješavanje važnih pitanja, predstavlja temelj komunikacijske arhitekture, a vodi ka uspješnom dizajniranju učinkovitih ITS rješenja. Sustav za podršku fizičke razmjene podataka objedinjuje rješavanje dva veoma bitna problema.

- Prvi problem predstavlja osiguravanje sredstva koja omogućuju prijenos podataka sa jednog mjesta na drugo na način pogodan za naš sustav u smislu troškova, korištenja i promjene.
- Drugi problem je odstupanje od strane primatelja što uzrokuje potrebe za standardizacijom protokola.

Europska komunikacijska ITS arhitektura upućuje na moguće rješenje ovih dvaju bitnih pitanja. Kada se uzmu u obzir ostale komponente Europske ITS arhitekture, komunikacijska arhitektura mora ostati tehnološki što neovisnija. Telekomunikacijske tehnologije se mijenjaju, napreduju velikom brzinom. Komunikacijska arhitektura kao i ostale Europske ITS arhitekture, teži ka tehnološkoj neovisnosti. Zbog brzog razvoja tehnologije nije moguće osigurati arhitekturu koja će biti temeljena na tehnologiji koja će dugoročno vrijediti.

Kod sustava upravljanja priljevnim tokovima u Europi uvriježeno je korištenje protokola za sigurnu komunikaciju i prijenos podataka TLS (engl. Transport Layer Security), dok se kod američkih sustava češće koristi protokol za državnu transportnu komunikaciju za inteligentne transportne sustave (engl. The National Transportation Communications for Intelligent Transportation System Protocol, NTCIP) .

3.2. Normizacija ITS usluga i zaštita osobnih podataka

ITS usluge normizirane su na međunarodnoj razini. Međunarodna organizacija za standardizaciju ISO početno je normizirao ITS usluge fokusirane na cestovni promet 1990. godine dokumentom ISO TR 14813-1 -Transport information and control systems — Reference model architecture(s) for the TICS sector. Njime je definirano osam funkcionalnih područja. Nova klasifikacija dolazi 1999. godine kada su na prijašnjih osam usluga dodane još tri nove usluge. Funkcionalna područja ITS-a su nabrojana i kratko objašnjena.

Područje vozila sadrži više usluga kojima se poboljšava operativna sigurnost vozila. Poboljšanje vidljivosti, asistencija vozaču i automatske radnje vozila, sprječavanje sudara, sigurnosna upozorenja neke su od njih.

Prijevoz tereta podrazumijeva upotrebu komercijalnih vozila, multimodalnu logistiku te međusobnu koordinaciju prijevoznika i drugih sudionika uključenih u proces prijevoza tereta. Primjeri usluga su upravljanje informacijama o prijevozu tereta, menadžment intermodalnih centara, upravljanje opasnim teretima, automatska provjera dokumenata i težine vozila.

Javni prijevoz skup je više usluga koje omogućuju redovite i učinkovite radnje javnog prijevoza uz pružanje ažurnih informacija korisnicima. Kao primjer tih usluga navest ćemo napredni sustav javnog prijevoza, praćenje voznog parka, napredni sustavi, zajednički

transport, automatska provjera nesreće, automatski poziv u slučaju nesreće te koordinirano upravljanje vozilima žurnih službi.

Usluge žurnih službi objedinjuju procese koji omogućuju brzu i efikasnu intervenciju hitne pomoći, policije, vatrogasaca i drugih žurnih službi. Sve više se integrira s upravljanjem incidentnim situacijama.

Elektronička praćenja vezana za transport su elektronička naplata javnog prijevoza, elektronička naplata cestarine, elektronička naplata parkiranja te daljinska plaćanja.

Osobna sigurnost u cestovnom transportu su usluge nadzor i zaštita u vozilima javnog prijevoza, kolodvorima i sl., sustav nadzora pješaka, sustav upozorenja o radovima na cesti i itd. Nadzor vremenskih uvjeta i okoliša su usluge nadzora vremenskih prilika na cestama, nadzora onečišćenja, nadzora razine vode ili leda, itd.

Upravljanje odzivom na velike nesreće povezuje usluge vezane za prirodne nesreće. Usluge koje pruža su jedinstveni pozivni broj, upravljanje podacima o velikim nesrećama, koordinacija žurnih službi i sl.

U području nacionalne sigurnosti i zaštite razvijaju se usluge koje omogućuju identifikaciju opasnih vozila, nadzor kretanja opasnih tvari, nadzor cjevovoda itd. Kao posljedica stvaranja ovog područja najbitniji su razni teroristički napadi kao npr. 11. rujna 2001. Kada je počinjen višestruki teroristički napad otimanjem putničkih zrakoplova u Sjedinjenim Američkim Državama.

3.3. Preporuke za zaštitu osobnih podataka u ITS-u

Vrste problema s kojima se susreću dioničari vezano uz zaštitu podataka i privatnosti ovisi o njihovim gledištima. Podaci pojedinačnih osoba često imaju još jedan ugao. No općenito se smatra da bi svi profitirali ako:

- je zaštita osobnih podataka prikladno obrađena u osnovnim uslugama i aplikacijama
- su dostupne jasne metode, pravila i pristupi kojih se treba pridržavati
- nove usluge koje pridodaju efikasnosti, sigurnosti i ugodnosti nisu nepotrebno ograničene

- se pojedinci osjećaju informirano i sigurno u svoju privatnost prilikom korištenja novih usluga i aplikacija.

Slika 6: Informacijske tehnologije **Izvor:** www.narodni-list.hr

Kako bi ovi ciljevi unutar područja informacijskih tehnologija (IT) bili ostvareni, potrebno je mnogo više koordinacije i suradnje.

Europska komisija bi trebala pokrenuti inicijativu za pripremu konkretnih smjernica zaštite osobnih podatka za specifičnu primjenu i aspekte ITS-a. Takve smjernice bi trebala imati predložak za procjenu učinka na privatnost za ITS-ove aplikacije i usluge. Osim što jasno opisuje metodu i postupak (PPI), po mogućnosti bi također ova inicijativa trebala uključivati smjernice za metode i kriterije privatnosti po dizajnu, PET-ove,sigurnosne mjere te kodeks prakse. Takav generički PPI obrazac mora biti upotpunjen prilagođenim smjernicama za aplikaciju ili područje aplikacije koje je od velike važnosti iz perspektive zaštite osobnih podataka. Industrija i potrošačke organizacije bi trebale biti pozvane na sudjelovanje u razvoju PPI obrasca. Članak 29 Radna skupina bi se također trebala pozvati kako bi dala savjete, pregledala rezultate i konačno podržala ishod.

Posebnu pažnju treba posvetiti:

1. Naplati korisnicima ceste na proširenim mrežama, uključujući osobne automobile
2. E-kartama u javnom prijevozu
3. Osiguranju „plaćaj kako voziš“
4. Podacima o plutajućem vozilu

5. Politici i mehanizmima za pristanak korisnika na usluge koje su isporučene ili omogućene na platformama u vozilima, rješavajući pri tom pitanja različitih vozača ili putnika koji koriste automobil i različitih aplikacija koje dijele jednu platformu u automobilu
6. Pravilima, metodama, alatima i kriterijima za pohranu geolokacijskih podataka i uzoraka mobilnosti u neosobne svrhe (npr. predviđanje prometa, urbanističko planiranje, analiza izvedbe vozila).
7. Utjecaju dijeljene odgovornosti za zaštitu podataka u ITS servisnim lancima s višestrukim ili zajedničkim procesorima i kontrolorima.

Europska komisija bi trebala potvrditi da je stručno znanje zaštite podataka uključeno u standardizacijske radne skupine i ITS zajednice za istraživanje i razvoj, jer iste su temelj i građevni blokovi na kojima će se realizirati privatnost po dizajnu ili arhitektura povećanja privatnosti. Europska komisija bi trebala to raspravljati s normizacijskim tijelima i ITS zajednicom za istraživanje i razvoj i trebala bi to uključiti kao uvjet prilikom izdavanja mandata za razvoj standarda u posebnim područjima ITS-a [13].

4. BIOMETRIJA KAO PRIMJER ZAŠTITE OSOBNIH PODATAKA

Biometrija je tehnika za autentikaciju ili ovjeru autentičnosti fizičkih osoba koristeći njihove jedinstvene fizičke karakteristike.

Jedan od jednostavnijih primjera biometrijske ovjere bi bila korisnička prijava na računalo, ne standardnim unošenjem korisničkog imena (user name) i lozinke (passworda), već da se korisnikov identitet potvrdi nečim jednostavnim za njega i različitim od drugih ljudi tj. korisnika.

Danas najčešće korištene osobine u biometrijskoj ovjeri su otisak prsta, geometrija šake i lica, izgled šarenice oka i druge osobine su jedinstvene svaku osobu.

Biometrija nalazi široku primjenu u informatičkoj sigurnosti i informatici generalno. Biometrija u širem smislu predstavlja statističko proučavanje bioloških fenomena, odnosno to je primjena matematike i statistike u razumijevanju živih bića. Biometrija se u užem smislu može definirati kao znanost koja se bavi istraživanjem mogućih prepoznavanja osoba na temelju njihovih fizičkih i ponašajnih karakteristika.

Tablica 1: Pregled biometrijskih karakteristika:

Fizičke	Otisak prsta, slika lica, dlan, rožnica, šarenica, termogram lica, termogram tijela, uho
Ponašajne	Potpis, boja glasa, dinamika tipkanja, miris, hod
Tvrde	Otisak prsta, šarenica, DNA, termogram lica
Meke	Visina, bojakose, težina, bojaočiju
Kontaktne	Otisak prsta, dlan, rožnica, šarenica, potpis, hod
Nekontaktne	Slika lica, glas, dinamika tipkanja, miris

Idealna različita razina prepoznavanja i zaštite bila bi potpuno prepoznavanje bilo koje slike iz bilo kojeg ugla, prepoznavanje bilo koje osobe u stvarnom vremenu, posjedovanje velike baze podataka s biometrijskim podacima, pristup velikoj bazi podataka sa podacima DNK svih živih bića uključujući osobe, biljke, životinje itd. Dostupnost svih tehnologija policijskim snagama i pravnim tijelima.

Dok u realnosti slika ovisi o utjecaju svjetla, kutu izuzimanja slike, veličini (primjerice lica), kvaliteti slikane slike i slike iz baze podataka itd. Za obradu u realnom vremenu u izuzimanju i procesiranju slike potrebni su suvremeni računalni resursi. Neki od sustava za prepoznavanje lica danas su u evaluaciji za alat koji će se koristiti za prepoznavanje počinitelja odnosno u zakonom propisane svrhe [5].

4.1. Načela primjene biometrijskih karakteristika u ITS aplikacijama

U samim počecima biometrije prednost je davana fizičkim karakteristikama u odnosu na karakteristike ponašanja itd. Kao glavni razlog bila je uočljivost i mišljenje da su fizičke karakteristike pouzdanije od karakteristika ponašanja.

Primjena kontrole pristupa danas je, zahvaljujući brzom razvoju računarske industrije praktično neograničena, zato spominjemo samo neke od niza mogućnosti:

- evidencija radnog vremena zaposlenika;
- evidencija posjetitelja i izvođača radova;
- kontrola ulaza u štićeni objekt;
- kontrola ulaza na parkirališta;
- kontrola pristupa u sve prostorije od posebne važnosti;
- nadzor obilazaka čuvarske ili neke druge nadzorne tehnološke službe;
- kontrola kretanja cjelokupnim štićenim prostorom i implementacija s drugim sustavma zaštite, kao što su sustav video nadzora, protuprovalni, protuprepadni i sustav zaštite od požara.

Danas su one ravnopravne te su podjednako zastupljene. Neke biometrijske karakteristike su razvijene, a uz neke koje su još u fazi razvoja cilj je imati preko 50-tak biometrijskih karakteristika.

Svaka karakteristika može biti niskog, srednjeg ili visokog rizika. U donjim tablicama su neke od najčešćih karakteristika koje koristimo.U tablici 1 data je usporedba biometrijskih karakteristika s obzirom na svoju univerzalnost, jedinstvenost i trajnost koje imaju potencijal primjene u ITS-u.

Tablica 1: Usporedba karakteristika s obzirom na univerzalnost, jedinstvenost i trajnost.

KARAKTERISTIKA	UNIVERZALNOST	JEDINSTVENOST	TAJNOST
Lice	VISOKA	NISKA	SREDNJA
Otisak prsta	SREDNJA	VISOKA	VISOKA
Geometrija dlana	VISOKA	SREDNJA	SREDNJA
Šarenica	VISOKA	VISOKA	VISOKA
Mrežnica	VISOKA	VISOKA	SREDNJA
Termogram	VISOKA	VISOKA	NISKA
Uho	SREDNJA	SREDNJA	VISOKA
Potpis	NISKA	NISKA	NISKA
Glas	SREDNJA	NISKA	NISKA
Dinamika tipkanja	NISKA	NISKA	NISKA
Miris	VISOKA	VISOKA	VISOKA

Modificirano prema [5]

Tablica 2: Usporedba karakteristika s obzirom na prikupljivost, izvedljivost, prihvatljivost i nadmudrivanje.

KARAKTERISTIKA	PRIKUPLJIVOST	IZVEDLJIVOST	PRIHVATLJIVOST	NADMUDRIVANJE
Lice	VISOKA	NISKA	VISOKA	NISKO
Otisak prsta	SREDNJA	SREDNJA	SREDNJA	VISOKO
Geometrija dlana	VISOKA	SREDNJA	SREDNJA	SREDNJE
Šarenica	SREDN JA	VISOKA	NISKA	VISOKO
Mrežnica	NISKA	VISOKA	NISKA	VISOKO
Termogram	VISOKA	SREDNJA	VISOKA	VISOKO
Uho	SREDNJA	SREDNJA	VISOKA	SREDNJE
Potpis	VISOKA	NISKA	VISOKA	NISKO
Glas	SREDNJA	NISKA	VISOKA	NISKO
Dinamika tipkanja	SREDNJA	NISKA	SREDNJA	SREDNJE
Miris	NISKA	NISKA	SREDNJA	NISKO

Modificirano prema [5]

Ove biometrijske karakteristike možemo koristiti i u prometu. Tehnologija napreduje i automobili su danas sve napredniji. Neke biometrijske karakteristike zahtjevaju skupu tehnologiju za svoju primjenu, dok neke zahtjevaju relativno mala ulaganja.

Sustav za pokretanje motora pomoću otiska prsta predstavlja revoluciju u automobilskoj tehnologiji. Kako bi se postigla potpuna sigurnost, uređaj se može programirati samo jedanput, najviše za četiri osobe. Svaka daljnja izmjena moguća je jedino kupnjom nove elektroničke kartice, isključivo kod ovlaštenog prodavača, nakon temeljite provjere identiteta vlasnika. Svako odstupanje od propisane procedure potpuno blokira sustav, te je deblokiranje moguće jedino u ovlaštenom servisu. Na taj način je spriječena neželjena uporaba automobila

Slika 7: Otisak prsta umjesto ključa za auto **Izvor:** www.autoportal.hr

4.2. Otisak prsta u ITS aplikacijama

Danas većina mobilnih uređaja sadrži aplikaciju koja očitava otisak prsta za otključavanje mobilnog uređaja. Otisak prsta u je uzorak izbočina i udubljenja na površini jagodice prsta, a nastaje sakupljanjem mrtvih, otvrdnulih stanica, koje se neprekidno u slojevima ljušte sa površine prsta. Oblik i formacija otiska ovise o prvotnim uvjetima razvoja embrija. Otisci prstiju su jedinstveni za svaki prst osobe, uključujući i jednojajčane blizance. Koriste se za identifikaciju već čitavo stoljeće i vrijednost takve identifikacije vrlo je dobro dokazana.

Slika 8: Mobilni uređaj koji koristi otisak prsta za otključavanje uređaja **Izvor:** www.iphoneeinstein.com

Uzorci pora i brazdi od trenja individualnih otisaka prstiju su jedinstveni za tu osobu. Otisci prstiju su jedinstveni za svaki prst osobe, uključujući i jednojajčane blizance. Jedna od komercijalno najdostupnijih biometrijskih tehnologija, uređaji za raspoznavanje otisaka prstiju za stolna i prijenosna računala, su sada široko dostupni od strane mnogih proizvođača. S tim uređajima, korisnici više ne trebaju unositi zaporke - umjesto toga, samo dodir pruža trenutni pristup računalu ili mobilnom uređaju.

Sustavi za otiske prstiju mogu se također koristiti identifikaciju. Nekoliko država u SAD-u provjerava otiske prstiju kod prijava ljudi za socijalne povlastice, kako bi osigurali da prijavljeni ne dobiju povlastice pod krivotvorenim imenima. Država New York ima preko 900 000 ljudi upisanih u takav sustav.

Slika 9: Digitalni predložak otiska prsta [9]

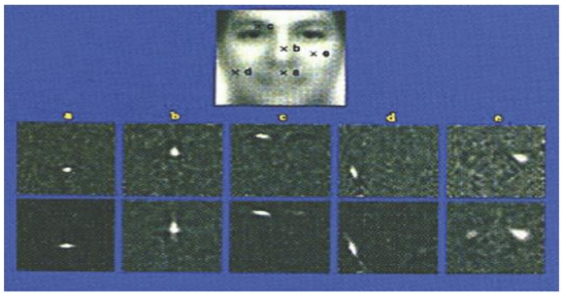
Uređaji za raspoznavanje otisaka prstiju za desktop i laptop pristup su sada široko dostupni od mnogih proizvođača po niskim cijenama. Sa tim uređajima, korisnici više ne trebaju utipkavati lozinke umjesto toga, samo dodir pruža trenutni pristup računalu. Kako bi se spriječilo korištenje umjetno napravljenih otisaka prstiju neke osobe, mnogi sustavi uz skeniranje otiska mjere i protok krvi. Korištenje više prstiju u procesu prepoznavanja eksponencijalno povećava sigurnost metode.

4.3. Prepoznavanje lica u ITS aplikacijama

Ova biometrijska tehnologija je jedna od jeftinijih metoda jer ne zahtijeva skupu specijalnu opremu. Dovoljni su osobno računalo i video kamera što je pristupačno gotovo svakome. U praksi je dovoljno da osoba prođe pored kamere i da ju sustav zabilježi, dok se prepoznavanje osobe obavlja pomoću prepoznavanja oblika lica. Pri analizi uzorka slike zahtijeva se izdvajanje ključnih indikatora kao što su karakteristični odraz, određivanje relativne važnosti indikatora kroz izbor njihovih koeficijenata važnosti i njihovog međusobnog djelovanja. Sustavi za raspoznavanje lica imaju primjenu u različitim područjima kao što su: video telefonija, kompresija baza slika, pristup računalnim resursima, kriminalističke svrhe itd.

Slika 10: biometrijska tehnologija za prepoznavanje lica na aerodromu u Amsterdamu **Izvor:** www.travelmagazine.rs

Početna faza prepoznavanja skenira odraz lica u različitim mjerilima i onda ocjenjuje po ključnim indikatorima segmente odraza lica i pod određenom vjerojatnošću određuje da li se radi o odrazu lica ili okoline. U drugoj fazi se određuje položaj glave što mora uzrokovati određene korekcije prilikom prepoznavanja i zahtijeva korekcije x, y i z osi. Neki sustavi za raspoznavanje lica zahtijevaju mirno poziranog korisnika kako bi mogli dohvatiti sliku, iako mnogi sustavi koriste proces u realnom vremenu za detektiranje glave osobe i lociraju lice automatski.



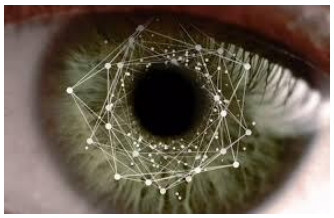
Slika 11: Biometrijski uzorak prepoznavanja lica **Izvor:** www.gao.gov

Tehnologija prepoznavanja lica identificira osobe prema specifičnim djelovima njihova lica koja su manje podložna promjenama. To su gornje crte očnih šupljina, površina oko

obraza i strane usta. Ovi sustavi za identifikaciju, sliku lica dobivaju pomoću kamera. Tako dobivena slika se generira i uspoređuje sa referentnim obrascem pohranjenim u bazi podataka.. Ova tehnologija također može uspoređivati slike lica koje se nalaze u digitaliziranim putovnicama (eng. biometric passport), sa obrascima iz baze podataka. Ova se tehnologija također može koristiti za verifikaciju i identifikaciju osoba.

4.4. Skeniranje oka u ITS aplikacijama

Prepoznavanje osoba pomoću šarenice je jedna od najsigurnijih biometrijskih metoda, najviše zbog prirodnih karakteristika šarenice.



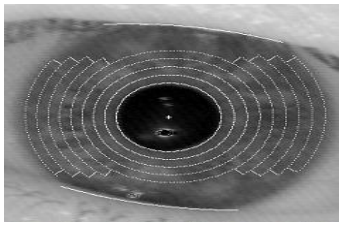
Slika 12: Skeniranje šarenice [5]

Šarenica poprima svoj izgled u najranijem djetinjstvu (čak i prije rođenja), te se ne mijenja, osim u slučaju bolesti ili ozljede. Kirurški ju je nemoguće krivotvoriti, barem ne bez velikog rizika od gubitka vida. Također se ova metoda ne može prevariti nošenjem kontaktnih leća, jer postoje algoritmi pomoću kojih se jasno ustanovljuje nosi li osoba leće ili ne.

Sama je tehnika vrlo jednostavna i učinkovita, te ima potencijal postati vodećom biometrijskom tehnikom budućnosti. Uzorci šarenice prenose se preko video - baziranog sustava za uzimanje slike. Uređaji za skeniranje šarenice koriste se u autentifikaciji osoba već više godina. Sustavima baziranim na raspoznavanju šarenice smanjila se je cijena, a očekuje se da će taj trend i dalje rasti. Tehnologija radi dobro i za verifikaciju i identifikaciju. Ona je ujedno i najsigurnija biometrijska karakteristika i radi toga se aktivno istražuje njeno područje primjene. Eventualni problem je korisnička prihvatljivost. Jer oko je jedno od osjetljivijih organa tijela.

Slika 13: Vojska koristi metodu skeniranja oka **Izvor**: www.dvidshub.net

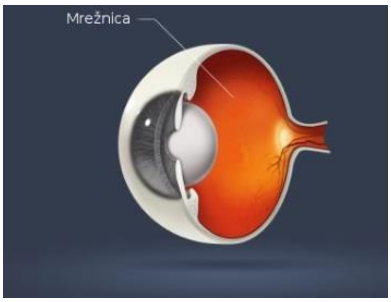
Skeniranje rožnice je tehnologija koja se najviše koristi prilikom kontrole ulaska osoba u neki zatvoreni ili ekskluzivni prostor, vođenju statistike posjetitelja, a slične varijante su i u upotrebi prilikom skeniranja korisničkih dokumenata. Prepoznavanje uzorka se odvija pomoću kamere koja snima zapis o rožnici korisnika, a pod pretpostavkom da je svaka jedinstvena, može se koristiti u smislu jednoznačnog označavanja.



Slika 14: Izgled predloška rožnice opisan točkama [9]

Dobivena slika rožnice se pomoću specijalnih programa opisuje pomoću točaka koje jednoznačno opisuju uzorak. Pomoću tehnologije opisivanja rožnice moguće ju je opisati s 242 jedinstvene točke, dok je npr. u tehnologiji prepoznavanja otiska prstiju predložak moguće opisati s 7 do 22 točaka. Što više neka biometrijska karakteristika sadrži jedinstvenih opisnih točaka to je prepoznavanje točnije i preciznije.

Mrežnica je tanki sloj stanica koji se nalazi sa stražnje strane oka. Mrežnica oka i njena struktura je karakteristika svake individualne osobe. Ovo je jedna od sigurnijih biometrijskih metoda jer nije jednostavno promijeniti ili replicirati unutarnju strukturu oka. Prva istraživanja ove metode počela su oko 1930. g. , a prva komercijalna izvedba se pojavila 1984. g. Ova biometrijska metoda do danas osigurava najveću točnost prepoznavanja.

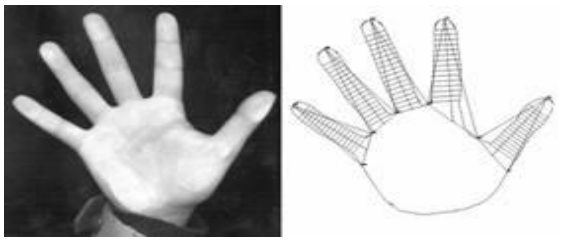


Slika 15: Mrežnica oka [14]

Ima veliku primjenu u vojnim objektima, te područjima visokog stupnja sigurnosti: policijske postaje, zatvori, nuklearne elektrane, osjetljivi laboratoriji i dr.

4.5. Geometrija šake u ITS aplikacijama

Biometrijska ovjera temeljena na raspoznavanju karakteristika šake dostupna je već više od dvadeset godina. Fizičke karakteristike šake ili prstiju uključuju dužinu, širinu, debljinu i površinu područja šake. Jedna od korisnih aspekata ovog pristupa je to što neki sustavi zahtijevaju mali biometrijski uzorak.



Slika 16 : Uzorak šake opisan krivuljama **[9]**

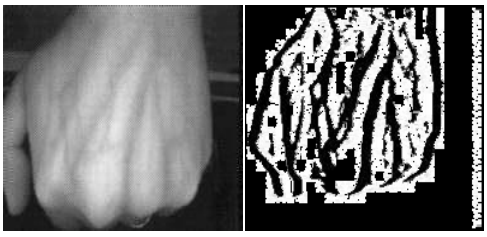
Geometrija šake je postigla prihvatljivost u dosegu aplikacija pa se često može uočiti u kontroli fizičkog pristupa u komercijalnim i rezidencijalnim aplikacijama, u vremenskim i poslužiteljskim sustavima te u generalnim aplikacijama za osobnu verifikaciju.

Slika 17: Primjer uređaja za skeniranje geometrije dlana **Izvor:** www.gradimo.hr

Ovu tehnologiju najčešće susrećemo u zračnom prometu za provjeru putnika. U početku se odnosila samo na stalne međunarodne putnike, ali sve veći zahtjevi za sigurnošću proširili su upotrebu na sve građane. Da bi putnici mogli koristiti ovu tehnologiju morali su registrirati svoj biometrijski uzorak, a za uzvrat su dobili magnetsku karticu. Nakon dolaska putnika na aerodrom putnik provuče magnetsku karticu kroz magnetski čitač i stavi ruku na uređaj za mjerenje dlana. Zatim sustav provjerava identitet u policijskoj i imigracijskoj bazi podataka. Ako je identitet potvrđen uređaj izdaje karticu pomoću koje putnik prolazi kroz kontrolu putovnica.

4.6. Provjera vena u ITS aplikacijama

Zapisi o biometrijskom opisu vena se koriste kao dodatni dio u jednoznačnom opisivanju osobe. Vene su veliki, nepromjenjivi i uglavnom skriveni predlošci. U kombinaciji s geometrijom ruke ili tehnologijom opisivanja otiska prstiju postiže se vrlo visok stupanj točnosti prepoznavanja osobe. Ova tehnologija se može koristiti i prilikom fizičke kontrole prolaska kao inteligentna vrata, brave i ostale fizičke barijere koje dolaze u kontakt s rukama korisnika.



Slika 18: Digitalizirani predložak vena dobivenih infracrvenim spektrom [9]

Japanske banke, na primjer, koriste ovu tehnologiju, što je usklađeno sa zakonom. Kamere za prepoznavanje uzorka vena se obično koriste i infracrvenim senzorom jer on prodire kroz tkivo ispod kojeg su vene te raspoznaje detalje koji nisu vidljivi ljudskom oku.

4.7. Potpis ili rukopis u ITS aplikacijama

Svaka osoba ima jedinstven rukopis koji se može iskoristiti tako da identificira tu osobu. Rukopis se zajedno sa potpisom razvija tijekom vremena. Uzastopni uzorci su različiti zato ne postoje potpunija preklapanja istih. Ovo je ujedno nenametljiva tehnika koju koristimo u svakodnevnom životu. No postoje i neki problemi poput pouzdanosti, načina izuzimanja koji mogu biti statički ili dinamički itd.

Slika 19: Potpis opisan krivuljama i njihovim međusobnim odnosima **[**9]

Identitet osobe se može potvrditi analizom vlastoručnog potpisa ili rukopisa. Tehnologija ovjere je bazirana na mjerenju brzine, pritiska i kuta koje koristi osoba kada se potpisuje ili kada piše određeni tekst.

Slika 20: Primjer potpisa u elektroničkom obliku**Izvor:** www.gradimo.hr

Jedno od smjerova prema kojima se je usredotočila ova tehnologija su i ebusiness aplikacije, ali i druge aplikacije gdje je potpis prihvaćen kao metoda osobne autentifikacije.

4.8. Glas u ITS aplikacijama

Karakteristike ljudskog glasa potpuno su određene vokalnim traktom, ustima, nosnom šupljinom i ostalim mehanizmima za stvaranje glasa u ljudskom tijelu koji se razvija tijekom vremena. Ovo spada pod nenametljivu tehniku koja ima problem pouzdanosti, bolesti, mutacija, senzora, jedinstvenosti itd.

Prepoznavanje glasa koristi se u svrhu ovjere različitih korisnika na temelju njihovih jedinstvenih glasovnih karakteristika. Naime, da bi se identitet korisnika potvrdio, isti mora izgovoriti neki tekst koji je prethodno izgovorio i koji je spremljen u bazu podataka. Ljudi uglavnom različito izgovaraju iste rečenice (tonalitet, brzina, prekidi), pa je stupanj jedinstvenosti među korisnicima vrlo visok. Ipak, ukoliko bi netko snimio ovlaštenu osobu, isti bi ju mogao i reproducirati pa je stoga ovu metodu ovjere potrebno koristiti u kombinaciji s drugim metodama. Danas je tehnologija prepoznavanja glasa dostupna na većini raspoloživih osobnih mobilnih uređaja u svrhu bržeg uspostavljanja telefonskih poziva.

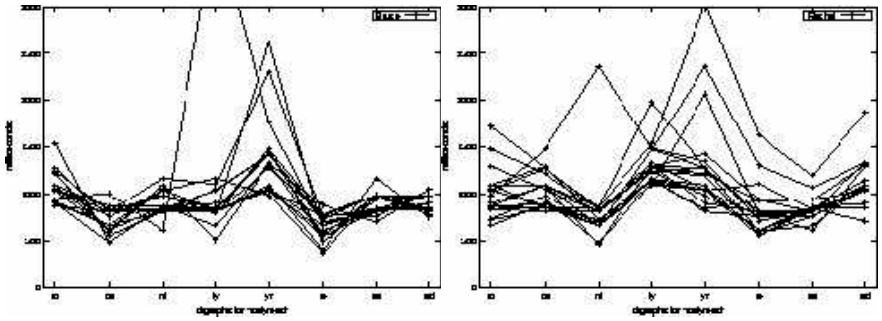
Prepoznavanje glasa ima i druge namjene kao što je prebacivanje glasovno izgovorenih riječi u tekstualni zapis. Postupak prepoznavanja govora se u tom slučaju sastoji od toga što se izgovorene riječi u kratkom vremenu unutar računala prepoznaju i prikazuju na zaslonu. Najnoviji programi za prepoznavanje govora omogućuju prepoznavanje tzv. prirodnog ili kontinuiranog govora koji ne zahtijevaju korištenje pauze između svake riječi već se izgovaraju prirodnim tokom dok računalni algoritam pokušava identificirati izgovoreno. Riječi se trenutno prikazuju na zaslonu i unutar nekog tekstualnog dokumenta. Moguće je diktirati paragrafe, slati elektroničku poštu, stvarati izvještaje i pisma te sve to i tekstualno obrađivati.

Svrha tehnologije prepoznavanja govora na prethodno navedeni način je povećanje produktivnosti korisnika. Koristeći se tehnologijom prepoznavanja govora moguće je raditi brže i efikasnije nego što je to moguće klasičnim načinom utipkavanja teksta u računalo.

4.9. Dinamika tipkanja u ITS aplikacijama

Ova tehnika se razvila tijekom II. svj. rata u radiotelegrafskoj komunikaciji jer je uočeno da se po brzini tipkanja mogu razlikovati pošiljatelji poruka. Kao tehnika je vrlo nenametljiva jer nije potrebno uvoditi nikakve dodatne uređaje za detektiranje, osim zvučne

kartice. Eventualno je moguće posjedovati i specijalizirani program koji bi na razini operativnog sustava pratio korisnikovo tipkanje. Glavna karakteristika na kojoj se ova tehnika bazira je vremenski razmak između korisnikovog pritiskanja na tipkovnicu [9].

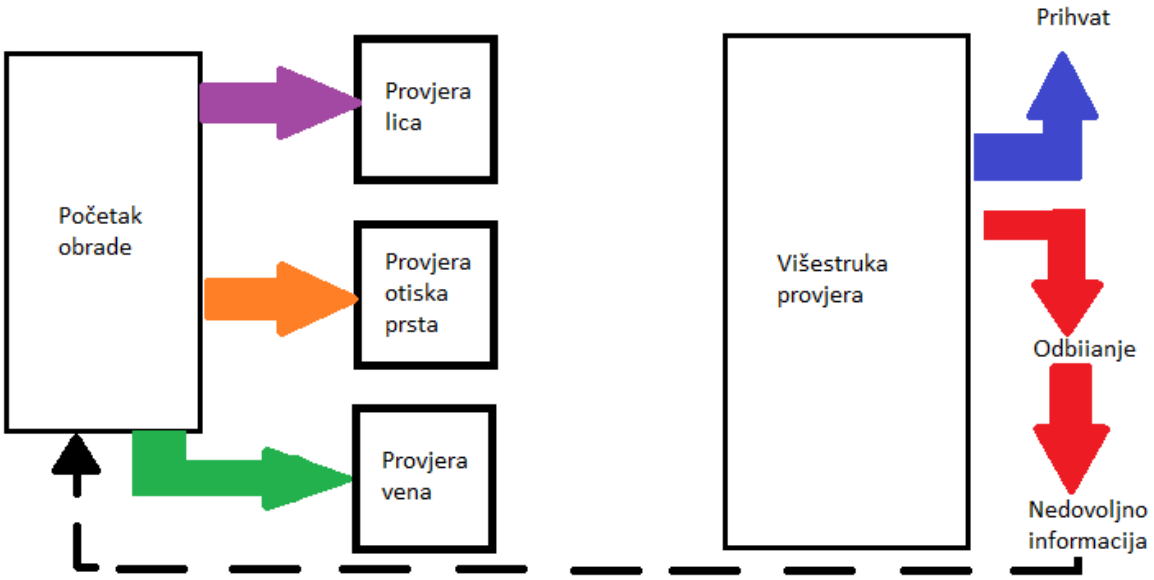


Slika 21: Grafički prikaz brzine tipkanja iste riječi od strane dvije različite osobe **[9]**

Danas dok govorimo o dinamici tipkanja onda se podrazumijeva dinamika tipkanja po pisaćoj tipkovnici.

4.10. Multimodalna biometrija

Multimodalna biometrija podrazumijeva kombiniranje svih prethodno navedenih biometrijskih tehnika. Ukoliko se u praksi koristi veći broj prethodno nabrojenih tehnika, može se izgraditi jedan sigurni biometrijski sustav. Multimodalni biometrijski sustavi se koriste na državnim graničnim prijelazima za kontrolu ulaska ili izlaska, za kontrolu pristupa nekom prostoru, civilnoj identifikaciji, mrežnoj sigurnosti itd.



Slika 22: Primjer multimodalne biometrije u carinskoj kontroli **[9]**

Multimodalna biometrija se koristi i kao potpora standardnim postupcima za provjeru identiteta ili ukoliko iz izvornih dokumenata i zapisa nije moguće dobiti dovoljan broj podataka kojima bi se opisala neka osoba. Preporuča se kombinacija standardnih sigurnosnih mehanizama i biometrijskih metoda jer uvijek postoji mogućnost zloupotrebe izolirane metode. Ovako se s većom mogućnošću može utvrditi kako se doista radi o toj osobi ili se može detektirati slučaj pokušaja krađe identiteta.

5. APLIKACIJE U ITS-U ZASNOVANE NA PRIKUPLJANJU I DORADI OSOBNIH PODATAKA

ITS je upravljačka i informatičko-komunikacijska nadgradnja klasičnog prometnog i transportnog sustava, tako što se postiže bitno veća propusnost, sigurnost, zaštićenost i ekološka prihvatljivost u odnosu na rješenja bez ITS aplikacija. Potrebno je prikupiti dovoljno podataka i obraditi ih u stvarnom vremenu. ITS je potrebno promatrati kao kompleksan "sustav sustava".

Razvoj inteligentnih sustava se može pratit kroz nekoliko osnovnih razvojnih područja:

- navigacijski sustavi,
- sustavi kontrole i bezgotovinske naplate,
- sigurnosni sustavi,
- prometni kontrolni i upravljački sustavi,
- održavanje,
- javni promet,
- komercijalni prijevoz,
- pješački promet,
- obilazni putovi za izvanredne situacije [15].

Stanovnik europskog grada izgubi prosječno jednu godinu života u dodatnim čekanjima zbog prometnih zagušenja. Možemo reći da ITS predstavlja napredni koncept rješavanja prometnih problema, znanstvenu disciplinu, skup tehnologija i novi tehnološki pokret.

Sustavi podržani telematikom koriste suvremena računala, informacijske i komunikacijske tehnologije kako bi se povećala mobilnost, sigurnost i zaštita okoliša. Cilj primjene telematskih sustava je stvaranje komunikacije između korisnika i onoga tko upravlja transportnim sustavom. Upotrebom telematike sustavom prometa se upravlja u realnom vremenu, od korisnika prometa se dobiva trenutačan odgovor, a na moguću promjenu u dobivaju se trenutačne reakcije.

5.1. Digitalni tahograf

Nadzorni uređaj koji se najviše koristi u praćenju vozila je digitalni tahograf. On osigurava upis vremena vožnje, vrijeme provedeno u obavljanju profesionalne aktivnosti bez

upravljanja vozilom, vrijeme odmora, brzinu kretanja vozila i prijeđenu udaljenost vozila. Digitalni tahograf je propisan kao obavezan. Prema zakonu o radnom vremenu, obveznim odmorima mobilnih radnika i uređajima za bilježenje u cestovnom prijevozu određeno je tko mora imati ugrađen digitalni tahograf, u cilju boljeg nadzora nad cestovnim prijevozom. Uvedena je personalizirana pametna kartica umjesto zapisnih listića analognih tahografa.

Slika 23: Digitalni tahograf [16]

GPS profesionalni uređaj se spaja na digitalni tahograf u vozilu, te se tako u sustav povlače svi podaci s digitalnog tahografa temeljem kojih se dobivaju korisni izvještaji. Digitalni tahograf bilježi prijeđeni put i brzinu vozila, identitet vozača, aktivnost vozača, podatke o kontroli, kalibraciji i popravku tahografa, uključujući identifikaciju radionice, događaje i kvarove.

Pretjerana obrada podataka u ovoj aplikaciji čini se kao najrelevantnija prijetnja. Sljedeća prijetnja je nezakonita sekundarna uporaba.

Mjere za poboljšanje privatnosti za ovu aplikaciju su: minimiziranje podataka, razdvajanje domene i distribuirana obrada.

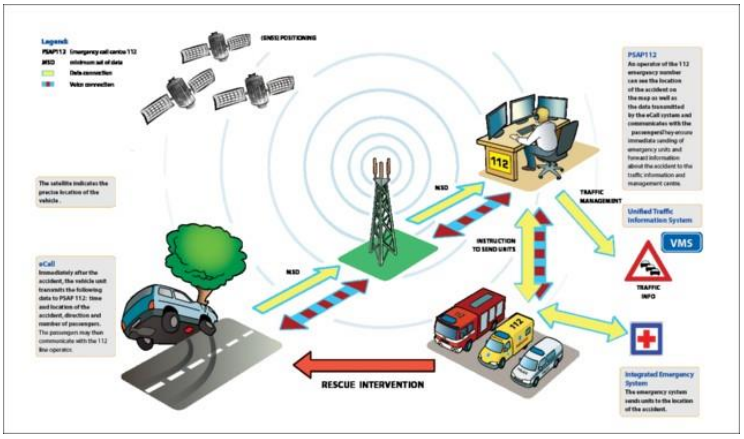
5.2. E- poziv

E-poziv je nova usluga bazirana na tehnologiji žurnog poziva 112. Ima za cilj povećati sigurnost prvenstveno u cestovnom prometu. Od 2015. svi novi modeli automobila proizvedeni za tržište Europske Unije morati će imati podršku za e-Poziv, dok će se u ostala vozila ta podrška, u obliku crne kutije, morati ugraditi do 2020. Crna kutija omogućiti će da u trenutku prometne nesreće, automobil sam automatski nazove broj 112, te za vrijeme prvih nekoliko sekundi poziva u Centar 112 prenese osnovne informacije o vozilu. Te informacije uključuju, primjerice, broj putnika, vrstu goriva te još niz drugih podataka. Najvažniji podatak

je precizna lokacija prometne nesreće, koja se dobiva GPS uređaja. Nakon što prenese podatke, koji su odmah vidljivi operateru u Centru 112, uspostavlja se glasovna komunikacija između centra i sudionika u vozilu.

Slika 24: Primjer e-poziva u automobilima **Izvor:** www.autoportal.hr

Po normama, cijeli proces, od nesreće do alarmiranja žurnih službi, smije trajati najviše 12 sekundi. E-poziv kao javni servis, besplatan za sve građane, bez obzira na vrstu vozila ili njegove nabavne cijene, će doprinijeti tom zajedničkom cilju smanjenja smrtnosti i ozbiljnosti ozljeda.



Slika 25: Prikaz e-poziva i interakcije između korisnika sa odgovarajućom institucijom **Izvor:** http://www.heero-pilot.eu

Prijetnja je prekomjerna obrada podataka, što znači da se obrađuje više podataka nego što treba u tom slučaju. Rizik je klasificiran kao srednji.

Mjere za ovu aplikaciju su: minimiziranje podataka i mehanizmi pristanka korisnika.

5.3. E - karte u javnom prijevozu

U proteklim desetljećima uvelike je uvedena zbirka elektroničkih zbirki u sustavima javnog prijevoza diljem Europe. Uvedene su sheme u većim gradovima poput Londona i Pariza. Neke od prednosti e - karte u javnom prijevozu su potpunije informacije za strateško planiranje javnog prijevoza, veće stope prilagodbi uz manje napore, veća fleksibilnost u tarifnim postavkama, više opcija za profiliranje i marketing, jednostavnost korištenja usluge. Sve što omogućuje bolju uslugu, bolju sliku javnog prijevoza može kao rezultat privući nove korisnike.

Područja prijetnji su neovlašteni pristup osobnim podacima, prisluškivanje. Ponovna uporaba osobnih podataka izvan zakonskih okvira ili izvan opsega pristanka korisnika. Prekomjerna obrada.

Mjere od posebne važnosti: anonimizacija, razdvajanje domene, mehanizmi pristanka korisnika.

5.4. Sustav naplate parkiranja

Uredjaji za obavljanje razlicitih elektronickih i novcanih transakcija. Modularne arhitekture i primjenjivi za niz podrucja primjene. Ti uređaji su jednostavni za rukovanje i odrzavanje, sadrže višejezično korisnisko sucelje, otporni su na klimatske utjecaje i vandalizam, prilagodljivi su hendikepiranim osobama. Također imaju mogućnost za više načina naplate poput plačanja kovanicama, kontaktnim i bezkontaknim karticama, mobilnim telefonima.

Slika 26: Razne vrste automata za naplatu parkiranja [11]

Automati za naplatu parkiranja izdaju papirnate karte za plaćanje određenog iznosa za određeno vrijeme parkiranja. Zbog nadzora nad parkiranjem, kartice moraju biti smještene na

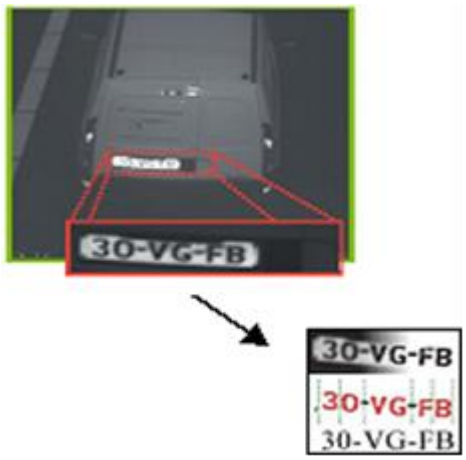
vidljivo mjesto. Posljednjih godina traže se rješenja koja bi smanjila količinu gotovine u aparatima, smanjenju prijevara, povećanju učinkovitosti izvršenja naplate te povećanje udobnosti korisnika automobila.

Područja prijetnji su: neovlašteni pristup osobnim podacima, ponovna uporaba osobnih podataka i prekomjerna obrada.

Odgovarajuće mjere: minimiziranje podataka, razdvajanje domene, brisanje podataka odmah nakon početne obrade, distributivna obrada, kontrola predmeta podataka.

5.5. Kontrola brzine

Kontrola brzine je metoda provođenja brzine koja uključuje niz fotoaparata instaliranih preko puta ceste. Slika koja nastane sadrži registarsku pločicu vozila i odgovarajuću vremensku oznaku. Na temelju izdvajanja registracije vozila oznake, zapisi o ulasku i izlasku se podudaraju.



Slika 27: Princip očitanja oznaka sa tablica **Izvor:** www.peek.hr

Na mjernim točkama vozila se detektiraju i snimaju te se vrši automatsko optičko prepoznavanje registarskih tablica. Podaci sa mjernih točaka šalju se centralnom serveru koji na osnovu podataka o vozilu, vremenu i pređenom putu računa prosječnu brzinu svih vozila na svakoj dionici.

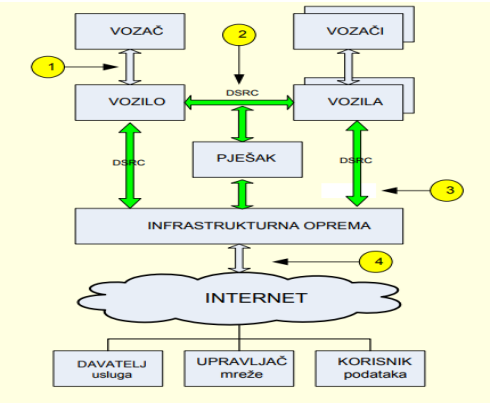
Slika 28: Primjer sustava koji regulira brzinu kretanja na cestama **Izvor:** www.prometna-signalizacija.com

Područje prijetnje je ponovno korištenje osobnih podataka izvan zakonskih okvira.

Mjere su: brisanje podataka odmah nakon početne obrade, distribuirana obrada.

5.6. Kooperativni sustavi

Sustavi suradnje pripadaju u posebnu kategoriju, jer ih se ne može smatrati jednom aplikacijom već neograničen broj aplikacija kojima je zajednička komunikacija sa drugim vozilima ili sustavima na cesti. Kooperativni sustav je kombinacija tehnologija, ljudi i organizacija koji olakšava komunikaciju i koordinaciju potrebnu da neka grupa učinkovito obavlja razne djelatnosti za ostvarenje zajedničkog cilja. Danas je većina aplikacija vezana uz sigurnost prometa ili sa upravljanjem prometa. Svako vozilo treba biti u stanju komunicirati sa bilo kojim drugim vozilom i sustavima na cesti. Standardizacija sustava je još u tijeku iako je do sada postignut značajan napredak.



Slika 29: Osnovni koncept kooperativnih sustava [17]

Kooperativni inteligentni transportni sustavi (engl. Cooperative Intelligent Transport Systems) obuhvaćaju napredne tehnologije koje omogućuju vozilima i okolnoj infrastrukturi. Imaju mogućnost da razmjenjuju informacije o lokaciji, brzini i smjeru s ostalim korisnicima. Potrebe za mobilnošću u svakodnevnom životu dovode do kontinuiranog povećanja prometa koji generira ozbiljne probleme u smislu zagušenja, sigurnosti i utjecaja na okoliš

Razina prijetnje su neovlašteni pristup osobnim podacima i ponovna uporaba osobnih podataka izvan zakonskih okvira ili izvan opsega korisničkog pristanka.

Mjere: pseudonimizacija, minimiziranje podatka, mehanizmi pristanka korisnika, brisanje odmah nakon početne obrade, distributivna obrada.

5.7. Praćenje vozila

Praćenjem priključnih vozila ona se identificiraju u transportnom sastavu, pozicioniraju, te je upravljanje njima lakše, bolje se integriraju u prijevozne operacije, veći je stupanj iskorištenja, praćenje temperature tereta sa mogućnošću signaliziranja u slučaju pada ili rasta, ispod ili iznad dozvoljene vrijednosti npr.kod hladnjača, i moguće je praćenje rada u prethodnom periodu. Na taj način se smanjuje broj priključnih vozila, povećava se iskorištenost priključnih vozila, prati se kretanje visokotarifne robe, u slučaju krađe omogućava se praćenje ukradene robe i priključnih vozila, daljinsko utvrđivanje temperature tereta bez obzira gdje se priključno vozilo nalazi, praćenje poslane robe čak i kada je ona isporučena od strane prijevoznika.

Slika 30: Nadzor vozila EOL fleet sustavom koji omogućuje on-line nadzor i interakciju s vozilima [18]

Sustav EOL fleet omogućuje online nadzor i interakciju s vozilima te pruža informacije ključne za razumijevanje učinaka vozila i radne snage. Moguće ga je prilagoditi za svaku tvrtku bez obzira na broj vozila. Usluga djeluje kao inteligentna, fleksibilna i kompaktna infrastruktura koja objedinjuje više naprednih tehnologija. Vozila opremljena ovim sustavom primaju GPS signal i podatke o vozilu te ih sigurnom konekcijom razmjenjuju s kontrolnim centrom.

5.8. Analiza aplikacija u ITS-u

Rezultati analiza sličnosti i razlike između različitih aplikacija u načinu obrade osobnih podataka, zakonodavstva, arhitekture i prijetnji privatnosti. U nastavku su opisane analize pojedinih aplikacija u ITS-u pomoću tablica. U tablici 4 analizirano je sedam ITS aplikacija s obzirom na pravnu osnovu i tipove prijetnji. Zelena boja predstavlja slabu prijetnju, žuta predstavlja srednji tip prijetnje i crvena boja koja predstavlja visoki tip prijetnje.

Tablica 4: Pravne osnove i razina tipa prijetnji ovisno o aplikaciji [13]

APLIKACIJA		**PRIJETNJA TIPA**		
broj	**ime**	**T1**	**T2**	**T3**
1	digitalni tahograf	**SLABA**	**SLABA**	**SREDNJA**
2	e-poziv	**SLABA**	**SLABA**	**SREDNJA**
3	e-karte u javnom prijevozu	**SREDNJA**	**VISOKA**	**VISOKA**
4	sustav naplate parkiranja			
4a	internet sustav naplate parkiranja	**SLABA**	**SREDNJA**	**SLABA**
4b	sustav naplate parkiranja pomoću automata	**SLABA**	**SREDNJA**	**SLABA**
5	područje kontrole brzine	**SLABA**	**SREDNJA**	**SLABA**
6	kooperativni sustavi	**VISOKA**	**VISOKA**	**SREDNJA**
7	praćenje vozila	**SREDNJA**	**SREDNJA**	**VISOKA**

Modificirano prema [13]

Legenda tablice:

T1 Neovlašteni pristup osobnim podacima, prisluškivanjem, neovlaštenim djelovanjem osoblja, sjeckanjem itd.

T2 Ponovno korištenje osobnih podataka izvan zakonski definiranih granica ili izvan opsega suglasnosti nositelja podataka.

T3 Pretjerana obrada, tj. obrada više osobnih podataka nego što je potrebno za tu svrhu.

Tablica 5 sadrži sedam aplikacija i ukupno osam mogućih mjera za poboljšanje privatnosti. Prikazuje nam za svaku aplikaciju posebno koje su sve mjere moguće za poboljšanje privatnosti namjenjene baš za tu aplikaciju.

Tablica 5: Pregled mogućih mjera za poboljšanje privatnosti po aplikaciji [13]

APLIKACIJA		**Moguće mjere za poboljšanje privatnosti**							
BROJ	**IME**	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**
1	digitalni tahograf			■	■			■	
2	e- poziv			■		■			
3	e- karte u javnom prijevozu	■			■	■			
4	sustav naplate parkiranja								
4a	sustav naplate parkiranja internetom				■		■		
4b	sustav naplate parkiranja automatom				■		■		
5	područje kontrole brzine						■	■	
6	kooperativni sustavi		■	■		■	■	■	
7	praćenje vozila			■					■

Modificirano prema [13]

Legenda:

M1 - anonimizaciju. Podaci se više ne mogu pratiti na fizičkoj osobi ili na vozilu.

M2 - pseudonimizaciju. Ulaženje u trag podatku je smanjeno pomoću privremenih indentiteta.

M3 - minimiziranje podataka.

M4 - razdvajanje domena, tj. podaci se obrađuju u odvojenom obliku domene. Nisu dostupni identifikacijski podaci. Druga domena obrađuje samo podatke o korištenju.

M5 - mehanizme pristanka korisnika. To su mehanizmi koji korisniku pružaju veću kontrolu i svijest koji se podaci obrađuju za koje svrhe.

M6 - brisanje podataka odmah nakon početka obrade

M7 - distribuiranu obradu. To je obrada najosjetljivijih i najdetaljnijih podataka.

M8 - kontrolu predmeta podataka u kojoj korisnik može kontrolirati detaljne osobne podatke koji su pohranjeni. Može brisati podatke djelomično ili potpuno i sam odlučuje hoće li poslati podatke ili ne.

ITS aplikacije nam pomažu u našem svakodnevnom životu poput e-poziva koji nam spašava živote u prometu zbog brzine reakcije hitnih službi. Aplikacija praćenja vozila koja u svakom trenutku prati naše vozilo i pomoću koje povećavamo iskorištenost vozila, možemo pratiti temperaturu u hladnjačama te u krađi vozila ili robe možemo točno locirati gdje se nalazi.

Svakim danom se nadograđuju stare aplikacije, a isto tako se razvijaju nove. Sa unapređenijim sustavima i tehničkim mogućnostima. Svaka od njih prikuplja i obrađuje osobne podatke koje se ovisno o aplikaciji nalaze u nižem, srednjem ili visokom tipu prijetnje, te ih je potrebno zaštititi. Moguće mjere za poboljšanje privatnosti su: anonimizacija, pseudonimizacija, minimiziranje podataka, razvijanje domena, mehanizmi pristanka korisnika, brisanje podataka, distribuirana obrada, kontrola predmeta podataka kojom korisnik sam kontrolira detalje svojih osobnih podataka.

6. ZAKLJUČAK

Uz pomoć rješenja ITS aplikacija, koje svakodnevno koristimo, postiže se bitno veća propusnost, sigurnost, zaštićenost i ekološka prihvatljivost prometnih i transportnih sustava. Funkcija ITS sustava je prikupljanja i obrade informacija, interakcije s vanjskim svijetom, komunikacije s čovjekom i s drugim inteligentnim sustavima, prikupljanja znanja, rukovanja znanjem, obrade znanja i zaključivanja, ali i planiranja.

U ITS aplikacijama susrećemo neke biometrijske karakteristike koje mogu biti dominantne te ujedno i razvijenije. Neke su još u fazi razvoja. Većina mobilnih uređaja sadrži aplikaciju koja očitava otisak prsta za otključavanje mobilnog uređaja. Ona je jedna od komercijalno najdostupnijih biometrijskih tehnologija, uređaji za raspoznavanje otisaka prstiju za stolna i prijenosna računala koja i u budućnosti ima prostora za široku primjenu.

Prepoznavanje lica u ITS-u je jedna od jeftinijih metoda jer ne zahtijeva skupu specijalnu opremu, te spada u nenametljivu tehnologiju. Imaju primjenu u različitim područjima kao što su: video telefonija, kompresija baza slika, pristup računalnim resursima, kriminalističke svrhe itd.

Skeniranje oka u ITS aplikacijama je jedna od najsigurnijih biometrijskih metoda, jednostavna i vrlo učinkovita. U isto vrijeme javljaju se problemi sa korisničkim prihvačanjem, jer je oko osjetljiv dio tijela. Koriste se u vojnim objektima te zahtjevaju nešto skuplja ulaganja. Skeniranje oka ima potencijal postati vodećom biometrijsom tehnikom budućnosti.

Još jedna dominantna tehnika koju koristimo svakodnevno i električnim putem je metoda rukopisa ili potpisa. Nenametljiva je metoda no isto tako i nepouzdana. Jedno od smjerova prema kojima se usredotočila ova tehnologija su financijske aplikacije.

Geometrija šake je tehnologija koju primjenjujemo već više od dva desetljeća. Najveća prednost joj je što zahtjeva mali biometrijski uzorak. Možemo ju naći nekim u aplikacijama.

Najveća mogućnost zaštite i sigurnosti dobijamo kombinacijom dvije ili više biometrijskih tehnologija. Preporuča se kombinacija standardnih sigurnosnih mehanizama i biometrijskih metoda jer uvijek postoji mogućnost zloupotrebe izolirane metode.

ITS je upravljačka i informatičko- komunikacijska nadgradnja klasičnog prometnog i transportnog sustava kojom se postiže veća propusnost, sigurnost, zaštićenost. I prije je postajala inteligencija u prometu, ali uz ITS aplikacije koje prikupljaju i obrađuju podatake dok su umrežene sa distribucijom informacija postižu znatno smanjenje zagušenja, čekanja

prometnih nesreća, neučinkovitosti prijevoza itd. Sa ciljem poboljšanja kretanja ljudi, robe i informacija. Taj cilj se još poboljšava i razvija.

Pravo na zaštitu osobnih podataka, kao i pravo na privatnost jedno je od najvažnijih ljudskih prava. Ovo temeljno ljudsko pravo, uređeno propisima različitih država koji prate razvoj informacijskih i komunikacijskih tehnologija. Zaštita osobnih podataka u ITS-u jedna je od značajnijih mjera koje treba provoditi od idejne faze pa sve do razgradnje sustava. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

LITERATURA

1 Zakon o zaštiti osobnih podataka, Narodne novine br. 103/03, 118/06, 41/08, 130/11, 106/12

2 Klarić, M.: Zaštita osobnih podataka i europska konvencija za zaštitu ljudskih prava i temeljnih sloboda; Zbornik radova Pravnog fakulteta u Splitu, 4/2016.

3 Zakon o radu ,Narodne novine,br. 149/09

4 URL: http://azop.hr/images/dokumenti/217/zastita_op_rh.pdf. (pristupljeno: rujan 2017.)

5 Škorput, P.: Računalna sigurnost,Autorizirana interna predavanja, FPZ, Zagreb, 2015.

6 Klir, G.J.: Architecture of Systems Problem Solving, Plenum Press, New York, 1985.

7 Klir, G. J.: Facets of Systems Science, Plenum, New York, 1995.

8 Bošnjak, I.: Inteligentni transportni sustavi- ITS 1,FPZ, Sveučilište u Zagrebu, Zagreb, 2006.

9 URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2006-09-167. (pristupljeno: rujan 2017)

10 URL: https://hr.wikipedia.org/wiki/Biometrija, (pristupljeno: rujan 2017.)

11 URL: http://www.echo.hr/fixpark0.htm (pristupljeno: rujan 2017.)

12 Milt, K.: Zaštita osobnih podataka, Kratki vodič o EU-u, Europski parlament, 06.2017.

13 Eisses S, van de Ven T, Fievée A; ITS Action Plan; FRAMEWORK CONTRACT TREN/G4/FV-2008/475/01; ITS & Personal Data Protection; Final Report;; 20121004_ITS AP5 1_D5 Final Report v1.0 SEI.docx; Amsterdam, October 4th, 2012

14 URL: http://www.optometrija.net./anatomija-oka/mreznica (pristupljeno: rujan 2017.)

15 Kovačević, D.: et al.:Razvoj telematike i njezina primjena u prometu, FPZ, Sveučilište u Zagrebu, Zagreb, 1993.

16. URL: http://www.tahograf.hr/clanak/nova-generacija-digitalnih-tahografa-vdo-dtco-1381-verzija-14/hr-1-71-3.html (pristupljeno: rujan 2017.)

17. Mandžuka, S.: Što su kooperativni sustavi?, Fakultet prometnih znanosti, Sveučilište u Zagrebu, 2013

18. URL: http://www.vidi.hr/Lifestyle/Business-3.0/EOL-Fleet-Inteligentni-sustav-nadzora-flota-vozila (pristupljeno: rujan 2017.)

19. URL: http://www.its-croatia.hr/index.php?option=com_docman&task (pristupljeno: rujan 2017.)

POPIS KRATICA

ITS (intelligent transportation system) inteligentni transportni sustav

EU (European Union) Europska Unija

RH (Republic of Croatia) Republika Hrvatska

TLS (Transport Layer Security) kriptografski protokoli

NTCIP (The National Transportation Communications for Intelligent Transportation System Protocol) protokol za državnu transportnu komunikaciju za inteligentne transportne sustave

GPS (The Global Positioning System) globalni pozicijski sustav

POPIS TABLICA I SLIKA