Sikkerhet og personvern

Oversikt over sikkerhetsteknologier

PASR - Preparatory Action on the enhancement of the European industrial potential in the field of Security research

Grant Agreement no. 108600

Supporting activity acronym: PRISE
Activity full name: Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

ISBN 978-82-92-44712-3

Utgitt: Oslo, august 2007
Omslag: Enzo Finger Design AS
Trykk: ILAS Grafisk

Elektronisk publisert på: www.teknologiradet.no

Innholdsfortegnelse **side**

Forord

Dette dokumentet inngår som en del av PRISE-prosjektet (PRIvacy and Security in Europe). Siktemålet med prosjektet er å bidra til en sikker fremtid for Europa i tråd med europeiske borgeres rettigheter og preferanser, og da særlig retten til personvern. Prosjektet gjennomføres i samarbeid med institusjoner i Danmark (Teknologirådet), Tyskland (Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein) og Østerrike (Institut für Technikfolgen-abschätzung, ITA).

Teknologirådet i Norge har vært ansvarlig for å kartlegge teknologier og metoder som brukes i sikkerhets- og antiterrorarbeid, og som kan påvirke menneskers personvern. Oversikten over teknologier skal brukes videre i prosjektet; både i en juridisk vurdering av sikkerhetsteknologiene og -metodene, og for å utvikle scenarier som beskriver hvordan sikkerhetsteknologiene kan påvirke menneskers dagligliv. Dokumentet står imidlertid også på egne ben, som en tilnærmelsesvis uttømmende oversikt over sikkerhetsteknologier som benyttes i dag. Hensikten – både med teknologioversikten og scenariene som bygger på den - er å synliggjøre hvordan de ulike teknologiene for overvåkning og sikkerhet påvirker samfunnet, og å stimulere til debatt rundt dette.

Teknologirådet jobber prosjektbasert, og involverer ressurspersoner som har særlig kompetanse innenfor de tema prosjektet omfatter. I arbeidet med denne oversikten har vi blant annet intervjuet en rekke ressurspersoner på sikkerhetsområdet. Vi vil gjerne takke alle ekspertene som har gitt av sin tid og kunnskap gjennom intervjuene (se Appendiks A for en liste over intervjuobjekter).

Vi vil også gjerne takke Einar Aas (NTNU) og Ove Skåra (Datatilsynet), som underveis i arbeidet har lest og kommentert dokumentets innhold. Arbeidet har vært ledet av Teknologirådets prosjektleder Christine Hafskjold.

Tore Tennøe
Sekretariatsleder, Teknologirådet

Oppsummering

Hva er sikkerhetsteknologi?
Sikkerhet kan defineres som fravær av fare – det vil si en situasjon hvor den ønskede tilstanden ikke er truet eller forstyrret på noen måte. I PRISE-prosjektet forstås sikkerhet som samfunnssikkerhet – eller mer nøyaktig – som sikkerheten til borgerne som utgjør samfunnet.

Begrepet *sikkerhetsteknologi* kan dekke alt fra private alarmsystemer og virusbeskyttelse for PC-er, til systemer for grensekontroll og internasjonalt politisamarbeid via internett. For å kunne fokusere arbeidet, har deltakerne i PRISE-prosjektet definert et sett med kriterier som sikkerhetsteknologier og -tiltak (systemer, lovgivning, osv.) må oppfylle for å være relevante for prosjektet:

- Teknologiene eller tiltakene er ment, eller har stort potensial, til å styrke samfunnets sikkerhet mot trusler fra individer eller grupper av individer (ikke stater). Dette dekker kriminalitetsbekjempelse, antiterrortiltak, grensekontroll, osv.
- Siden fokuset er samfunnssikkerhet, dekkes ikke teknologier som fokuserer på å beskytte enkeltindivider eller enkeltforetak, slik som boligalarmer eller sikkerhetssystemer for private datamaskiner eller datanettverk.
- Vi vil bare se på teknologier som direkte eller indirekte kan krenke individers personvern.
- Teknologiene eller tiltakene som diskuteres er enten teknologier som allerede er i bruk, teknologier vurderes som viktige i overskuelig fremtid eller som er del av et pågående forsknings- og utviklingsprosjekt.

Teknologimodellen
Selv når vi bruker de ovennevnte kriteriene, utgjør sikkerhetsteknologier og sikkerhetstiltak et stort felt. For å organisere funnene våre, har vi delt teknologiene inn i ulike kategorier: *Grunnleggende teknologier* er grunnlaget for *anvendelsesområder* i forbindelse med sikkerhet. Vi identifiserer fire grunnleggende teknologier: *Kommunikasjonsteknologi, sensorer, datalagring* og *analyse- og beslutningsstøtte*. For å illustrere anvendelsesområder gir vi en rekke *eksempler på systemer*. Eksemplene er kjente anvendelser fra den virkelige verden.

Hensikten med *teknologimodellen* er å vise at sikkerhetsanvendelser avledes fra mange grunnleggende teknologier og dermed arver de truslene mot personvernet som er assosiert med disse teknologiene. For eksempel: Fordi biometriske pass (Machine Readable Travel Documents, MRTD) er basert på både kommunikasjonsteknologi, sensorer, datalagring og biometri, stilles de overfor de samme personvernutfordringer som hefter ved alle disse grunnleggende teknologiene.

Styrken i modellen ligger i evnen til å analysere anvendelsesområder som fortsatt er på forskningsstadiet, og til og med fremtidige teknologier som bare er på idéstadiet. Hvis disse teknologiene kombinerer én eller flere av de nevnte grunnleggende teknologiene, kan de også arve teknologienes personvernegenskaper. Dette gjør det mulig å analysere disse

teknologienes innvirkning på personvernet, og dermed også deres relevans for PRISE-prosjektet.

Grunnleggende teknologier
De grunnleggende teknologiene finnes i mange områder i samfunnet – ikke bare i sikkerhetsanvendelser. Det er imidlertid viktig å se nærmere på disse teknologiene og deres innvirkning på personvernet, for å bedre forstå de følgene som anvendelsesområdene og eksemplene på systemer har for personvern.

Den første grunnleggende teknologien som presenteres i denne rapporten er *kommunikasjonsteknologi*. Kommunikasjon er en forutsetning for nesten alle anvendelser: Det er kommunikasjon mellom sensorer og lesere, mellom lokale datasystemer og sentrale databaser, osv. Hovedutfordringen i forhold til personvern er at kommunikasjon som inneholder sensitiv informasjon kan bli fanget opp av uvedkommende. Kommunikasjonsteknologi kan også avsløre hvor en person befinner seg – enten direkte eller gjennom en grundigere analyse av kommunikasjonsdata. I tillegg er ikke kommunikasjon mellom anvendelser som bruker radiofrekvensidentifisering (RFID) nødvendigvis transparent – det vil ikke være mulig for den berørte personen å sjekke hva som er kommunisert.

En s*ensor* er en innretning som konverterer en egenskap fra den fysiske verden om til et elektrisk signal. Sensorer finnes i en rekke anvendelser som spenner fra videoovervåking (elektrooptiske sensorer) til lesere for ID-kort som inneholder integrerte kretser. Den største personvernutfordringen i forbindelse med sensorer er mangelen på gjennomsiktighet (transparens). Den registrerte vet vanligvis ikke at hans eller hennes informasjon har blitt samlet inn eller behandlet (f.eks. et bilde tatt ved videoovervåking, en samtale fanget opp av en mikrofon eller en RFID-brikke lest på avstand av en leser).

Biometrisk teknologi kan betraktes som en undergruppe av sensorteknologi, men fordi biometri ofte brukes i sikkerhetssammenheng, gir vi denne teknologien bred omtale i rapporten. Biometri brukes til å identifisere individer gjennom å bruke deres biologiske eller atferdsmessige kjennetegn. Ansiktskjennetegn og fingeravtrykk er de mest anvendte biometriske kjennetegnene. Biometri berører personvern på en rekke måter:

- Biometri forholder seg til en persons atferdsmessige og fysiologiske kjennetegn og kan brukes til en entydig identifisering av vedkommende. Det er ingen form for biometrisk verifisering som tillater pseudonymitet eller anonymitet.
- Biometriske data som fingeravtrykk og DNA-prøver kan samles inn uten at den registrerte vet om det.
- Biometri kan avsløre sensitiv informasjon som etnisitet, humør og – slik tilfellet er med DNA – arvelige faktorer og sykdommer.
- Biometriske systemer er sårbare for såkalt *spoofing* (forfalskninger). Fordi det er en så sterk forbindelse mellom den registrerte og de biometriske kjennetegnene, er det meget vanskelig for et offer å bevise misbruk fra en bedrager.

Datalagring og *analyse- og beslutningsstøtte* er de siste grunnleggende teknologiene som beskrives i denne rapporten. Lagring av personopplysninger gir en rekke personvernutfordringer. Når ulik informasjon om en person kobles sammen, avdekkes mer enn dersom kun deler av informasjonen er tilgjengelig. Denne utfordringen øker når flere datakilder kobles sammen og analyseres (datautvinning, søketeknologi), ofte uten at den registrerte vet om

det. Databaser er også utsatt for såkalt formålsutglidning (*function creep*) – det vil si at data brukes til et annet formål enn det de opprinnelig ble samlet inn for. Sentrale databaser er også utsatt i forhold til brudd på sikkerheten.

I denne rapporten har vi valgt å ta med noen eksempler på systemer som i dag kun brukes i USA, og også enkelte som ikke lenger er i bruk. Rapporten skal gi en oversikt over hvilke teknologier som kan brukes til sikkerhetsformål i Europa. Fordi amerikanske retningslinjer synes å ha stor innvirkning på europeisk sikkerhet, blir teknologier og anvendelser som for tiden kun brukes i USA relevante for PRISE. I tillegg vet vi at data om EU-borgere allerede er samlet inn og bearbeidet av sikkerhetssystemer og sikkerhetsanvendelser i USA.

Noen av *eksemplene på systemer* som beskrives i denne rapporten er ikke sikkerhets-teknologier slik vi har definert det i dette kapitlet – dette gjelder for eksempel ”black box” forsikring (se kapittel 2.5.2) eller systemer for å håndtere innvandring, slik som EURODAC (se kapittel 3.5). Systemene er tatt med her på grunn av det potensialet som den beskrevne teknologibruken har for overvåkings- og sikkerhetsanvendelser.

Noen av teknologiene i denne rapporten beskrives i detalj, mens andre kun omtales kort. Dette skyldes at det er tilstrekkelig med en kort beskrivelse for å forstå enkelte av tekno-logiene og deres konsekvenser for personvern, mens det for andre er nødvendig med tekniske detaljer for å kunne analysere og vurdere innvirkningene på personvern på en tilstrekkelig grundig måte (se PRISE-rapport D 3.2).

Rapporten innledes med et overblikk over de rettslige forutsetningene som ligger til grunn for personvern- og sikkerhetsspørsmål. I de påfølgende kapitlene presenterer vi de ulike teknologiene: *Kommunikasjonsteknologi, sensorteknologier, datalagring* og *analyse- og beslutningsstøtte*.

Kapittel 1 Europeisk og internasjonal personvernlovgivning

1.1 Innledning

Dette kapitlet gir et overblikk over internasjonale og europeiske reguleringer for bruk av sikkerhetsteknologier, samt en oversikt over personvernlovgivningen. En mer detaljert beskrivelse av de juridiske kravene finnes i rapport D 3.2.

Både myndigheter, borgere og forretningsforetak kan være berørt av databehandling i forbindelse med bruk av sikkerhetsteknologi. Enkelte reguleringer, som for eksempel politivedtekter, gjelder kun offentlige myndigheter. Andre forskrifter skiller ikke mellom adressatene og er rettet mot både myndigheter, forretningsforetak og individer.

1.2 Internasjonale kilder

EU-landene er ikke bare bundet av EUs overnasjonale lover, men også av internasjonale lover. De første skrittene for å sikre personvern som en menneskerettighet på et internasjonalt nivå kan dateres tilbake til 1950.

1.2.1 Reguleringer av personvern og databeskyttelse

I de fleste vestlige land er personvern en grunnlovsfestet rettighet som er beskyttet av klare regler.

Den første internasjonale reguleringen som presenterte personvern som en menneskerettighet er artikkel 12 i Menneskerettighetserklæringen, som ble vedtatt av FN i 1948.[1] Nesten nøyaktig samme ordlyd gjentas i artikkel 17 av Den internasjonale konvensjonen om sivile og politiske rettigheter, som FN vedtok i 1976. Mens denne konvensjonen er forpliktende, er ikke Menneskerettighetserklæringen rettslig forpliktende for nasjonale lover.

I 1950 vedtok Europarådet, med sine 46 medlemsland, Den europeiske konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter (EMK). EMK er en forpliktende traktat. EMKs artikkel 8 stadfester retten til respekt for privat- og familieliv.[2] I 1981 vedtok Europarådet Konvensjonen om personvern i forbindelse med elektronisk databehandling av personopplysninger, den såkalte Konvensjon 108. Samtlige EU-land stadfestet denne konvensjonen, som nedfeller databeskyttelse som beskyttelsen av grunnleggende rettigheter og særlig den enkeltes rett til personvern. I tillegg har Europarådet gitt anbefalinger på veldig mange særområder innenfor personvernlovgivning, som for eksempel beskyttelsen av personopplysninger innenfor teletjenester eller videreformidling av personopplysninger som innehas av offentlige instanser til tredjeparter.

---

[1] Menneskerettighetserklæringen, Artikkel 12: *Ingen må utsettes for vilkårlig innblanding i privatliv, familie, hjem og korrespondanse, eller for angrep på ære og anseelse. Enhver har rett til lovens beskyttelse mot slik innblanding eller slike angrep*. Se http://www.unhchr.ch/udhr/lang/nrr.htm.

[2] EMK Artikkel 8: *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.*

Organisasjonen for økonomisk samarbeid og utvikling (OECD) vedtok i 1980 Retningslinjer for beskyttelse av privatlivet og overføring av personopplysninger over landegrensene. OECDs retningslinjer, Konvensjon 108 og Personverndirektivet (95/46/EF) representerer hver for seg grunnleggende verktøy innen personvernbeskyttelse.

1.2.2 Reguleringer av personvernbeskyttelse og håndhevelse av indre sikkerhet

I mai 2005 undertegnet syv av EUs medlemsland en internasjonal traktat, Prüm-traktaten, om en opptrapping i samarbeidet over landegrensene, særlig i forhold til å bekjempe terrorisme, kriminalitet over landegrensene og ulovlig innvandring.[3] Traktaten innfører tiltak for å forbedre informasjonsutveksling om DNA og fingeravtrykk. Alle medlemslandene i EU har mulighet til å undertegne. Underskriftslandene sikter mot å innarbeide Prüm-traktatens bestemmelser i EUs juridiske rammeverk. Prüm-traktatens siktemål er å i verksette tilgjengelighetsprinsippet på et mellomstatlig nivå, slik det fremsettes i Rådets rammebeslutning om utvekslingen av informasjon under tilgjengelighetsprinsippet (COM (2005) 490 endelig).[4]

Europarådet vedtok Konvensjonen om forebygging av terrorisme i 2005. Denne konvensjonen sikter mot å iverksette tiltak som kan være nødvendige for å forbedre eller utvikle samarbeidet mellom nasjonale myndigheter for å hindre terrorangrep. Dette innbefatter informasjonsutveksling og en forbedring av den fysiske beskyttelsen av mennesker og eiendom.

1.3 EU-reguleringer

Den europeiske union er bygget på tre søyler. Den første søylen, eller *Fellesskapssøylen*, er overnasjonal lovgivning. Den andre og tredje søylen er mellomstatlig lovgivning.

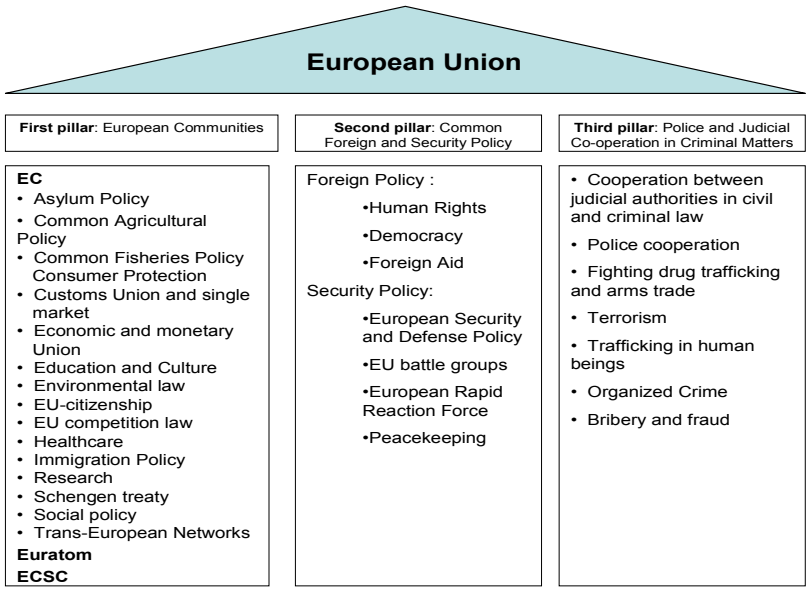
Den første søylen utgjøres av de tre europeiske Fellesskapene og inneholder Fellesskapets domsrett. Innenfor EUs rammeverk kan Fellesskapets institusjoner utarbeide lovgivning i de respektive ansvarsområder som direkte angår medlemslandene. Artikkel 249 i traktaten som etablerer Det europeiske fellesskap gir Fellesskapets institusjoner flere verktøy for å regulere europeisk lovgivning: forordninger, direktiver, beslutninger og anbefalinger.

Felles utenriks- og sikkerhetspolitikk (FUSP) utgjør den andre søylen og er regulert i artikler 11-28 i traktaten om Den europeiske union. Politi- og strafferettslig samarbeid utgjør den tredje søylen og er regulert i artikler 29-42 i traktaten om Den europeiske union. Tresøylestrukturen til Den europeiske union stammer fra forhandlingene som ledet frem til Maastricht-traktaten og gjenspeiles i strukturen til traktaten om Den europeiske union.

---

[3] Publisert av Statewatch i http://www.statewatch.org/news/2005/aug/Pr%FCm-Convention.pdf .
[4] Se kapittel 1.3.2

Innenfor den andre og den tredje søylen har ikke Det europeiske fellesskap noe uttalt eller antydet makt, og domsretten er for det meste mellomstatlig. Beslutninger som angår felles utenriks- og sikkerhetspolitikk gjøres på grunnlag av samarbeid medlemslandene imellom. Verktøy på dette mellomstatlige nivået er for eksempel prinsippvedtak, fellestiltak, felles standpunkter eller rammebeslutninger. Rammebeslutninger kan sammenlignes med et EU-direktiv.



Figur 1: EUs tre søyler

1.3.1 Reguleringer av personvern og databeskyttelse

Med utgangspunkt i reguleringene i Konvensjon 108, vedtok Europakommisjonen direktiv 95/46/EF (Personverndirektivet) etter fire år med samtaler, og dermed ble medlemslandene forpliktet til å endre sin lovgivning i tråd med direktivet. Direktivet inneholder grunnleggende regler både for lovligheten av å behandle personopplysninger og rettigheter for den registrerte.

Direktivet nedfeller en rekke generelle prinsipper for databeskyttelse:

- *Legitimitet*: Personopplysninger[5] må behandles[6] på en lovlig måte og behandlingen trenger enten et rettslig grunnlag eller den registrertes samtykke.
- *Nødvendighet*: Personopplysninger kan bare behandles dersom

[5] Se artikkel 2 (a): *"personopplysninger" skal forstås som enhver form for informasjon om en identifisert eller identifiserbar fysisk person ("den registrerte").*

[6] Se artikkel 2 (b): *"behandling av personopplysninger" skal forstås som enhver operasjon eller rekke av operasjoner – med eller uten bruk av elektronisk databehandling – som personopplysninger gjøres til gjenstand for, f.eks. innsamling, registrering, systematisering, oppbevaring, tilpasning eller endring, utvelgelse, søkning, bruk, overbringelse ved overføring, formidling eller enhver annen form for tilgjengeliggjøring, sammenstilling eller samkjøring, blokkering, sletting eller tilintetgjørelse.*

- den registrerte har gitt samtykke eller behandlingen er nødvendig for utførelsen av en kontrakt (som den registrerte er part i), eller
- behandling er nødvendig for å etterkomme rettslige forpliktelser som den registeransvarlige[7] er underlagt, eller
- dersom behandlingen er nødvendig for å utføre en oppgave som gjøres i utøvelsen av offentlig myndighet.

- *Formålsbinding*: Personopplysninger kan bare samles inn for bestemte, uttalte og legitime formål og ikke viderebehandles på en måte som er uforenelig med disse formål.
- *Gjennomsiktighet*: Den registrerte må være klar over eventuell databehandling som finner sted og hvilke opplysninger som blir behandlet av hvilken aktør.
- *Datakvalitet*: Personopplysninger som samles inn må være nøyaktige og, der det er nødvendig, holdes oppdaterte. Alle rimelige skritt må tas for å sikre at data som er unøyaktige eller ufullstendige med hensyn til formålet de ble samlet inn eller viderebehandlet for, blir slettet eller korrigert.
- *Datasikkerhet*: Den registeransvarlige skal iverksette passende tekniske og organisatoriske tiltak for å beskytte personopplysninger mot tilfeldig eller ulovlig ødeleggelse eller tap, endring, uautorisert avsløring eller innsyn, og mot alle andre ulovlige former for behandling.

Siden 1995 har flere direktiver blitt vedtatt innenfor spesifikke områder. Direktiv 2002/58/EF om personvern og elektronisk kommunikasjon gjelder spørsmål som sikkerhet og taushetsplikt ved kommunikasjon, samt lagring av trafikkdata[8] og lokasjonsdata.

Europakommisjonen har utarbeidet et forslag til en rammebeslutning om beskyttelse av personopplysninger behandlet i sammenheng med Politi- og strafferettslig samarbeid (COM 2005 (475)). Forslaget sikter mot å forbedre rettslig samarbeid, særlig i forhold til å avverge og bekjempe terrorisme. Personverndirektivet (95/46/EF) gjelder ikke aktiviteter som faller utenfor rekkevidden av Fellesskapets lovgiving, slik som for eksempel strafferettslig samarbeid.

Traktaten som skal etablere en forfatning for Europa har ikke trådt i kraft, siden ikke alle medlemsland har stadfestet den ennå. Artikkel II-67 i forfatningen nedfeller personvern som en grunnleggende rettighet: *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kontakt med andre*. Beskyttelse av personopplysninger er regulert i artikkel II-68:

Enhver har rett til beskyttelse av personopplysninger som angår ham/henne.
Disse opplysningene skal behandles korrekt, til uttrykkelig angitte formål og på grunnlag av de berørte personers samtykke eller på et annet berettiget grunnlag fastsatt ved lov. Enhver har

---

[7] Se artikkel 2 (d): *"den registeransvarlige" skal forstås som den fysiske eller juridiske person, offentlige myndighet, institusjon eller ethvert annet organ som alene eller sammen med andre avgjør til hvilket formål og med hvilke midler personopplysningene skal behandles.*

[8] Bestemmelsene om lagringen av trafikkdata til faktureringsformål ble erstattet av direktiv 2006/24/EF (datalagring), se kapittel 1.3.2.

rett til innsyn i den innsamlede informasjonen som angår ham eller henne og til rettelse av denne. Overholdelsen av disse reglene er underlagt en uavhengig myndighetskontroll.

1.3.2 Reguleringer av personvernbeskyttelse og håndhevelse av indre sikkerhet

Regler om politipraksis og -forpliktelser, og dermed også polititjenestemenns bruk av sikkerhetsteknologier, er fortsatt i stor grad regulert gjennom den nasjonale lovgivningen. Metoder for å bekjempe kriminalitet, slik som videoovervåking, kommunikasjonskontroll, overvåking av private eiendommer, benyttelse av lokasjonsteknologi eller DNA-databaser, er regulert i den nasjonale lovgivningen.

Reguleringer på et europeisk – overnasjonalt – nivå med hensyn til polititjenestemenns bruk av sikkerhetsteknologier finnes bare for saker som oppstår i områder som Det europeiske fellesskap har domsrett over. Rådets forordning (EF) nr. 2252/2004, om standarder for sikkerhetselementer, biometri i pass og reisedokumenter som er utstedt av for eksempel medlemslandene, var ment å nedfelle regler som skulle gi effekt til konvensjonen som iverksatte Schengen-avtalen.[9] Bestemmelser om grensekontrolls- og visuminformasjonssystemene SIS (Schengen informasjonssystem), SIS II og VIS (Visuminformasjonssystemet) er også regulert på et europeisk nivå.[10]

Videre forsøker man gjennom forslaget for en rammebeslutning fra Rådet om utveksling av informasjon under tilgjengelighetsprinsippet (COM (2005) 490 endelig) å etablere regler for å sikre at informasjon som er nødvendig for å bekjempe kriminalitet kan krysse de interne landegrensene i EU uten hindringer. Tilgjengelighetsprinsippet forsøker å sikre at informasjon som er tilgjengelig for visse myndigheter i ett medlemsland også må overleveres til tilsvarende myndigheter i andre medlemsland. Den foreslåtte rammebeslutningen fra Rådet følger samme målet som Prüm-traktaten. Utvekslingen av politiinformasjon inkluderer sensitive data som fingeravtrykk og DNA-informasjon.

Datalagringsdirektivet (2006/24/EF), om lagring av data som er opprettet eller behandlet i forbindelse med tilveiebringelsen av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller elektroniske kommunikasjonsnett, ble vedtatt i begynnelsen av 2006. Direktivet regulerer omfanget av lagring av trafikk- og lokasjonsdata i medlemslandene, for å sikre at opplysninger er tilgjengelige for å undersøke, avsløre og rettsforfølge alvorlige forbrytelser, slik de defineres av de enkelte medlemsland i sine nasjonale lover.

Før det nye direktivet trådte i kraft måtte trafikk- og lokasjonsdata slettes når de ikke lenger var påkrevd for å kunne opprette en kommunikasjonslinje, eller yte en merverditjeneste. Behandling av trafikkdata var bare tillat for faktureringsformål, eller til slutten av perioden hvor fakturaen kunne rettmessig bestrides. Det nye direktivet forlenger lagringsperioden til *ikke mindre enn seks måneder og ikke mer enn to år fra kommunikasjonsdatoen.*

---

[9] Protokoll 2 som er vedlagt traktaten om Den europeiske union integrerer Schengenregelverket inn i rammeverket til Den europeiske union.

[10] Se kapittel 5.3

Medlemslandene Irland og Slovakia har tatt rettslige skritt mot direktiv 2006/24/EF i EU-domstolen, idet de hevder at et feilaktig rettslig grunnlag lå til grunn for direktivet.[11]

[11] I mai 2006 avga EU-domstolen sin kjennelse om at avtalen mellom Det europeiske fellesskap og USA om PNR-data (Passenger Name Records) til flypassasjerene som ble overført til USA var basert på et feilaktig rettslig grunnlag og annullerte de respektive beslutninger. Dataene ble opprinnelig samlet inn til et formål som faller inn under Fellesskapets lovgivning (kjøp av en flybillett), mens dataens overlevering, som hadde det formål å beskytte offentlig sikkerhet, faller inn under rammeverket om offentlig sikkerhet. Direktiv 2006/24/EF endrer formålet med datalagring fra å yte en kommunikasjonstjeneste til å muliggjøre etterforskningen, avsløringen og rettsforfølgelsen av alvorlige forbrytelser. Se også kapittel 5.4

Kapittel 2 Kommunikasjonsteknologi

Med kommunikasjonsteknologi mener vi mobiltelefoni, fasttelefoni (PSTN) og kommunikasjon over internettprotokollen (IP). Fordi sporing gjennom satellittbasert posisjonering og GSM-nettverket har mye til felles, har vi også valgt å ta med en beskrivelse av satellittbasert posisjonering i dette kapitlet, selv om det strengt tatt ikke er en kommunikasjonsteknologi.

Å utveksle informasjon ved hjelp av kommunikasjonsteknologi kan gi tre typer data:

- *Trafikkdata*: Hvem utvekslet informasjon, når, og for hvor lenge?
- *Lokasjonsdata*: Hvor var de berørte partene på det tidspunktet de hadde kontakt? Fra et rettslig standpunkt anses slike lokasjonsdata som er nødvendig for å håndtere en forbindelse (for eksempel ID-en til basestasjonen (celle-ID)), som trafikkdata.
- *Innhold*: Hvilken informasjon ble utvekslet?

Sikkerhetstiltak og sikkerhetsteknologier i forbindelse med kommunikasjonsteknologi innebærer vanligvis tilgang til én eller flere av disse formene for data, enten i sanntid eller gjennom at data lagres for senere bruk.

2.1 Personvernutfordringer i forbindelse med kommunikasjonsteknologi

Den mest åpenbare personvernutfordringen i forbindelse med kommunikasjonsteknologi er at kommunikasjon som inneholder sensitive opplysninger kan fanges opp av uvedkommende: Telefonsamtaler kan avlyttes, og tekstbasert kommunikasjon som ikke er kryptert kan leses av alle med tilgang til serveren meldingen er lagret på. Selv radiokommunikasjonen mellom RFID-brikker og deres lesere kan fanges opp av hvem som helst med riktig utstyr.

Kommunikasjonsteknologi kan også avsløre hvor en person er eller har befunnet seg. Så godt som alle bruker mobiltelefon – som kan lokaliseres gjennom basestasjonene den kommuniserer med. Mobiltelefoner er i økende grad utstyrt med GPS-moduler som gir en enda mer nøyaktig posisjon.

I tillegg er ikke kommunikasjon mellom apparater som bruker radiofrekvensidentifisering (RFID) nødvendigvis transparent – det vil som regel ikke være mulig for den berørte personen å sjekke hva som er blitt kommunisert.

2.2 Fasttelefoni

Med fasttelefoni mener vi det tradisjonelle linjesvitsjede telenettet. I praksis dekker dette både tradisjonell fastlinjekommunikasjon og mobiltelefoni, men siden den informasjonen som registreres for kommunikasjon over mobilapparater avviker fra den for fastlinjetelefoni, vil mobiltelefoni beskrives i et eget avsnitt.

Telenettet har vært i bruk i over 100 år, og dekker store geografiske områder og milliarder av brukere. Det har derfor vært viktig å utvikle standarder som beskriver hvordan brukerinformasjon skal kodes, hvordan informasjon om flere samtaler skal håndteres

(multipleksing) og hvordan forespørsler om å tilkoble og frakoble samtaler skal kodes og sendes (signalering).

Følgende informasjon registreres for hver forbindelse:

- starttidspunkt
- rutingsinformasjon (hvilket nummer som foretar anropet, og hvilket nummer anropet er til)
- sluttidspunkt

Telefonnummeret er forbundet med kabeluttaket, det vil si at nummeret ikke er forbundet med en bestemt person eller telefon, men med uttaket som telefonen er koblet til. Posisjonen kan derfor finnes gjennom kundeinformasjonen (adressen) for det gitte nummeret.

2.3 Mobiltelefoni

En mobilterminal, som for eksempel en GSM-telefon (Global System for Mobile communication), oppretter kommunikasjon gjennom såkalte basestasjoner. Disse er antenner med mottakere/sendere som formidler signalet mellom nettverket og mobilterminalene. Trafikk fra en mobiltelefon sendes som radiobølger til den nærmeste basestasjonen. Derfra går signalet gjennom det kabelbaserte nettverket til enten en fasttelefon eller til en mobilterminal via basestasjonen som ligger nærmest der mottakeren befinner seg.[12]

I motsetning til det linjesvitsjede nettverket, er mobilnummeret knyttet til selve apparatet, eller mer nøyaktig til apparatets SIM-kort (Subscriber Identity Module).

For å kunne opprette en forbindelse, må mobilnettverket vite hvor hver terminal befinner seg til enhver tid. For å kunne gjøre dette, sender mobilenheten regelmessige rapporter til nettverket, og mottar i sin tur informasjon, for eksempel når:

- Den har blitt slått av, og slås på igjen
- Når den er på og flyttes fra ett lokasjonsområde (basestasjon) til et annet
- Et forhåndsdefinert tidsintervall har løpt ut

Lokasjonsinformasjon lagres i to forskjellige registre som opprettholdes av mobiloperatøren: *Home Location Register (HLR)* og *Visitor Location Register (VLR).* Disse registrene brukes til å holde rede på hvor mobilenhetene beveger seg, og er nødvendige for å kunne yte en mobil tjeneste.

HLR inneholder informasjon om:

- Koden og nummeret som abonnenten er tildelt
- Hvilke tjenester det abonneres på

[12] Den tekniske informasjonen om mobiltelefoni er i hovedsak basert på Riksaasen T. (1993/94) *Telematikknett*

- Begrensninger i tjenestene (for eksempel bare innenrikssamtaler, og lignende)
- Informasjon om hvilket VLR mobilenheten er registrert i. Dette gjør det mulig for innkommende anrop å bli rutet til mobilenheten. Når enheten flyttes, oppdateres informasjonen.

VLR inneholder informasjon om:

- Abonnentens ID-kode
- Abonnementsinformasjon (som med HLR)
- Lokasjonsinformasjon (Location Area Identity, LAI)

Dette betyr at mobilenhetens posisjon hele tiden er kjent av systemet så lenge enheten er slått på, og ikke bare når den er i aktiv bruk. Når kommunikasjon finner sted, lagrer operatøren data om hvilke basestasjoner som ble brukt som en del av trafikkdataene. Dette brukes senere ved fakturering.

Viktig informasjon i forbindelse med mobilkommunikasjon er:
Telefonnummeret: Dette er et nummer som SIM-kortet tildeles av en nettverksoperatør. Nummeret kan "flyttes" fra én mobiltelefon til en annen ved å flytte SIM-kortet, og mobilen kan også bli tildelt til et nytt SIM-kort dersom brukeren velger å bytte operatør (nummerportabilitet).

IMSI – (International Mobile Subscriber Identity): Alle mobilabonnenter tildeles et unikt 15-sifret IMSI-nummer. IMSI utgjøres av tre deler:

- Landskode (MCC)
- Nettverkskode (MNC)
- Abonnentsnummer (MSIN)

IMSI-nummeret lagres i abonnentens SIM-kort.

TMSI (Temporary Mobile Station Identity): Denne identifikasjonskoden brukes istedenfor IMSI-en i radiogrensesnittet for å begrense den mulige sporingen av en abonnent. Beskyttelse av identitet er særlig viktig i mobilkommunikasjonssystemer, hvor abonnenten og nettverket identifiserer seg for hverandre før forbindelsen opprettes.

IMEI (International Mobile Equipment Identity): Alle GSM-telefoner tildeles en unik 15-sifret IMEI-kode. Gjennom denne koden kan man finne produsenten, modelltypen og hvilket land som har godkjent utstyret. IMEI-koden lagres i EIR-registeret (Equipment Identity Register).

Celle-ID: ID-nummeret til en bestemt basestasjon.

SIM-nummeret: Samtlige SIM-kort for mobiltelefoner har blitt tildelt hvert sitt unike SIM-kortnummer.

GSM-kommunikasjon krypteres gjennom A5/1-kryptering. Denne krypteringen skulle opprinnelig holdes hemmelig, men ble lekket i 1994. Utstyr som kan plukke opp og dekode GSM-kommunikasjon er nå kommersielt tilgjengelig (se en mer utførlig beskrivelse i kapittel 2.3.2). Noen av avlyttingssystemene har også funksjoner for gjenkjenning av ord. Dette

betyr at i tillegg til å plukke opp og lagre kommunikasjonen, kan systemet identifisere ord og uttrykk ut fra en forhåndsdefinert database.[13] I de fleste land er det ulovlig å selge slikt utstyr til andre enn politimyndigheter eller andre autoriserte offentlige etater. Til tross for dette er det en økende tendens til at slike og andre former for overvåkingsteknologi blir mer tilgjengelig på privatmarkedet.[14] Faktisk er det slik at privatpersoner, gjerne i forbindelse med privat etterforsking eller kriminelle aktiviteter, ofte har tilgang til overvåkingsutstyr som det er forbudt for politiet å bruke til lovlige formål.

2.3.1 Avlytting

Grunnleggende teknologier: *PSTN*
Mobilkommunikasjon
Internettkommunikasjon
Satellittkommunikasjon

Det finnes ulike systemer som er designet for å overvåke borgere og deres kontakt med hverandre, enten det finner sted over internett, telenettet eller innenfor avgrensede områder. *Telefonavlytting* er en form for avlytting som i hovedsak går ut på å installere avlyttingsutstyr i forbindelsen mellom to telefoner som er del av en samtale. Avlyttingsutstyret kan monteres på telefonen til den som skal overvåkes, men også på telefoner til personer han eller hun forventes å kontakte. For politiet er det ofte unødvendig å installere slikt utstyr – de kan enkelt få tilgang til de nødvendige dataene gjennom nettverksoperatørenes systemer.

For avlytting av mobilnettverk vil politiet vanligvis sørge for at nettverksoperatøren får IMSI-nummeret til telefonen de ønsker å avlytte. Politiet vil deretter være i stand til å avlytte (og dekode) kommunikasjonen gjennom nettverksoperatørens utstyr.[15]

En mer omfattende form for telefonavlytting er å vilkårlig avlytte samtlige kommunikasjonslinjer (telefon, mobil, internett) på jakt etter samtaler som kan være av interesse.

Eksempel: Echelon
Echelon-nettverket styres av en allianse mellom USA, Storbritannia, Canada, Australia og New Zealand. Systemet har vært i drift siden Den kalde krigen og ble opprinnelig opprettet for å overvåke kommunikasjon i eller til Sovjetunionen og Øst-Europa. Systemets eksistens ble allment kjent som et resultat av en rapport fra EU-parlamentets teknologivurderingsorgan STOA (Scientific Technology Options Assessment).[16] Siden alliansen selv nektet å gi noen kommentar, nedsatte EU-parlamentet en komité for å vurdere Echelons eksistens og metoder. Komiteen konkluderte[17] med at systemet finnes, og at formålet er å overvåke privat og forretningsmessig kommunikasjon. Kommunikasjonsmønstre kan analyseres, og

[13] Se for eksempel innføringen i *GSM Intercept A5.1 Chatter Guard* i http://www.gcomtech.com/product.aspx?ID=37&CID=6
[14] Hegghammer T (2006) *Terrorisme og ny kommunikasjonsteknologi*
[15] Kilde: Telenor
[16] Wright S. (1998) *An appraisal of the Technologies of Political Control* og Campbell D. (1999) *Interception Capabilities 2000*
[17] Temporary Committee on the ECHELON Interception System (2001) *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*

innholdet kan skannes for interessante nøkkelord. Meldinger som er identifisert av systemet kopieres så for manuell analyse.[18]

Systemet kan utføre kvasi-total overvåking, det vil si at alle typer elektronisk kommunikasjon – telefonsamtaler, SMS-er, fakser, e-post og internettrafikk – kan overvåkes. Overvåkningssystemet er i hovedsak avhengig av å fange opp verdensomspennende satellittkommunikasjon. Nettverket synes ikke å være så omfattende som tidligere antatt, siden bare en liten andel av kommunikasjonen i områder med mye trafikk overføres via satellitt.

2.3.2 Teknisk identifisering av telefoner og kommunikasjonsutstyr

Grunnleggende teknologier: *Mobilkommunikasjon*

Identiteten til mobiltelefoner som brukes i det som mistenkes å være kriminell virksomhet er ofte ukjent for politiet, siden forbrytere har en tendens til å bytte telefoner ofte, bruke anonyme telefoner (hvor det er mulig) eller stjålne telefoner. For å få en rettskjennelse til å foreta telefonavlytting, må telefonen eller kommunikasjonsutstyret først identifiseres.

Identifiseringen kan oppnås gjennom utstyr som kalles en IMSI-catcher. En IMSI-catcher logger IMSI-numrene til alle mobiltelefonene i et spesifikt område. En telefon kan identifiseres ved å rette utstyret mot vedkommende ved to eller flere anledninger, og gjøre krysshenvisninger til IMSI-numrene for å utelate andre telefoner som tilfeldigvis befinner seg i det samme området. I andre tilfeller er det nødvendig å avlytte samtalene som finner sted for å identifisere personen som holder telefonen. I slike tilfeller kan også samtalene til en uskyldig tredjepart fanges opp.[19]

Dette betyr også at mobilsamtaler innenfor et begrenset geografisk område, som for eksempel et bygningskompleks, kan avlyttes. I Danmark har det blitt foreslått at politiet burde tillates å gjøre slik skanning når særlige forhold tilsier det.

En telefons IMSI-nummer er vanligvis beskyttet, men det overføres i full åpenhet når telefonen oppretter en forbindelse med en ny basestasjon.[20]

En IMSI-catcher er vanligvis en del av utstyret som brukes til å fange opp GSM-kommunikasjon, og slikt utstyr er kommersielt tilgjengelig på markedet. En typisk IMSI-fanger vil ha en overvåkingsradius på noen hundre meter, og vil være i stand til å registrere et spekter med IMSI-, TMSI- og IMEI-numre forbundet med en bestemt basestasjon. Den vil også være i stand til å høre på én eller flere samtaler. I slike tilfeller etterligner utstyret en celle, og det er mulig å foreta avlytting fordi forbindelsen gjøres av catcher-cellen.

---

[18] Teknologirådet (2005): *Elektroniske spor og personvern*
[19] Justis- og politidepartementet (2005) *Ot.prp. nr. 60 (2004-2005): Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)*
[20] Kilde: Telenor

2.4 Kommunikasjon over internettprotokollen

Nettverk som bruker utvekslings- og overføringsprotokollen TCP/IP (Transmission Control Protocol/ Internet Protocol) ruter datapakker (små segmenter med data) fra én unik identifikator (IP-adresse) til en annen. Dette er en helt annen metode enn de linjesvitsjede nettverkene beskrevet ovenfor, hvor en linje opprettes for hver forbindelse som gjøres, og er reservert for akkurat den forbindelsen så lenge oppringningen varer.

Innenfor et privat nettverk kan IP-adresser tildeles på tilfeldig grunnlag så lenge hver adresse er unik. Ved kobling av et privat nettverk til internett bruker man registrerte IP-adresser (også kalt internettadresser) for å unngå duplikater. *Datalagringsdirektivet* (se kapittel 5.2) vil kreve at internettleverandører (Internet Service Providers, ISP-er) lagrer informasjon om hvilken kunde som har hvilken IP-adresse på ethvert tidspunkt i inntil to år.

Noen av de viktigste begrepene forbundet med internett og internettprotokollen er:[21]
IP-adresse: En IP-adresse er en identifikator for en datamaskin eller et apparat på et TCP/IP-nettverk. Når en bruker besøker en nettserver, vil serveren ofte lagre informasjon om brukerens besøk på ulike nettsider. Denne informasjonen vil normalt være tidspunkt, brukerens IP-adresse, brukernavn for internettkontoen og hvilke nettsider som ble besøkt. Dersom brukeren har en fast IP-adresse og ikke bruker adressemapping i en brannmur, kan brukerens maskin bli entydig identifisert.

URL(Uniform Resource Locators): URL-er er strenger som identifiserer nettressurser: dokumenter, bilder, nedlastbare filer, tjenester, elektroniske postkasser og andre ressurser. De gjør at ressurser som er tilgjengelige under et mangfold av navngivingssystemer og tilgangsmetoder, som for eksempel HTTP og FTP, får en adresse på samme enkle måte.[22]

HTTP-referanse: HyperTekst Transfer Protocol (HTTP) er protokollen som brukes for å levere så godt som alle filer, søkeresultater og andre data på internett. De virker slik når en lenke følges fra én side til en annen, sendes adressen (URL-en) fra denne siden sammen med forespørselen etter den nye siden. Det nye nettstedet kan dermed se hvilket nettsted brukeren kom fra, og på denne måten samle informasjon om brukerens aktiviteter på nettet. Når man klikker på en lenke etter et søk, vil ordene i søkestrengen vanligvis være en del av URL-en, og dermed bli videresendt til det nye nettstedet.

Informasjonskapsler (cookies): Informasjonskapsler er meldinger som sendes til en nettleser fra en web-server. Nettleseren lagrer meldingen i en tekstfil på brukerens datamaskin. Meldingen sendes deretter tilbake til serveren hver gang nettleseren spør om en side fra den serveren som leverte den. Hovedformålet med informasjonskapsler er å identifisere brukere og om mulig forberede spesielt tilrettelagte nettsider for dem. Serveren kan bruke informasjonen i informasjonskapslen til å presentere spesielt tilrettelagt innhold, som tidligere lagrede ønskelister eller tilbud basert på tidligere handlemønster.

To ulike typer aktører kan lagre informasjonskapsler på brukerens datamaskin. Førsteparts informasjonskapsler lagres av web-serveren som brukeren besøker. Tredjeparts infor-

[21] Beskrivelsene er hentet fra Teknologirådet (2005) *Elektroniske spor og personvern*
[22] Definisjon fra www.w3.org

masjonskapsler lagres derimot av et selskap som har reklame på den besøkte nettsiden. Disse informasjonskapslene kan brukes til å samle informasjon om brukerens surfevaner på nettsider hvor selskapet reklamerer.

De tre viktigste utvekslingsmetodene for innhold over IP-protokollen er:
E-post: E-post er meldinger som overføres over kommunikasjonsnettverk. Når en melding sendes, kan den lagres på to eller flere ulike servere på sin vei fra senderen til mottakeren. Med mindre e-posten er kryptert, kan den leses av mennesker som har tilgang til disse serverne. I tillegg til innhold, kan informasjon om senderens og mottakerens IP-adresser loggføres, samt informasjon om hvilke adresser meldingen har passert gjennom på veien mellom sender og mottaker.

Lynmeldinger: Lynmeldinger (Instant Messaging, IM) er en krysning mellom en telefonsamtale og en e-post. IM-systemer gjør deg i stand til å opprettholde en liste over mennesker som du ønsker å ha kontakt med. Brukeren kan se hvilke av disse menneskene som er pålogget til ethvert tidspunkt, og kan delta i en skriftlig samtale i et vindu på skjermen. Lynmeldinger bruker mottakerens IP-adresse for å åpne opp en forbindelse mellom de to datamaskinene. Meldinger og forbindelsesinformasjon opprettholdes på servere som kontrolleres av leverandøren av IM-tjenesten.

IP-telefoni (VoIP): IP-telefoni (VoIP, eller Voice over IP) er en metode for å gjøre analoge lydsignaler om til digital data som kan overføres over internett. VoIP bruker bredbåndsnettverk for å overføre samtaler, og derfor er ukrypterte samtaler sårbare for avlytting.

I de neste avsnitt ser vi på teknologier som brukes til å få tilgang til informasjon som er overført over et datanettverk eller generert i en datamaskin.

2.4.1 Pakkesniffing

Grunnleggende teknologier: *Internettkommunikasjon*

En pakkesniffer er et program som kan se all informasjon som sendes over nettverket den er koblet til. En datamaskin vil vanligvis bare se på datapakker som er adressert til den. En pakkesniffer vil derimot se på alt som kommer forbi. Den kan da enten fange opp all kommunikasjon, eller bruke et filter for å fange opp bare de pakkene som inneholder bestemte data.

En pakkesniffer som befinner seg på en av serverne hos en internettleverandør kan potensielt overvåke alle internettaktiviteter, som for eksempel:

- Hvilke nettsteder man har besøkt
- Hva man ser på i løpet av besøket på nettstedet
- Hvilke streaming events som brukes, slik som audio-, video- og bredbåndstelefoni
- Hvem som besøker et bestemt nettsted
- Hva som er lastet ned fra et nettsted
- Hvem e-post sendes til og innholdet i denne

Eksempel: Carnivore
Carnivore er sannsynligvis det mest kjente pakkesniffingssystemet. Det ble utviklet av FBI for å avlytte elektronisk kommunikasjon.[23] Carnivore-systemet installeres hos en internettleverandør (ISP) og kan overvåke all trafikk som beveger seg gjennom akkurat den leverandøren. FBI hevder at Carnivore "filtrerer" datatrafikk og gir etterforskerne tilgang til bare de datapakkene de har adgang til å se i henhold til loven.[24] Det er blitt rapportert at systemet ikke lenger brukes av FBI,[25] siden de nå får den informasjonen de trenger fra internettleverandørene. Kritikere hevder at dette har ført til enda mer invaderende overvåkingsmetoder.[26]

2.4.2 Tastelogging (keystroke logging)

Grunnleggende teknologier: *Internettkommunikasjon*

Tasteloggingsprogrammet ligger inne på en utvalgt datamaskin på samme måte som en trojansk hest. Når den er installert på den utvalgte datamaskinen, vil den logge alle tastetrykk, inkludert tekst som på et senere tidspunkt slettes av brukeren. Utstyret kan fysisk installeres på en spesifikk datamaskin eller sendes som et virus. Et problem med pakkesniffere (se forrige avsnitt), som for eksempel Carnivore, er at de ikke greier å forstå krypterte meldinger. Formålet med tastelogging er å få tilgang til passord og krypteringsnøkler, og å kunne lese vanlige tekstmeldinger som er sendt over internett i kryptert form. Den mest kjente tasteloggeren er FBIs Magic Lantern-system.[27]

2.5 Lokaliseringssystemer[28]

Mobilkommunikasjon kan gi en generell idé om hvor brukeren befinner seg. Det finnes imidlertid mer spesialiserte teknologier som kan fastslå mer nøyaktig posisjon. Disse teknologiene er basert på å beregne posisjonen til brukerens utstyr, istedenfor å bare gi informasjon om hvilken basestasjon som har forbindelse med brukeren. Teknologiene bruker faste eller kjente posisjoner til å beregne hvor brukeren er. Slike teknologier kan være bakkebaserte eller satellittbaserte, eller en blanding av de to.

2.5.1 Lokalisering gjennom GSM-basestasjoner

Det er mulig å beregne hvor brukerens mobilutstyr er gjennom å bruke de kjente koordinatene til for eksempel GSM-basestasjoner.

Beregningene gir en omtrentlig posisjon som kan variere fra noen få hundre meter i tettbefolkede områder til flere kilometer i landlige områder. Nøyaktigheten kan forbedres gjennom å ta signalforsinkelse i betraktning. Mer nøyaktige metoder er *Enhanced time difference* (for GSM) eller *Observed time difference of arrival* (for UMTS). Disse metodene utnytter det faktum at brukere vanligvis befinner seg innenfor området til flere base-

[23] CDT (2000) *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age*
[24] EPIC (2005) *Carnivore page*
[25] FOX News (2005) FBI *Ditches Carnivore Surveillance System*
[26] McCullagh, D. (2007) *FBI turns to broad new wiretap method*
[27] Teknologirådet (2005) *Elektroniske spor og personvern*
[28] Innholdet i dette kapitlet er basert på Teknologirådet (2005) *Elektroniske spor og personvern*

stasjoner samtidig og bruker de relative signalforsinkelsene til de ulike basestasjonene til å beregne beliggenheten, vanligvis innenfor 100-300 meter.

De samme prinsippene kan anvendes med andre typer basestasjoner, slik som WLAN eller Bluetooth. Disse teknologiene har en kortere rekkevidde, og nøyaktigheten vil derfor være høyere.

Det finnes både profesjonelle og mer underholdningsorienterte tjenester basert på GSM-posisjonen:

Eksempel: Radiocelleforespørsel i Tyskland
Basert på en rettskjennelse kan politimyndighetene i Tyskland skaffe seg trafikkdata fra alle GSM-abonnenter innenfor rekkevidden til den radiocellen som ligger nærmest åstedet når en alvorlig forbrytelse finner sted. Denne metoden for å fremskaffe historiske trafikkdata til alle som brukte en teletjeneste nær et åsted kalles for en radiocelleforespørsel (*Funkzellen-abfrage*).[29] Det er per i dag ikke kjent nøyaktig hva slags data som blir fremskaffet, men det er klart at det i det minste er nok data til å identifisere abonnenten.

Eksempel: Buddy/KidsOK
En norsk mobiloperatør hadde tidligere en tjeneste kalt Buddy. Tjenesten gikk ut på at en gruppe venner (to eller flere) inngikk en avtale om at de ønsket å kunne be om hverandres posisjon. Straks avtalen var inngått (via SMS), kunne enhver av de registrerte "buddiene" be om posisjonen til enhver av de andre ved å sende en SMS. Han eller hun ville da motta informasjon om hvor hans eller hennes "buddy" befant seg.[30]

Et tilsvarende system i Storbritannia (KidsOK) lar foreldre spore sine barn. Posisjonen vises på et kart eller sendes til moren eller faren i form av en tekst som beskriver hvor barnet befinner seg.[31]

Den samme teknologien kan brukes av politiet eller andre offentlige etater til å spore en mistenkt etter at mobilenheten deres har blitt identifisert (se kapittel 2.3.2).

2.5.2 Satellittbaserte posisjoneringssystemer

Grunnleggende teknologier: *Mobilkommunikasjon*
Satellittkommunikasjon

Virkemåten til posisjoneringssystemer er egentlig ganske enkel: Satellittene i konstellasjonen utstyres med en atomisk klokke som måler tid meget nøyaktig. Satellittene sender fra seg karakteristiske signaler som viser det nøyaktige øyeblikket da signalet forlot satellitten. Bakkemottakeren har lagret nøyaktige detaljer om banene til samtlige satellitter i konstellasjonen. Ved å tolke det innkommende signalet, kan bakkemottakeren kjenne igjen

[29] Paragraf 100g i den tyske strafferetten: *Dersom bestemte fakta underbygger mistanken om at en person begikk, sto bak eller var ellers medskyldig i en forbrytelse av stor alvorlighet [...] kan det beordres at de som ytte telekommunikasjonstjenester på kommersielt grunnlag må uten utilbørlig utsettelse overlevere trafikkdata i den grad det er nødvendig for å løse forbrytelsen.*
[30] Kilde: *Netcom.* https://netcom.no/privat/kundeservice/veiledninger/buddy.html
[31] *KidsOK*: http://www.kidsok.net/how.php

den enkelte satellitt, fastslå tiden det tok signalet å komme frem og beregne avstanden til satellitten. Straks bakkemottakeren mottar signalene fra minst fire satellitter samtidig, kan den beregne den nøyaktige beliggenheten.[32]

GPS

GPS er en forkortelse for *global postioning system*, et verdensomspennende satellitt-navigeringssystem som består av 24 satellitter som går i bane rundt jorden og deres korresponderende bakkemottakere. Ved å bruke tre satellitter, kan GPS beregne mot-takerens lengde- og breddegrad basert på hvor de tre sfærene krysser hverandre. Ved å bruke fire satellitter, kan GPS også fastslå høyden over havet. GPS er et amerikansk militært system som har blitt gjort allment tilgjengelig.

Fordi teleoperatørene i USA har en forpliktelse til å lokalisere hvor et nødanrop kommer fra, forventes det at stadig flere mobiltelefoner vil utstyres med GPS. I Japan må alle mobil-telefoner ha GPS innen 2007.

Galileo

Galileo vil være et verdensomspennende nettverk av 30 satellitter som gir nøyaktig tids- og lokasjonsinformasjon til brukere på bakken og i luften. Det planlegges å være i full operativ drift i 2010. Nettverket vil være mer nøyaktig enn GPS-systemet, og det vil ha større utbredelse. Galileo er et sivilt system og skal drives av et privat konsortium.[33]

Eksempel: "Black box" forsikring – "Pay as you drive"

Et forsikringsselskap i Storbritannia har innført et forsikringsprodukt kalt Pay as you drive (betal som du kjører). For å dra fordel av produktet, må sjåføren installere en *black box* ("svart boks") i bilen sin. Denne boksen bruker GPS-teknologi og registrerer hvor ofte, når og hvor bileieren kjører.[34]

I USA bruker Progressive Insurance Company nå såkalt "svart boks"-teknologi for å tilby rabatter til sjåfører basert på hvor mye, hvor fort og når de kjører. Et apparat kalt TripSensor plugges inn i bilens diagnoseport, som finnes i nærheten av rattstammen til de fleste biler produsert etter 1996. Sensoren registrerer kjørelengde, tidspunktet motoren startes og slås av, og hastigheten kundene kjører med. Av sikkerhetsgrunner registrerer apparatet også informasjon om bremsing og akselerasjon.[35]

Eksempel: eCall

eCall er et tiltak utviklet for å redde liv ved å sørge for at redningsarbeidere kommer fortere frem til ulykkesstedet. Fra september 2009 er det meningen at samtlige nye biler som selges i land som har undertegnet intensjonsavtalen (*Memorandum of understanding*) skal være utstyrt med eCall-apparater.[36] Apparatet inneholder sensorer som aktiveres etter en ulykke. Det ringer nødnummeret og overfører informasjon om ulykken, inkludert tidspunktet, den

---

[32] D-G Energy and Transport: *Galileo – Satellitte Navigation System,* http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm
[33] Kilde: ESA. http://www.esa.int/esaNA/SEM5K8W797E_galileo_0.html
[34] Norwich Union: *Pay as you drive.* http://www.norwichunion.com/pay-as-you-drive/index.htm
[35] Love, D. (2004): *Progressive's Black Box: Is Big Brother Good for the Industry* http://www.insurancejournal.com/magazines/southeast/2004/12/06/features/50322.htm
[36] European Commission. Information Society and Media: *eCall.*

nøyaktige posisjonen, kjøretøyets kjøreretning og kjøretøyets identifikasjon.[37] De samme data overføres hvis eCall aktiveres manuelt.

Apparatet er ikke permanent tilkoblet et mobilnettverk, og vil bare kobles til når apparatet aktiveres. Det er imidlertid uttrykt bekymring over planlagt overføring av tilleggsdata (for eksempel til forsikringsselskaper), og over mulighetene for uautorisert tilgang til databaser hvor eCall-data er lagret.[38]

[37] Safety Support *eCall: Saving a life every four hours!*
[38] Article 29 Data Protection Working Party (2006) *Working document on data protection and privacy implications in eCall initiative*

Kapittel 3 Biometri

Biometri er ikke en *grunnleggende teknologi* på samme måte som kommunikasjons-teknologi, sensorer, datalagring eller analyse- og beslutningsstøtte. Men fordi det er vanlig at sensorer brukt i sikkerhetsanvendelser har biometri (for eksempel ansiktsgjenkjenning, fingeravtrykk eller irisskanning) som en viktig del av sin funksjon, har vi valgt å ta med et kapittel om biometri før vi går videre til å presentere sensorteknologier i Kapittel 4.

Biometrisk teknologi identifiserer individer automatisk ved å bruke deres biologiske eller atferdsmessige kjennetegn. Biometri kan brukes til å kontrollere tilgang til fysiske områder eller tilgang til informasjon (datamaskiner, dokumenter). Teknologien kan også brukes til å finne ut om en person allerede finnes i en database, som for eksempel ved visumsøknader.

Følgende kriterier kan brukes til å beskrive og vurdere ulike former for biometri:[39]

Allmenngyldighet	Alle mennesker har de samme fysiske kjennetegn – som et ansikt eller DNA – som kan brukes til identifisering.
Egenart	Kjennetegnene er unike for den enkelte, og utgjør dermed et særtrekk.
Uforanderlighet	Kjennetegnene forblir stort sett uforandret i løpet av en persons liv.
Hvor lett det er å samle inn	En persons unike fysiske kjennetegn må kunne samles på relativt enkel måte for rask identifisering.
Ytelse	Identifiseringen må ha en høy grad av nøyaktighet.
Aksept	Anvendelser vil ikke lykkes hvis bruken av biometri ikke er allment akseptert.
Sikring mot omgåelse	For å gi ytterligere sikkerhet, må et system være vanskelig å omgå eller overliste.

De mest anvendte formene for biometri i sikkerhetssystemer er fingeravtrykk og ansiktskjennetegn, som vi kommer til å beskrive mer utførlig senere i kapitlet. Vi vil også se på irisgjenkjenning, siden dette er en av teknologiene som anbefales av ICAO (Den internasjonale organisasjonen for sivil luftfart) for biometriske pass. Andre biometriske teknologier inkluderer:

- *håndgeometri*: analysen av håndformen og lengden på fingrene
- *netthinnen (retina)*: analysen av blodkarene bakerst i øyet
- *signatur*: analysen av måten en person underskriver navnet sitt på

[39] Jain, Bolle og Pankanti (1999): *Personal Identification in Networked society*

- *vener*: analysen av venemønsteret på den bakre delen av hånden og på håndleddet
- *stemme*: analysen av tonefallet, tonehøyden, rytmen og frekvensen til en persons stemme
- *ganglag*: måten man går på
- *ørestruktur*
- *lukt*

Disse formene for biometri vil få forskjellig vurdering etter de forannevnte kriteriene og kan være nyttige for ulike anvendelsesformer i ulike settinger og på varierende sikkerhetsnivåer. I noen settinger er det viktig at analysen kan gjøres fort, mens en høy grad av nøyaktighet kan være avgjørende i andre situasjoner. Basert på en objektiv vurdering er ikke fingeravtrykk og ansiktskjennetegn nødvendigvis de "beste" formene for biometri, men befolkningens kjennskap til disse gjør at de brukes mye.

DNA-gjenkjenning regnes ikke som biometri, ettersom det ikke kan utføres i en automatisert prosess.[40] Det er likevel et biologisk kjennetegn som kan brukes til å identifisere et individ, og det er mulig at analysen vil ta kortere tid i fremtiden. Vi vil derfor ta for oss DNA-profilering i kapittel 3.6.

3.1 Fremgangsmåten

Prosessen knyttet til et biometrisk system kan deles inn i en rekke oppgaver: innsamling, behandling, lagring og sammenligning.

3.1.1 Datainnsamling

Biometriske data samles vanligvis inn ved hjelp av en sensor. Vanlige sensorer som er kjent fra hverdagen er kameraer (optiske sensorer) og mikrofoner (for stemmegjenkjenning). Fingeravtrykkssensorer som gjenkjenner godkjente brukere kommer nå ofte som en integrert del av nye bærbare datamaskiner og annet elektronisk utstyr.

Biometriske avbildninger kan komprimeres for å forminske filstørrelsen ved overføring og lagring. Man kan også kryptere biometriske data.

3.1.2 Behandling

I de fleste tilfeller gjøres det biometriske bildet om til en *mal*, som er en digital avbildning av de biometriske kjennetegnene. Malen lages som regel ved å bruke en algoritme som i de fleste tilfeller er proprietær. Slike algoritmer tar originalbildet eller rådataene og trekker ut de relevante kjennetegnene som trenges for å gjøre det hele om til et matematisk format, også kalt et *feature set*. Denne prosessen kalles også for *uttrekking*. Dersom malen har god nok kvalitet, kan den lagres i enten en database eller på en brikke.[41]

[40] Se Biometrics Catalog; www.biometricscatalog.org
[41] Albrecht, A. (2003) *Privacy Best Practices in Deployment of Biometric Systems*

3.1.3 Lagring

I de fleste biometriske systemer er det kun malen som lagres, og det opprinnelige bildet slettes. I systemer som brukes av politiet internasjonalt, eller til ansiktsgjenkjenning generelt, hender det imidlertid at det opprinnelige bildet beholdes.[42] Dette er også tilfellet med ICAOs biometriske pass (se kapittel 4.6 for mer om dette).

De tre første fasene (innsamling, behandling og lagring) kalles også for *innrullering*.

3.1.4 Sammenligning

Når en biometrisk prøve sammenlignes med en forhåndslagret mal, resulterer det i en poengsum. En beslutning om "godkjent" eller "avvist" baseres deretter på hvorvidt denne poengsummen overstiger en viss terskel.

Vi kan skille mellom to typer sammenligning:

- *Identifisering*, som er en én-til-mange prosess hvor en biometrisk prøve sammenlignes med alle lagrede maler for å fastslå identiteten til den som avga prøven.
- *Verifisering,* hvor en biometrisk prøve fra en viss identitet sammenlignes med den lagrede malen til den samme identiteten, for å bekrefte at den som avga prøven er den som han eller hun hevder å være (én-til-én).

Det finnes to feilkilder når det gjelder biometrisk sammenligning: Systemet kan feilaktig identifisere et individ i forhold til den påståtte identiteten. Dette kalles for *falsk positiv*. Dersom et biometrisk system mislykkes i å identifisere et individ som er registrert i systemet, kalles det *falsk negativ.* Sannsynligheten for at systemet vil feilaktig identifisere et individ kalles derfor *feilakseptrate (False acceptance rate, FAR)*, mens sannsynligheten for at systemet vil mislykkes i å identifisere en som er innrullert kalles *feilavvisningsrate (False rejection rate, FRR).*[43]

En av utfordringene med å kalibrere et biometrisk system er at dersom du setter terskelen til et nivå hvor ingen blir feilaktig identifisert, vil avvisningsraten øke, og omvendt. Terskelen bør derfor innstilles på et nivå hvor både FAR og FRR ligger på et forsvarlig nivå for det gitte systemet.

Det er også en utfordring at mens andre autentiseringsteknikker kan tilby ulike grader av pseudonymitet eller anonymitet (for eksempel ved attributtautentisering), er dette ikke mulig med biometrisk autentisering.[44]

---

[42] Albrecht, A. (2003) *Privacy Best Practices in Deployment of Biometric Systems*
[43] ICAO TAGMRTD/NTWG (2004) Biometrics *Deployment of Machine Readable Travel Documents*
[44] Fra *Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"*

3.2 Fingeravtrykk

Fingeravtrykk er den mest anvendte formen for biometri og har blitt brukt til å identifisere forbrytere siden 1880-tallet.[45] Det er lett å bruke og har den fordelen at det allerede finnes store datamengder som kan brukes til å gjøre sammenligninger.

Hver finger har et unikt avtrykk, og siden de fleste individer har flere fingre, finnes flere alternativer hvis én av fingrene ikke lenger kan brukes. Dette betyr at *allmenngyldighets-kriteriet* oppfylles for denne formen for biometri. Det er noen unntak – fingeravtrykk kan slites bort ved arbeid eller nedfiling, men i slike tilfeller vil de vanligvis "gro tilbake". Noen mennesker har fingeravtrykk som ikke egner seg for biometrisk identifisering. Fingeravtrykk er også *egenartede* og er nokså *uforanderlige*. Elektroniske fingeravtrykkssensorer kan ta høykvalitets bilder, og biometriske systemer basert på fingeravtrykk tilbyr god *ytelse*. Når det gjelder *aksept* har fingeravtrykk vanligvis blitt forbundet med forbrytere, men i tråd med at flere forretningsforetak tar i bruk fingeravtrykk[46] (for bærbare datamaskiner, tilgang til treningsstudioer, osv.) vil aksepten sannsynligvis øke.

3.2.1 Hva er fingeravtrykkgjenkjenning?

Et fingeravtrykk består av trekkene og detaljene til en fingertupp. Fingeravtrykk har tre hovedtrekk: bue (arch), løkke (loop) og virvel (whorl). Hver finger har minst ett hovedtrekk. De underordnede trekkene (eller minutiae) består av posisjonen til rillenes endepunkter (rillene er linjene som flyter i ulike mønstre gjennom et fingeravtrykk) og til rilledelingene (punktet hvor rillene deler seg i to). Når fingeravtrykk sammenlignes på grunnlag av de tre hovedtrekkene kalles det mønstersammenligning, mens den mer mikroskopiske tilnærmingen kalles minutiaesammenligning.[46]

Den vanligste formen for fingeravtrykkbaserte biometriske systemer har to hoveddeler: sensoren og algoritmen som bearbeider bildet om til en mal for så å sammenligne denne med én eller flere lagrede maler.

For internasjonale sikkerhetsanvendelser er det for tiden et problem at de fleste systemer for fingeravtrykkgjenkjenning er basert på proprietære algoritmer tilknyttet sensor-produsentene. Dette betyr at for at systemet skal virke, må sensoren og algoritmen som brukes til å ta og lagre den biometriske malen være de samme som de som senere brukes til identifisering eller verifisering. På grunn av manglende interoperabilitet og standardisering på feltet, er ikke dette alltid mulig, særlig for politi- og grensekontrollsystemer hvor ulike land og organisasjoner er involvert. Som følge av dette må det opprinnelige bildet lagres i databasen til slike systemer (se kapittel 3.7 for mer om følgene av dette).

Eksempel: Biometrisk ombordstigning (SecBoard)[47]
SecBoard er et samarbeid mellom Lufthansa Systems og Bundesdruckerei. Når passasjeren innrulleres i systemet blir hans eller hennes fingeravtrykk registrert, digitalisert og lagret i et smartkort. Ved innsjekking avgir passasjerene fingeravtrykket sitt på nytt, og dette sammenlignes med fingeravtrykket på kortet. Hvis de to avtrykkene stemmer overens, kan

[45] Cole, S. A. (2004) *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*
[46] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[47] Beskrivelsen er basert på: Lufthansa Systems (2005) *Boarding with biometric data*

passasjeren gå ombord. Smartkortet bruker den samme sikkerheten som det biometriske passet, BAC (se kapittel 4.6.2). Lufthansa forventer at passasjerer med et elektronisk lesbart identitetskort i fremtiden vil kunne passere sikkerhetskontrollen raskere og enklere enn vanlige reisende.

Eksempel: Biometrisk ombordstigning (SAS)[48]
SAS vil innføre et system for biometrisk ombordstigning for å etterkomme krav som skal sikre at den personen som sjekker inn bagasje er den samme som går ombord i flyet. Dette gjøres ved å registrere passasjerens fingeravtrykk ved innsjekking. Avtrykket digitaliseres og malen blir lagret i en lokal database sammen med bagasjens ID. SAS sier at de kun lagrer 20 av de 180 målepunktene og at det er umulig å gjenskape fingeravtrykket basert på malen.

Passasjeren avgir så sitt fingeravtrykk på nytt ved ombordstigning, hvor det sjekkes opp mot databasen. Fingeravtrykket slettes fra systemet straks flyet har landet. Systemet er frivillig – passasjeren kan be om en manuell ID-sjekk istedenfor. Etter at systemet ble innført i Sverige, benytter 98% av passasjerene seg av dette.[49]

3.3 Ansiktskjennetegn

Ansiktet er et opplagt valg som biometrisk kjennetegn, siden det brukes av mennesker hver eneste dag for å gjenkjenne andre. *Ansiktsgjenkjenning* er den automatiserte prosessen med å sammenligne ansiktsbilder.

Når vi vurderer ansiktsgjenkjenning på grunnlag av de kriteriene som ble innført i innledningen til dette kapitlet, ser vi at metoden er god i forhold til *allmenngyldighet* (alle har et ansikt), *hvor lett det er å samle inn* (2D-ansiktsgjenkjenning bruker foto, som er lett å skaffe) og *aksept* (mennesker er vant med å bruke ansiktet til identifisering, og teknikken er ikke påtrengende).

Det er problemer med *egenart* og *uforanderlighet*, siden ansiktsmønstre ikke er så entydige som for eksempel fingeravtrykk, og de forandres over tid og under ulike forhold. Hår, briller, luer og skjerf – selv et smil – kan skygge for ansiktet. Teknologien er også følsom overfor lysforhold, positur og bildekvalitet. Ansiktsgjenkjenning har følgelig en mye lavere nøyaktighetsrate enn andre biometriske teknologier.

Ansiktsgjenkjennings *motstand mot omgåelse* kommer an på anvendelsen (se kapittel 3.3.1 for mer om *spoofing*). Den lave nøyaktighetsraten til ansiktsgjenkjenning gjør det også lettere for bedragere å bli feilaktig godkjent enn for eksempel med bruk av fingeravtrykk.[50]

Sensorer som oppfanger ansiktskjennetegn inkluderer:

- 2D-kamera (vanlig foto)
- 3D-kamera

[48] Beskrivelsen er basert på: Strande M. (2006) *Ingen finger-id på norske flyplasser* og Halvorsen, F. (2006) *SAS får benytte fingeravtrykk*
[49] Strande M (2007) *Gi finger'n i sommer,* http://www.tu.no/data/article83840.ece
[50] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*

- Infrarødt kamera

Selv om ansiktsgjenkjenning fremdeles ikke er en moden teknologi, er det likevel dette biometriske kjennemerket ICAO har valgt som hovedkjennemerke i biometriske pass.

3.3.1 Automatisk ansiktsgjenkjenning

Systemer for automatisk ansiktsgjenkjenning fungerer slik at en persons bilde tas automatisk og sammenlignes med en database for identifisering eller verifisering. Siden identifisering av en tilfeldig person basert på denne teknikken ville kreve en veldig stor database og behandlingskapasitet utover det som i dag er praktisk mulig, brukes slike systemer vanligvis til å bekrefte at en person ikke er på en liste over for eksempel kjente forbrytere eller terrorister. Økningen i omfanget av videoovervåking i løpet av de siste 10 årene har ført til større interesse for anvendelsen av automatisk ansiktsgjenkjenning.

Tester gjennomført av det tyske magasinet *c't* viser at systemer kan lures av stillbilder eller videosløyfer.[51] En annen sikkerhetsbegrensning er den høye forekomsten av tvillinger. I tillegg til muligheten for spoofing, har en rekke andre argumenter blitt lansert mot automatiske ansiktsgjenkjenningssystemer:[52]

Stort potensial for misbruk
Integrerte automatiske systemer for ansiktsgjenkjenningsteknologi kan brukes til å spore individer. Dersom systemer som brukes av ulike organisasjoner kan samkjøres med hverandre, vil det være mulig å spore et individ fra sted til sted.

Informasjon kan ses i sammenheng med informasjon fra andre teknologier
Ansiktsgjenkjenning er den biometriske teknologien som krever minst samarbeid fra det enkelte individ. Dette betyr at det er større sjanse for at dine biometriske kjennetegn oppfanges uten at du vet om det. Informasjon fra ansiktsgjenkjenningssystemer kan også lett slås sammen med informasjon fra såkalte lokasjonssystemer.

Lav nøyaktighetsgrad
Teknologien har en lav nøyaktighetsgrad. Blant mulige ulemper er falske positive, hvor en person forveksles med en forbryter eller terrorist. På de fleste offentlige steder er forholdene for fotografering og gjenkjennelse langt fra ideelle, og dette gjør det mer sannsynlig at feil vil oppstå. I takt med at databasen med ansiktsbilder vokser, øker sjansene for et feilaktig treff.

Borgere er uvitende om overvåkingssystemenes virkemåte og funksjon
Befolkningen er dårlig informert om overvåkingskameraenes egenskaper. De vet stort sett ikke at egenskaper knyttet til helse og humør kan analyseres ved bruk av infrarøde bilder eller ved å analysere ansiktsuttrykk.

Personvernbevisste borgere har ingen reelle valgmuligheter
På de fleste offentlige steder er det vanskelig å gjøre publikum oppmerksom på kameraenes tilstedeværelse og egenskaper, og nærmest umulig å skaffe informert samtykke. Det å

[51] Thalheim et al. (2002) *Body Check*
[52] Agre, P. E. (2003) *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places*

ferdes på offentlige steder, som for eksempel offentlige kontorer eller knutepunkter for offentlig kommunikasjon, er knapt et selvstendig valg. Selv i privat sektor kan det være vanskelig å gjøre hverdagsoppgaver som matinnkjøp uten å registreres av et kamera.

Ikke alle land tar borgerrettigheter like alvorlig
Dersom ansiktsgjenkjenningsteknologier lanseres i land hvor borgerrettigheter står forholdsvis sterkt, blir det mer sannsynlig at de også vil tas i bruk i land hvor borgerrettigheter knapt finnes.

3.4 Iris

Iris (regnbuehinnen) er den fargede ringen rundt pupillen. Dette er et fysisk kjennetegn som kan måles og dermed brukes for biometrisk verifisering eller identifisering.

3.4.1 Irisgjenkjenning

Det er viktig å merke seg at det finnes to ulike metoder for bruk av øyet som biometrisk kjennetegn. Irisgjenkjenning er den nyeste metoden. En eldre, og svært ulik, metode er retinaskanning (netthinneskanning). Ved retinaskanning avbildes mønsteret til de røde blodkarene bak øyeeplet. Denne teknikken krever atskillig mer samarbeid fra brukeren, i tillegg til mer avansert optisk utstyr. Retinaskanning markedsføres ikke lenger aktivt.[53]

En irisskanning er et høykvalitets fotografi av irisen som tas med nærinfrarød (near-IR) belysning. Irisgjenkjenningssystemer bruker stort sett smalvinkelkamera, noe som forutsetter at brukeren posisjonerer øynene sine riktig i forhold til i kameraets synsfelt. Det påfølgende fotografiet analyseres for å lokalisere irisen, trekke ut informasjon om dens kjennetegn og dermed lage en biometrisk mal. Nåværende systemer kan operere med en rekkevidde på rundt 10-20 cm, men det finnes alternativer som opererer med en rekkevidde på 5 meter.[54]

Irisgjenkjenning fungerer veldig bra i forhold til kriteriene som ble nevnt tidligere i dette kapitlet. Alle mennesker (inkludert de blinde) har iris, med noen få unntak: Det mest opplagte er mennesker med aniridia, som er fraværet av en iris. Andre tilfeller er blinde som kan synes det er vanskelig å stille opp øynene på linje med kameraet, og de som lider av nystagmus (ufrivillige øyebevegelser).[53]

Det er vitenskaplig bevist at irismønstre er *egenartede*, og at de forblir *uforandret* fra spedbarnstadiet til alderdom, med unntak for effektene av noen øyelidelser. Nåværende sensorer kan ta høykvalitets bilder (*lett å samle inn*), selv om det kan være nødvendig med flere forsøk. Irisgjenkjenningssystemet tilbyr fremragende *ytelse*, selv i identifiseringsmodus med store databaser over innrullerte brukere.[54]

Nyere irisgjenkjenningssystemer er *vanskelige å omgå*, men teknologien sliter med å bli *akseptert* i befolkningen. Dette skyldes delvis en feiloppfatning om hvordan systemet virker – mange mennesker antar at irisen skannes med en laser som kan skade øyet. [54]

---

[53] Rejman-Greene, M. (2003): *BIOVISION Roadmap* issue 1.1
[54] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*

3.5 Automatiske identifiseringssystemer

Grunnleggende teknologier: *Ulike sensorer*
Biometri
Kommunikasjonsteknologier
Datalagring

Automatiske identifiseringsløsninger hjelper offentlige myndigheter å bruke fingeravtrykksanalyse, ansiktsgjenkjenning, bildebehandling og biometrisk informasjon til å identifisere, spore og overvåke individer.

Eksempel: EURODAC
EURODAC[55] er et EU-system som brukes i alle medlemsland (i tillegg til Norge og Island) for å sammenligne fingeravtrykkene til asylsøkere. Systemet gjør det mulig for medlemslandene å sammenligne fingeravtrykkene til asylsøkere eller noen som oppholder seg ulovlig i landet, for dermed å fastslå om vedkommende tidligere har søkt asyl i et annet land. EURODAC er det første felles AFIS-systemet (*Automated Fingerprint Identification System*) innenfor Den europeiske union, og det ble satt i drift i januar 2003.

Systemet består av en sentral database og et system for elektronisk overføring mellom de forskjellige medlemslandene og sentralenheten. Data som overføres inkluderer:

- Fingeravtrykk
- Det opprinnelige innreiselandet
- Sted og dato for asylsøknaden
- Kjønn
- Referansenummer

Data samles inn for alle asylsøkere over 14 år, og beholdes i inntil 10 år. Dersom vedkommende får innvilget statsborgerskap eller oppholdstillatelse i et medlemsland, eller forlater EURODAC-området, slettes informasjonen.

Eksempel: Guardia kontrollsystem
Dette danske systemet lager en tredimensjonal kopi av et menneskehode. Systemet kombinerer flere biometriske elementer som for eksempel 3D-ansiktsgeometri, hudteksturanalyse og temperaturmønster. Informasjonen lagres i en sentral database. Fordi systemet kan måle varmemønsteret i ansiktet ved å bruke et infrarødt kamera, kan det avsløre mulige sykdommer som forårsaker feber, som for eksempel SARS og fugleinfluensa.[56]

Eksempel: FaceIt
FaceIt-programvaren er tatt i bruk med sikkerhetskameraer på Keflavik flyplass på Island. Keflavik var den første flyplassen som innførte slik teknologi. Hensikten er å identifisere personer som befinner seg på listen over ettersøkte og forhindre at de går om bord i et fly.

---

[55] Informasjonen om EURODAC er basert på tilgjengelig informasjon fra Europakommisjonen.
[56] Informasjon fra www.guardia.dk

Systemet undersøker 80 ansiktskjennetegn og sammenligner så den påfølgende malen med en database over mistenkte terrorister og forbrytere. Etter seks måneders drift hadde ingen ettersøkte terrorister blitt identifisert på Keflavik.[57]

3.6 DNA-profilering

DNA, eller deoksyribonukleinsyre, anses kanskje for å være den fremste identifikatoren. Hver person bærer i seg en unik genetisk kode (med unntak for eneggede tvillinger). I motsetning til fingeravtrykk, finnes det ingen mulighet til å forandre en persons DNA ved kirurgi eller ved å file vekk avtrykkene.[58]

Det å ta en DNA-prøve fra en mistenkt anses for å være et brudd på legemlig integritet, og veldig strenge regler har blitt innført for å beskytte rettighetene til de mistenkte og i noen grad også til domfelte forbrytere. Dette skyldes ikke at det er spesielt traumatisk å avgi en DNA-prøve (for eksempel spytt), men at analysen og behandlingen av en DNA-prøve kan avsløre sensitiv informasjon om en person, som for eksempel arvelige faktorer og medisinske lidelser. Dersom en DNA-prøve lagres på ubestemt tid, kan fremtidig teknologi gjøre det mulig å trekke ut enda mer informasjon enn i dag.[59]

Det er en generell tendens til at DNA-profilering og DNA-identifisering brukes stadig mer i politiarbeid. Noen land tillater allerede at DNA samles inn fra alle som er dømt for en forbrytelse, selv de som er mindre alvorlige, mens andre land har begrenset det til forbrytere som har fått en dom over et visst nivå.

I Norge har det for eksempel kommet forslag om å øke politiets adgang til å lagre DNA-prøver fra alle som har blitt idømt fengselsstraff.[60]

DNA-databaser beskrives i kapittel 5.2.

3.7 Etiske problemstillinger knyttet til biometriske systemer

Artikkel 29-gruppen vedrørende databeskyttelse sier helt konkret at biometriske data er av en særlig karakter idet de vedrører et individs atferdsmessige og fysiologiske kjennetegn og gjør det mulig å foreta en entydig identifisering av vedkommende.[61]

Vi nevnte tidligere at ansiktsgjenkjenning kan brukes til å fange opp et individs følelsesmessige tilstand. Andre biometriske kjennetegn har også "bivirkninger" som kan være problematiske fra et etisk synspunkt.

Fingeravtrykk anses vanligvis for å være et nøytralt kjennetegn som kun kan brukes til identifisering og verifisering. Dette er imidlertid ikke tilfelle. Fra 1890-tallet har det blitt forsket på hvordan fingeravtrykkmønstre sammenfaller med rase, etnisitet og visse karaktertrekk som sinnssykdom og forbryterskhet. Faktisk ble klassifiseringssystemene som sorterer alle fingeravtrykkmønstrene inn i tre grupper – buer, løkker og virvler – hoved-

[57] Petrie, E. (2002): *Iceland places trust in face scanning*
[58] OECD Working Party on Information Security and Privacy (2004): *Biometric-based technologies*
[59] Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*
[60] Justis- og politidepartementet (2005) *NOU 2005:19. Lov om DNA-register til bruk i strafferettspleien*
[61] Article 29 Data Protection Working Party (2003) *Working document on biometrics*

sakelig utarbeidet for å kunne bruke fingeravtrykkmønstre som legemlige markører på arvelighet og karakter. En studie gjort av den norske biologen Kristine Bonnevie fant ut at asiater hadde en høyere andel av virvler, og en lavere andel buer enn europeere.[62] I tillegg er visse papillmønstre avhengige av kostholdet til personens mor i tredje måned av svangerskapet.[63]

Også visse kromosomforstyrrelser – som Downs syndrom, Turners syndrom og Klinefelters syndrom – er kjent for å være forbundet med typiske fingeravtrykkmønstre hos en person. Det er imidlertid viktig å slå fast at det ikke er mulig å avgjøre rase, etnisitet eller visse sykdomstyper direkte fra fingeravtrykket, men kun å oppgi en statistisk sannsynlighet. For eksempel viser en studie at 50 % av mennesker med en gitt type fingeravtrykk har en bestemt form for mageproblem.[62]

Iridologi er analysen av irisens tekstur. Iridologiens tilhengere hevder at systematiske forandringer i irismønsteret gjenspeiler helsetilstanden til alle kroppsorganene, en persons humør eller personlighet, og kan til og med avsløre en persons fremtid. Iridologi anses for å være tvilsomt av vitenskapsfolk, som ofte sammenligner det med å spå i hånden, og metoden er ikke anerkjent som medisinsk praksis.[64] Men visse sykdommer som grønn stær og regnbuehinnebetennelse kan diagnostiseres fra et (rå)bilde av irisen.[65]

Som tidligere nevnt er spoofing et av problemene knyttet til biometri. En måte å forsøke å unngå spoofing på er ved å iverksette tiltak for å gjenkjenne livstegn, såkalt *liveness detection*. Ved å overvåke livstegn som puls eller pupillrespons, blir biometriske apparater en kilde til sensitiv biometrisk informasjon:[66]

- Pupillresponsen avhenger av hvorvidt man er gravid, alderdom og om man har drukket alkohol eller brukt legemidler/narkotika
- Forandringer i blodstrømmen forbindes både med en rekke medisinske tilstander og med følelsesmessig respons
- Nervøsitet kan gjenkjennes i stemmeleiet

Et avsluttende poeng er at bruken av biometri kan føre til at mennesker blir sosialt ekskludert uten grunn. Som nevnt under beskrivelsen av de forskjellige formene for biometri, gjelder det for de fleste slike teknologier at det finnes en liten andel som ikke kan innrulleres i et system som bruker den biometriske metoden de har et problem med.[67]

3.8 Sikkerheten til biometriske systemer

En av hovedfordelene med biometriske kjennetegn er at de er så sterkt knyttet til en person. De kan ikke mistes eller avsløres ved en tilfeldighet, slik som et passord eller en PIN-kode. Dette betyr at andre typer personopplysninger kan beskyttes bedre ved å bruke biometri enn ved tradisjonelle metoder. Biometrisk autentisering gir bedre adgangskontroll, og identitets-

[62] Cole, S. A. (2004) *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*
[63] Lyon, Hardenberg (2001) *Warum Neugeborene mehr wissen als Grosse manchmahl ahnen*
[64] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[65] Gasson et.al. (red.) (2005) *D 3.2: A study on PKI and biometrics*
[66] Fra www.biteproject.org
[67] Fra *Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"*

tyveri blir mye vanskeligere når personopplysninger knyttes utelukkende til den riktige personen.[68]

Ironisk nok er dette også den største ulempen ved biometriske systemer. Straks et sett med biometrisk data kompromitteres (for eksempel stjeles), er det kompromittert for alltid. For autentiseringssystemer basert på fysiske gjenstander som nøkler og skilt, kan en kompromittert gjenstand lett annulleres og brukeren tildeles en ny gjenstand. På tilsvarende måte kan brukernavn og passord byttes så ofte som nødvendig. Men brukeren har kun et begrenset antall biometriske kjennetegn (i de fleste tilfeller ett ansikt, ti fingre, to øyne). Dersom de biometriske data kompromitteres, kan brukeren gå tom for biometriske kjennetegn som kan brukes til autentisering.[69] I tilfeller av identitetstyveri ville det være veldig vanskelig for offeret å bevise misbruk fra en bedrager.

Truslene mot et system varierer med anvendelsen. I adgangskontroll er faren typisk den at noen prøver å få adgang ved å utgi seg for å være en som er innrullert i systemet. For andre anvendelser, som visum- og innvandringssystemer, er problemet et annet – brukere prøver å utgi seg for å være en annen enn seg selv (men ikke nødvendigvis en bestemt person), slik at de ikke skal gjenkjennes av systemet. Dette er stort sett lettere enn å gi seg ut for å være en annen, spesifikk person.[70]

3.8.1 Spoofing (forfalskning og omgåelse)

Det har blitt utført en rekke uformelle undersøkelser av forskjellige fingeravtrykkssystemer, og undersøkelsene viser at systemene kan overlistes (bli *spoofed*) ved å reaktivere latente avtrykk (avtrykket til den siste personen som brukte apparatet), bruke kunstige fingre, osv. En måte å sikre systemet mot omgåelse kan være å bruke enten flere fingre, krypteringsteknikker eller tiltak for å sjekke etter livstegn.[71] Automatiske ansiktsgjenkjenningssystemer har blitt overlistet ved bruk av stillbilder eller videosløyfer.

3.8.2 Sikkerhet ved DNA-profilering

DNA-prøver er vanskelig å overliste gitt visse forhold (prøvene samles inn under tilsyn uten mulighet for datakorrumpering). Dersom prøveinnsamlingen gjøres uten tilsyn, kan imidlertid en bedrager innlevere DNA-en til hvem som helst. Vi etterlater DNA-spor overalt hvor vi går (et hårstrå er nok til gi en prøve) og derfor er det umulig å unngå at andre får tilgang til DNA-prøver fra en selv.[71]

[68] Albrecht, A. (2003) BIOVISION: *Privacy Best Practices in Deployment of Biometric Systems*
[69] Ratha, Connell og Bolle (2001) *Enhancing security and privacy in biometrics-based authentication systems*
[70] Rejman-Greene, M. (2003): *BIOVISION Roadmap issue 1.1*
[71] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*

Kapittel 4 Sensorteknologier

En *sensor* er en innretning som konverterer en egenskap fra den fysiske verden om til et elektrisk signal.[72] En slik egenskap kan være varmeenergi, elektromagnetisk energi, akustisk energi, trykk, magnetisme eller bevegelse.[73]

En sensor som kan operere uten innsignal fra en operatør eller et annet system kalles *autonom*. Slike sensorer kalles også *selvorganiserende* eller *selvstyrende*. Vi skiller også mellom *aktive* og *passive* sensorer, og mellom *mobile* og *stasjonære* sensorer.[74]

En aktiv sensor avgir energi som reflekteres når den treffer en gjenstand. Sensoren mottar og analyserer deretter den reflekterte energien. Radar er et eksempel på en aktiv sensor. En passiv sensor avgir ikke energi, men mottar energi som på en eller annen måte angir menneskelig tilstedeværelse eller annen aktivitet.

Vanlige sensorteknologier inkluderer:

- Biosensorer
- Kjemiske sensorer
- Sensorer for ioniserende stråling (dvs. radioaktiv stråling, røntgenstråler)
- Elektrooptiske sensorer (kameraer)
- Akustiske sensorer (mikrofoner)
- Radarer
- Terahertzteknologier
- Elektromagnetiske sensorer
- Mekaniske sensorer
- Varmesensorer
- Radiofrekvensidentifisering (RFID)

Mange sikkerhetsanvendelser er basert på sensorer, slik som skannere som sjekker etter våpen og sprengstoff på flyplasser, radarer og forskjellige anvendelsestyper forbundet med RFID, som biometriske pass. Senere i kapitlet vil vi gi en mer detaljert beskrivelse av noen av sensortypene som er mest relevante for sikkerhetsteknologier.

---

[72] Wilson, D. H. (2005): *How to survive a robot uprising. Tips on defending yourself against the coming rebellion*
[73] Se *FS 1037C. Federal Standard*, 7. august, 1996
[74] De generelle beskrivelsene av sensorene er for det meste basert på Berg et al. (2004) *Autonomous sensor systems. Communication needs for independent sensors*

4.1 Sensorer som brukes til skanning

4.1.1 Sensorer for ioniserende stråling

Ioniserende stråling er stråling som inneholder nok energi til å fjerne ett eller flere elektroner fra et atom eller molekyl. Dette inkluderer radioaktiv stråling, røntgenstråling og kortbølge ultrafiolett stråling.

En anvendelse som brukes i for eksempel flyplassikkerhet er *XBT-teknologier* (*X-ray Backscatter Technologies*), som benytter aktive sensorer med høyenergi røntgenstråling til å ta bilder av gjenstander som er laget av materialer med ulik tykkelse. Dette vil avsløre hva som ligger skjult under klærne til en person. Den vanligste sikkerhetsanvendelsen er å identifisere skjulte våpen eller sprengstoff, men i praksis vil det vise hvordan personen ser ut naken, hva de har i lommene sine, osv. Dette kan avsløre mye om vedkommendes privatliv, og det ses dermed på som en krenkelse av personvernet.

4.1.2 Terahertzteknologier

Frekvenser fra 0,1 til 10 THz anses for å være THz-stråling.[75] THz-systemer kan brukes til å overvåke offentlige anlegg og tettbefolkede bygninger på jakt etter giftige industrikjemikalier, kjemiske virkestoffer og sprengstoff.

Fordi terahertzstråling har bedre gjennomtrengning i materialer enn optiske stråler, kan den brukes til å avsløre og avbilde våpen som er skjult under klær. Bildet skapes fra refleksjons- og absorpsjonsmønsteret til terahertzbølgene. Strukturdybden kan beregnes ved tidsforskyvningen mellom når bølgen ble strålt ut og når den ble reflektert tilbake.

Ved siden av å sørge for strukturell informasjon, kan terahertzbølger identifisere materialer. Forskjellige molekyler absorberer og reflekterer terahertzbølger på en gjenkjennelig måte, noe som kan kalles for et *terahertzfingeravtrykk.*[76] Dette vil for eksempel gjøre det mulig å skille Semtex fra modelleire. Med hensyn til personvern gjelder de samme utfordringene som med ioniserende stråling.

Eksempel: "Nakenmaskinen"
En nakenmaskin (*naked machine)* bruker sensorteknologier som XBT til å avsløre at noen bærer skjulte våpen eller skjult sprengstoff på sin person. Forskjellige systemer er i bruk. Noen systemer avslører alt under klærne, ikke bare skytevåpen og sprengstoff – derav navnet nakenmaskinen. Denne formen for flyplassikkerhet har blitt utprøvd på Heathrow (Terminal 4) siden 2004.[77] Andre anvendelser avbilder de skjulte gjenstandene og kopierer bildene over på en nøytral modell. Skannere som brukes på denne måten vil kunne redusere bruddene på personvern, fordi de vil begrense behovet for kroppsvisiteringer.[78]

---

[75] Innholdet i dette avsnittet er hovedsakelig basert på informasjon fra Argonne National Laboratory, US, Homeland Security Applications. http://www.et.anl.gov/sections/sinde/highlights/homeland_security.html
[76] Begrepet stammer fra Dr. David Cumming, lederen for Microsystems Group ved University of Glasgow, i The Royal Society: *Superhuman vision – seeing with terahertz*. http://www.royalsoc.ac.uk/exhibit.asp?id=4661&tip=1
[77] Gadher, D. (2004) *Plane passengers shocked by their X-ray scans*
[78] Fra *Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"*

Eksempel: PROBANT
PROBANT (People Real-time observation in buildings: Assessment of new technologies in support of surveillance and intervention operations) er et PASR 2005-prosjekt. Det fokuserer på utviklingen, integreringen og valideringen av teknologier som gjør operatørene i stand til å observere individer som befinner seg inne i bygninger og spore dem i sanntid. I tillegg til å lokalisere og identifisere mennesker som ligger skjult bak vegger, kan målinger av biometriske verdier bidra til å avgjøre om disse menneskene er i live, nervøse, sovende, osv.[79]

4.2 Elektrooptiske sensorer

Denne sensortypen er følsom for lys i området fra ultrafiolett (UV) til infrarødt (IR). Typiske anvendelser inkluderer to- og tredimensjonal bildedannelse, måling av stråleintensitet og strålетemperatur, bevegelsessporing og avstandsidentifisering av forskjellige materialer. Elektrooptiske sensorer inkluderer vanlige kameraer og videokameraer, da disse i realiteten er sensorer som opererer med synlig lys.

Selv små varmekameraer kan brukes til å spore mennesker på lang avstand, i spennvidden mellom noen hundre meter og opp til noen kilometer. FLIR-teknologi (*Forward Looking Infrared*) kan brukes for kameraovervåking under særdeles dårlige lysforhold. Passive infrarøde bevegelsesdetektorer kan brukes til skjult overvåking.

De fleste elektrooptiske sensorteknologier i dag opererer på bestemte plattformer med liten mulighet for kommunikasjon seg imellom. Det spås at fremtidige systemer vil være plattformuavhengige, med et felles grensesnitt til et kommunikasjonsnettverk og beslutningssystem.[80]

4.2.1 Videoovervåking

Grunnleggende teknologier: *Elektrooptiske sensorer*
Databaser
Ansiktsgjenkjenning
Mønstergjenkjenning

Videoovervåking er i realiteten en anvendelse av elektrooptiske sensorer (kameraer). Idéen om å bruke fjernsyn til å hjelpe politiet går langt tilbake i tid: i 1947 ble det foreslått at politiet burde få tillatelse til å "evaluere" BBCs dekning av det kongelige bryllup i London for å bistå i utplasseringen av patruljerende politibetjenter. I 1960 satt Metropolitan Police i London opp to kameraer på Trafalgar Square for å overvåke folkemengden under et statsbesøk til Parlamentet. I takt med at videoopptakeren ble kommersielt tilgjengelig på 60-tallet skjedde det en vekst i bruk av videoovervåkingsutstyr i detaljhandelen.[81]

Denne formen for overvåking av offentlige områder er utbredt i Europa, men graden av overvåking på åpne gater varierer veldig – fra over 500 systemer i London til ingen i

[79] Fra PROBANT-prosjektets beskrivelse: http://ec.europa.eu/enterprise/security/doc/project_flyers/766-06_probant.pdf
[80] Berg et al. (2004) *Autonomous sensor systems. Communication needs for independent sensors*
[81] Norris, McCahill, Woods (2004) *Editorial. The Growth of CCTV: A global perspective in the international diffusion of video surveillance in publicly accessible space*

København.[82] I takt med at videoovervåkingssystemer blir mer avanserte, blir det også lettere å foreta skjult overvåking.[83]

Forskjellige typer videoovervåkingssystemer
Kameraovervåking kan deles inn i to kategorier: Aktive kameraer og passive kameraer. Bare et fåtall av kameraene vi ser i hverdagen er aktive.[84]

Med *aktive kameraer* følger en operatør med på en tv-skjerm og kan kontrollere kameraet (dreie, vippe, zoome) for å følge et individ eller en situasjon som utvikler seg. Med kameraer av høy kvalitet kan en polititjenestemann komme mye nærmere en situasjon enn ved å faktisk være tilstede på gaten. Aktive kameraer kan brukes sammen med automatiserte visuelle overvåkingsprogrammer som bruker algoritmer til å oppdage mistenkelige bevegelser eller identifisere mennesker ved å sammenligne bildet deres med en referansedatabase (se kapittel 3.3.1).

Passive kameraer tar opp på bånd det som skjer på et bestemt sted (for eksempel i en kiosk). Båndet spilles kun av dersom en situasjon oppstår, for eksempel et ran, en slåsskamp, osv. I mange tilfeller har filmen blitt brukt så mange ganger (i Norge må båndet slettes etter 7 dager, og brukes da vanligvis om igjen) at det nesten er umulig for politiet å bruke opptaket dersom det har oppstått en situasjon som må granskes. I mange tilfeller virker ikke passive kameraer, eller de er narrekameraer som har til hensikt å skremme bort uønsket aktivitet. Enkelte steder vil til og med sette opp oppslag om at området er videoovervåket, men la være å investere i selve utstyret. I systemer som inneholder både aktive og passive kameraer, brukes i praksis bare de aktive kameraene.

Vi bør også skille mellom *privat* og *offentlig* kameraovervåking: Offentlig overvåking er den som gjøres av politiet i systemer som overvåker åpne gater. Privat overvåking på offentlige steder som butikksentre, banker og stasjoner gjøres vanligvis av private sikkerhetsselskaper.

Forskjellige anvendelser av videoovervåking
Videoovervåkingssystemer kan brukes av forskjellige grunner:[85]

- *Overvåking av offentlige områder*
  Dette gjøres stort sett ved å bruke aktive kameraer med høy oppløsning.
- *Opptak av situasjoner*
  Situasjonene tas opp for å brukes som bevis og for å bistå i undersøkelser.
- *Målrettet overvåking*
  Overvåkingen av områder hvor en mistenkt forventes å være.
- *Allmennprevensjon*
  For å avverge forbrytelser, eller for å flytte slik virksomhet annetsteds. Narrekameraer og falske oppslag om overvåkingssystemer er også en del av en slik strategi.

---

[82] Hempel og Töpfer (2004) *CCTV in Europe*
[83] European Parliamentary Technology Assessment Network (2006) *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries*
[84] Fra intervju med Heidi Mork Lomell, 18. mai 2006
[85] Parliamentary Office of Science and Technology (2002) *Postnote number 175: CCTV*

Det er også noen utfordringer knyttet til det å bruke bilder fra videoovervåking som bevismateriale.[86] Den første utfordringen er at politiet må finne frem til bildet. Der hvor videoovervåkingssystemer samler mye materiale, må politiet kanskje gå gjennom tusenvis av timer med videoopptak for å finne de relevante bildene. Det andre problemet er at bildene ofte er av dårlig kvalitet. Selv med bilder av bra kvalitet, kan det være vanskelig å bruke videoovervåkingsbilder når vitner skal identifisere mistenkte. Forskning viser at det er veldig vanskelig å kjenne igjen ukjente mennesker på grunnlag av videoovervåkingsbilder.[87] Dette står i motsetning til identifisering av kjente ansikter, som ofte blir identifisert nøyaktig, selv med opptak av dårlig kvalitet.

Mens de tidligste videoovervåkingssystemene var analoge, blir digitale systemer nå stadig mer utbredt. Digitale bildesøk kan spare tid når man skal finne bestemte situasjoner eller spore mistenkte i en eksisterende database. I 1998 bemerket det britiske Overhusets vitenskaps- og teknologikomité hvor lett det er å kopiere eller manipulere digitale bilder, selv på datamaskiner som brukes i hjemmet.[88] Selv om ekthet kan fastslås gjennom å bruke revisjonsspor eller vannmerker, er muligheten for bildemanipulasjon fortsatt bekymringsfull.

Intelligent Video Management/Automatisk overvåking

Grunnleggende teknologier:	*Elektrooptiske sensorer* *Databaser* *Ansiktsgjenkjenning* *Mønstergjenkjenning*

Intelligent Video Management-systemer er systemer som kan programmeres til å ta opp og markere forhåndsdefinerte hendelser (for eksempel utløsing av en alarm, bevegelse i et definert område, osv.), personer (basert på ansiktsgjenkjenning), kjøretøy eller andre gjenstander (definert for eksempel ved størrelse).

Automatisk overvåking er nært beslektet med slik Intelligent Video Management. Idéen er å knytte videoovervåkingssystemer opp til databaser som inneholder tilsvarende informasjon som beskrevet ovenfor. Dette kan brukes til å spore menneskers bevegelser, og innebærer som sådan en trussel mot personvernet. Eksempler på slike systemer er:[86]

Automatisk ansiktsgjenkjenning (AFR)
Det finnes automatiske systemer som kan korrelere videoovervåkingsbilder med digitale fotodatabaser (se kapittel 3.3.1). Automatisk ansiktsgjenkjenning kan brukes til å utløse alarmer når individer på en overvåkingsliste går inn i et område som er bevoktet av overvåkingskameraer.

Et mulig fremtidig scenario er å bruke AFR-systemer til å kjenne igjen en person, og så bruke identiteten til å få tilgang til – og samle inn – ytterligere informasjon fra andre offentlige databaser. Dette er ikke praktisk mulig i dag, men politiet i Oslo bruker en "lett" utgave av et

[86] Parliamentary Office of Science and Technology (2002) *Postnote number 175: CCTV*
[87] Henderson, Bruce og Burton (2001) *Matching faces of Robbers captured on Video*
[88] The House of Lords (1998) *Fifth report of the House of Lords Science and Technology Select Committee*

slikt system, hvor datasystemer brukes aktivt i samspill med kameraene.[89] Hvis de for eksempel ser en bil som har blitt parkert på en mistenkelig måte, sjekker de bilregisteret AUTOSYS for å finne ut hvem eieren er. De kan deretter sjekke politiets database for å se om eieren har et kriminelt rulleblad. Dersom han ikke har det, kan de sjekke familieforbindelsene hans i folkeregisteret og finne ut om han har en sønn/fetter/søster/osv. med kriminelt rulleblad. På dette grunnlaget kan de vurdere situasjonen og hvordan de skal opptre. Dette er ikke så effektivt som en automatisert prosess kan tenkes å være i fremtiden, men det betyr fortsatt at det er mulig å danne et meget omfattende bilde av en person gjennom dagens teknologier.

Automatisk bilskiltgjenkjenning (Automatic Number Plate Recognition, ANPR)
ANPR-systemer leser bilskilt som er tatt opp ved videoovervåking og sammenligner dem med en database. Det kan være vanskelig for systemene å kjenne igjen bilskilt som ikke samsvarer med forhåndsbestemte spesifikasjoner (f.eks. bokstavstørrelse eller font) – slik at utenlandske og forfalskede bilskilt kan bli oversett eller feiltolket av systemet.[90] ANPR-systemer er i bruk i en rekke land, ofte i forbindelse med bomstasjoner eller fotobokser.

Sporing og identifisering av mistenkelig atferd
Systemer kan spore individer og gjenstander (f.eks. biler) fra kamera til kamera og gjøre operatørene oppmerksomme på situasjoner som trengsel eller vandalisme. Automatiserte gjenkjenningsteknologier han spore "mistenkelig atferd" eller få øye på mistenkelige pakker.[91] Mennesker som er i ferd med å hoppe foran et tog har et typisk bevegelsesmønster som kan programmeres inn i systemet. Det samme gjelder for mennesker som er i ferd med å bryte seg inn i en bil på en parkeringsplass – de beveger seg på en helt annen måte enn mennesker som har legitime gjøremål på det samme stedet. På den annen side er lommetyver praktisk talt umulige å få øye på og programmere mønstre for. Det samme gjelder overraskende nok for ran, mens slåsskamper er lette å få øye på. ADVISOR-prosjektet har arbeidet med å bruke dataalgoritmer til å avsløre uvanlig menneskelig atferd, som vandalisme og slåsskamper. Prosjektet viste en meget høy gjenkjenningsgrad (89 %) for de definerte atferdsmønstrene, og en meget lav grad av falske alarmer (6,5 %).[92]

For tiden forsker PASR 2005-prosjektet ISCAPS (Integrated Surveillance of Crowded Areas for Public Security) på automatisert overvåking av tettpakkede områder gjennom å analysere mønstre for mistenkelig atferd.

4.3 Akustiske sensorer

Akustiske sensorer registrerer vanligvis lyd gjennom én eller flere mikrofoner. Lyden blir så digitalisert og bearbeidet før den overføres til en sentralenhet for å analyseres. Når den produserer resultatet, kan sentralenheten ta i betraktning ytre faktorer som trafikkstøy, været, osv. Lydsensorer er vanligvis passive og av liten størrelse, og de er derfor vanskelige å identifisere.

[89] Fra intervju med Heidi Mork Lomell, 18. mai 2006
[90] Parliamentary Office of Science and Technology (2002) *Postnote number 175: CCTV*
[91] Tendler, S. (2005) *"Smart" CCTV could fight terrorist threat in stations*
[92] Naylor og Attwood (2003): *Annotated Digital Video for Intelligent Surveillance and Optimised Retrieval*

Lydsensorer kan brukes til en rekke oppgaver, inkludert avstandsmåling (sonar) og oppsporing av kjemikalier, men deres mest interessante egenskap i forhold til overvåkning er sannsynligvis avlytting med skjult mikrofon, hvor ulike mikrofontyper tas i bruk.

4.3.1 Avlytting

Grunnleggende teknologier: *Akustiske sensorer*
Elektrooptiske sensorer

Begrepet avlytting brukes om skjult overvåking av samtaler gjennom bruk av teknisk utstyr. Vanligvis vil mikrofoner utstyrt med sendere eller opptaksutstyr plasseres i et rom hvor den mistenkte forventes å oppholde seg, og den avlyttede samtalen vil overføres til en nærliggende lytterpost. Avlyttingen kan også utføres med retningsmikrofoner eller annet utstyr som kan brukes på avstand (for mindre mikrofoner ca 100 meter, og for parabolmikrofoner opptil 300 meter). En mer omfattende utgave av slik avlytting er å installere skjulte kameraer i rom eller områder hvor en mistenkt forventes å oppholde seg.

Avlyttingsoperasjoner består vanligvis av tre hoveddeler:[93]

- *Opptaksutstyr:* En mikrofon, et videokamera eller et annet apparat tar opp lyd eller videobilder. Det er mulig å bearbeide opptaket, for eksempel å filtrere vekk bakgrunnsstøy.
- *Overføring:* Lyden og/eller videobildet må på en eller annen måte sendes til lytterposten. Dette kan gjøres trådløst eller over en overføringslinje. Sendeutstyret kan være i kontinuerlig drift eller, i mer avanserte operasjoner, fjernstyres.
- *Lytterpost:* Dette er et sikkert område hvor signalene kan overvåkes, tas opp eller videresendes til et annet område for behandling. Lytterposten kan være så nær som naborommet eller så langt unna som noen kvartaler.

Etter loven kan avlytting bare gjøres av politiet etter en rettslig fullmakt. På grunn av den voldsomme økningen i miniatyrteknologi, har avlyttingsutstyr aldri vært billigere eller lettere tilgjengelig. Både miniatyrisert avlyttingsutstyr og retningsmikrofoner er kommersielt tilgjengelige fra en rekke såkalte "spy shops".[94]

Selv i lovlige operasjoner iverksatt av politiet er det alltid en risiko for at samtalene til uskyldige tredjeparter vil bli tatt opp som en del av avlyttingen. Nylig har både Norge og Danmark vedtatt lover som vil gjøre det lettere for politiet å bruke avlytting og andre metoder for hemmelig etterforskning.[95]

---

[93] Texas A&M Research Foundation *Employee's guide to security responsibilities. Bugs and Other Eavesdropping Devices*
[94] Se for eksempel http://www.endoacustica.com/ eller http://www.thespystore.com/microphones.htm
[95] Justis- og politidepartementet (2005) *Ot.prp. nr. 60 (2004-2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)* (for Norge) og Det danske utenriksdepartementet (2004) *En verden i forandring - nye trusler, nye svar. Redegørelse fra regeringen om indsatsen mod terrorisme (for Danmark)*

Eksempel: Lydgjenkjenningssystemer
Myndighetene i Chicago har tatt i bruk ny teknologi som kan kjenne igjen skudd, dreie et overvåkingskamera i retning av gjerningsmannen og ringe nødnummeret. 30 slike apparater har blitt installert i nabolag med mye kriminalitet. Det planlegges også å prøve ut systemet i en rekke andre amerikanske byer.[96]

Slike systemer kan også programmeres til å kjenne igjen andre lyder enn skudd. *Sigard* er et lydgjenkjenningssystem som er programmert til å avdekke truende munnbruk.[97] Systemet brukes for tiden på 300 steder i Nederland (bl.a. i Amsterdam og Groeningen) og vurderes nå av britiske myndigheter i forkant av OL i 2012.[98] Mikrofonene kan avsløre lyd på 300 meters avstand og ta opp aggressive samtaler før de blir voldelige.

4.4 Ubemannede luftfartøy (Unmanned Arial Vehicles, UAV)

Grunnleggende teknologier: *Elektrooptiske sensorer*
Radarer
Ulike andre sensorer
Kommunikasjonsteknologier

UAV defineres som et motordrevet luftfartøy som ikke har en menneskelig pilot ombord, bruker aerodynamiske krefter til å få oppdrift, kan fly autonomt eller fjernstyres, kan ofres eller hentes tilbake og kan frakte dødelig eller ikke-dødelig nyttelast.[99]

UAV-er kan som regel utstyres med overvåkingskameraer med varme- og mørkesyns-egenskaper. Elektrooptiske sensorer (kameraer) kan identifisere en gjenstand på størrelse med en melkekartong fra en flyhøyde på 60.000 fot. UAV-er kan utstyres med radarsystemer for å ta høyoppløsningsbilder som kan overføres til en bakkestasjon. Til en viss grad kan bevegelige mål spores.[100] Forskjellige UAV-er kan fly i 20-50 timer uten å måtte etterfylle drivstoff. Flyene kan også kan utstyres med målrettede våpensystemer.[101]

Mini UAV-er (MAV-er) er UAV-er som kan bæres av en politibetjent eller soldat til bruk i områder hvor det er vanskelig å få et overblikk fra stor høyde. MAV-en er laget for å operere på bakken eller i høyder opptil ca. 150 meter. De har en driftstid på rundt én time, og opererer i opptil 10 km fra utskytingspunktet. Bærbare UAV-er har blitt sammenlignet med en avstandskikkert som kan se bak en åskam.[102] På bakken kan MAV-en opptre som en sensor og samle inn data på samme måte som i luften.

Det har vært antydet at slike fartøy i fremtiden vil kunne brukes til sivile overvåkings-formål.[103]

---

[96] Reichgott, M. (2005) *Chicago Pairing Surveillance Cameras with Gunshot Recognition Systems*
[97] Se http://www.soundintel.com/products.html
[98] The Sunday Times (2006): *Word on the street ... They're listening*
[99] Definisjonen er fra USA Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02
[100] Bolkcom, C. (2005) *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*
[101] EPIC (2005) *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking*
[102] Sweetman, B. (2005) Mini *UAVs – the next small thing?*
[103] Surveillance Studies Network (2006) *A Report on the Surveillance Society*

4.5 Radiofrekvensidentifisering (RFID)

Grunnleggende teknologier: *RFID*
Ulike sensorer
Lagringsteknologi
Beslutningsstøtte
Kommunikasjonsteknologier

RFID er et begrep for automatisk identifisering ved bruk av radiobølger. Ørsmå integrerte kretser som inneholder informasjon knyttes til dokumenter eller innlemmes i produkter eller emballasje. En leser kan deretter brukes til å lese informasjonen på RFID-brikkene som er innenfor rekkevidde. Et fullstendig RFID-system vil vanligvis omfatte brikker, lesere, et databasesystem og noen ganger også en form for beslutningsstøttesystem.

Hvert RFID-system defineres ut fra følgende tre kjennetegn:[104]

- *Elektronisk identifisering*:
  Systemet muliggjør en entydig merking av gjenstander eller personer ved hjelp av elektronisk lagrede data.
- *Kontaktløs dataoverføring:*
  Data som identifiserer gjenstanden kan trådløst leses gjennom en radiofrekvenskanal.
- *Overføring ved forespørsel (på anrop):*
  En merket gjenstand overfører data bare når en motsvarende leser igangsetter denne prosessen.

4.5.1 Hva består et RFID-system av?

Et RFID-system består av tre grunnelementer: en RFID-transponder (også kalt en brikke eller krets), en RFID-leser, og eventuelt også et datanettverk som brukes til å knytte leserne sammen.[105]

Datainnsamlingen gjøres av sensorer. Data som er lagret på brikken overføres til en leser og eventuelt til en tilknyttet referansedatabase gjennom radioteknologi. Datalagringen realiseres på brikken og eventuelt ved det tilknyttede administrasjonssystemet. Data som er overført til administrasjonssystemet kan videreanalyseres eller brukes til profileringsformål og beslutningsstøtte.

Brikken
Brikken, som er den grunnleggende byggeklossen i RFID, består av en antenne og en liten silikonbrikke som inneholder en radiomottaker, en radiomodulator for å gi tilbakemelding til leseren, kontrollogikk, en viss minnekapasitet og i noen tilfeller også strømforsyning. Brikken befinner seg på gjenstanden eller personen som skal identifiseres.

RFID-brikker finnes både som *aktive* og som *passive* brikker. Aktive brikker har eget batteri og vil derfor være større enn passive brikker, men de kan romme mer informasjon og virke

[104] German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems*
[105] Se den detaljerte tekniske beskrivelsen i Finkenzeller (2003) *RFID-Handbook*, 2. utgave, kapittel 3

på lenger avstand. Et typisk eksempel på aktive brikker er bompengebrikker, som gjør bomstasjoner i stand til å kjenne igjen og fakturere passerende biler.

Passive brikker inneholder ikke et batteri, men får den nødvendige energien fra leserens radiosignal. Typiske sikkerhetsanvendelser som benytter passive brikker er maskinlesbare reisedokumenter (biometriske pass) og ID-kort, men den vanligste anvendelsen av denne teknologien finnes i detaljhandelen, hvor RFID brukes i forsyningskjeden. I det sistnevnte tilfellet inneholder brikkene vanligvis bare en identifikator, og den egentlige informasjonen hentes fra en database. Passive brikker kan være veldig små, og en hovedbekymring er at brukere ikke vet at de bærer på en brikke eller når den leses.[106]

Brikker finnes i mange forskjellige former og størrelser. Hitachis Mu-chip[107] er mindre enn 0,44 mm på den ene siden og ble laget for å spore dokumenter som printes ut i kontor-omgivelser. Hitachi har også presentert en enda mindre brikke, som bare er 0,05 mm på hver side og som for det blotte øyet ser ut som pulverflekker.[108] Også VeriChip-en,[109] en implan-terbar brikke, er på størrelse med et riskorn og – siden det er en passiv brikke – har en veldig begrenset avlesningsrekkevidde.

Med tanke på overføring kan vi skille mellom *promiskuøse* og *sikre* brikker. Mens de fleste brikker er promiskuøse og kommuniserer med en hvilken som helst leser, krever sikre brikker at leseren oppgir et passord eller annen form for akkreditering før brikken overfører data til leseren. De fleste brikker, både aktive og passive, kommuniserer bare på forespørsel fra en leser.

Brikker kan utstyres med forskjellige typer minne:

- *Read-write*
  Mer avanserte RFID-brikker kan inneholde "read-write" minne. Dette betyr at inn-holdet i brikken kan endres av leseren. Slike brikker vil vanligvis ha en eller annen grunnleggende sikkerhetsmekanisme for å unngå uautoriserte dataendringer.
- *Read only*
  Skrivebeskyttede brikker kan bare leses av leseren, men ikke omprogrammeres. Slike brikker vil ofte bare inneholde et serienummer, og den egentlige informasjonen som er forbundet med den merkede gjenstanden er lagret i en database som er tilknyttet RFID-systemet.

Enkelte RFID-brikker har sensorer som gjør brikken i stand til miljøovervåking, som for eksempel temperatur, lufttrykk, luftfuktighet, bevegelse, biokjemiske virkemidler eller akselerasjon. Det er mulig å lagre sensorens resultater i et read-write minne som kan leses senere, men brikken kan også rapportere resultatene til RFID-leseren enten til forhånds-definerte tidspunkter eller når et forhåndsdefinert resultat inntreffer.[110]

---

[106] Article 29 Data Protection Working Party (2005) *Working document on data protection issues related to RFID technology*
[107] RFID Journal (2003) *Hitachi Unveils Smallest RFID Chip*
[108] BBC News (2007) *World's tiniest RFID tag unveiled*
[109] Se nettsiden til VeriMed Patient Identification: http://verimedinfo.com/patient_demo/
[110] Heinrich, C. (2005) *RFID and beyond. Growing your business through real world awareness*

Brikken kan også utstyres med en selvutslettende eller "kill"-egenskap som gjør merket inaktivt, med eller uten mulighet for gjenoppliving.

Leseren
En RFID-*leser* (transceiver/sender/mottaker) består av en radiofrekvensmodul, en kontrollenhet, og en tilkoblingsdel for utspørringen av elektroniske brikker gjennom bruk av radiofrekvenskommunikasjon.[111] Leseren sender en puls med radioenergi og lytter så etter brikkens respons. Energien oppdages av brikken, som i sin tur sender tilbake en respons som inneholder en unik identifikator (serienummer) og eventuelt annen informasjon. I enkle RFID-systemer virker pulsen med radioenergi som en av/på-knapp, mens den i avanserte RFID-systemer kan inneholde instrukser til brikken, passord eller instrukser til å lese eller skrive inn data som er lagret på brikken.

En RFID-leser står vanligvis på, idet den kontinuerlig sender ut radioenergi og venter på brikker som kommer innenfor dens operasjonsområde. Det er imidlertid mulig å konfigurere en RFID-leser slik at den sender en radiopuls bare når en ytre hendelse inntreffer.

I likhet med brikkene finnes lesere i ulike størrelser. Størrelsen kan variere fra størrelsen til en stasjonær datamaskin med flere antenner til lesere på størrelse med et frimerke som kan bygges inn i mobiltelefoner.

Administrasjonssystem
I mange RFID-systemer blir informasjonen som mottas av leseren sendt via et grensesnitt til et databehandlingssystem (eller administrasjonssystem). Avhengig av RFID-systemet kan dette ganske enkelt være en datamaskin som sammenliger det overførte serienummeret med en referansedatabase, eller systemet kan også være mer avansert og bestå av en rekke datamaskiner og servere.

4.5.2 Utfordringer med RFID

RFID-brikken vil ofte bare inneholde et unikt serienummer som muliggjør en entydig identifisering av brikken og dermed også den merkede gjenstanden. Gjennom å identifisere en gjenstand, kan vedkommende som bærer gjenstanden være identifiserbar.[112] Videre kan RFID-brikker også plasseres direkte på eller i den registrerte, for eksempel ved implantering, og dermed gjøre det mulig med en direkte identifisering av individer.

Avhengig av den enkelte RFID-teknologi, kan informasjon lagres på brikkene. Dersom informasjonen ikke er kryptert eller på annen måte sikret, kan den leses av enhver som er utstyrt med en RFID-skanner/leser.[113] I Norge ble det nylig avdekket at de siste 100 bomstasjonspasseringer blir lagret på bompengebrikkene. Denne informasjonen, som avslører bilens bevegelsesmønster, kan leses ved å bruke en helt vanlig leser.[114]

---

[111] Sarma, Weis og Engels (2003) *RFID Systems and Security and Privacy Implications*
[112] Se direktiv 95/46/EF, betraktning 26 om begrepet "identifiserbar": *"Beskyttelsesprinsippene skal gjelde enhver opplysning om en identifisert eller identifiserbar person; for å avgjøre om en person er identifiserbar, tas alle de hjelpemidler i betraktning som med rimelighet kan tenkes å bli tatt i bruk, enten av den registeransvarlige eller av enhver annen person, for å identifisere vedkommende."*
[113] Fra *Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"*
[114] Datatilsynet (2007) *Statens Vegvesen holdt tilbake viktig AutoPASS-informasjon*

Det finnes en rekke mulige angrep på RFID-systemer som er relevante for integriteten til dataen som overføres eller lagres, og dermed også for datakvaliteten. Sikkerheten til et RFID-system kan for eksempel krenkes av ondsinnet programkode (såkalt *malware*) som er plantet i administrasjonssystemet og som derigjennom får uautorisert tilgang til de lagrede dataene, eller ved å klone dataene som er lagret på brikken og simulere brikkens opprinnelige identitet. I forsøk har forskere også lykkes med å smitte administrative RFID-mellomvaresystemer gjennom RFID-merket.[115]

Angrep på RFID-systemer har vanligvis ett av følgende formål:[116]

- *Spionering*: Angriperen får uautorisert tilgang til informasjon gjennom for eksempel avlytting eller uautorisert tilgang til administrasjonssystemer.
- *Bedrageri*: Angriperen lurer operatøren eller brukeren av et RFID-system ved å mate systemet med desinformasjon.
- *Blokkering, for eksempel gjennom tjenestenekt (Denial of Service, DoS)*: Tilgjengeligheten til RFID-systemets funksjoner kompromitteres enten på lesernivået eller i administrasjonssystemet.
- *Skjerming eller å sette brikken ut av spill ved for eksempel å bruk av faradaybur eller ødelegging av RFID-brikken*: En brikke kan gjøres ulesbart gjennom bruk av for eksempel fysisk makt.

Eksempel: OpTag[117]
OpTag-systemet ønsker å feste RFID-brikker til flypassasjerer for å kunne finne passasjerer før ombordstigning. Systemet er ment å øke trygghet og sikkerhet, men også å forkorte tiden det tar for ombordstigning.

Hver brikke sender ut en puls to ganger i sekundet, og pulsen vil mottas av minst to lesere. Systemet utnytter det faktum at flere antenner mottar signalet fra hver enkelt brikke, og bruker signalvinkelen til å beregne brikkens posisjon. Det skal være mulig å spore passasjerer med en nøyaktighet på én meter og oppdatere informasjonen hvert sekund. Personlig informasjon i flyselskapets system, slik som passasjerenes navn, alder, kjønn og rutenummer, kan kobles til merkets unike ID-nummer.

Data fra RFID-systemet vil kobles sammen med bilder fra et panoramakamerasystem, slik at brikkens posisjon vises på bildet. Når tiden er inne for ombordstigning, kan systemet lage en liste over passasjerer som befinner seg langt borte fra utgangen, og flyselskapet kan da sende ansatte som er utstyrt med bilder og posisjonen for å finne passasjerene som er sent ute.

I fremtiden vil OpTag også kunne brukes til sikkerhetsformål i samspill med programvare for ansiktsgjenkjenning.

---

[115]Rieback et al (2006) *Is Your Cat Infected with a Computer Virus?*
[116]Se German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems*
[117]Denne beskrivelsen av systemet er basert på: Wessel, R. (2006) *Airport monitoring system combines RFID with video*

Systemet har blitt utviklet av et konsortium bestående av europeiske selskaper, og mottar støtte fra EU.

Eksempel: SECCONDD (Secure Container Data Device Standardisation)
SECCONDD[118]-prosjektet ser på denne formen for sikkerhetsteknologi i forhold til containere. Idéen er å utvikle et grensesnitt som gjør politiet og tollmyndigheter i stand til å lese sikkerhetsdata, inkludert informasjon som lagres fra interne sikkerhets- og lokasjonssensorer. Det vil dermed være mulig for dem å fastslå hvor containeren eller kjøretøyet har vært, hvorvidt gjenstander (f.eks. eksplosiver) eller mennesker har sluppet inn underveis, og hvorvidt farlige gjenstander kan befinne seg i containeren.

4.6 Maskinlesbare reisedokumenter (Machine Readable Travel Documents, MRTD)

Grunnleggende teknologier: *RFID*
Lagringsteknologi
Biometri
Kommunikasjonsteknologier

Et maskinlesbart reisedokument (MRTD) er et internasjonalt reisedokument (f.eks. et pass eller visum) som inneholder både data som kan leses av et menneske og maskinlesbare data. Alle land som har en kontrakt med Den internasjonale organisasjonen for sivil luftfart (ICAO) må ta i bruk maskinlesbare pass innen 2010. 110 land bruker slike pass i dag, og ytterligere 40 planlegger å oppgradere til en biometrisk utgave innen utgangen av 2006.[119] Maskinlesbare reisedokumenter har så langt (mars 2006) blitt innført i Belgia, Sverige, Norge og Tyskland.

Det finnes tre typer MRTD:[120]

- Et *pass* viser at personen er en borger av landet som utstedte passet
- Et *visum* viser at utstedelseslandet har gitt en person som ikke er en borger særretten til å reise inn og forbli i landet for en bestemt tidsperiode og i en bestemt hensikt
- *Andre reisedokumenter* er i hovedsak identifiserings-/grensekryssingskort som utstedes på særskilt grunnlag til personer som ikke er borgere.

Dette avsnittet vil hovedsakelig fokusere på *pass,* benevnt som *biometriske pass*. Anvendelsen av slike pass vil etter hvert berøre et stort antall mennesker: bare på ruteflyvninger flyr hvert år over 2 milliarder passasjerer!

En av hovedgrunnene til å innføre biometriske pass er behovet for å gjøre pass sikrere mot forfalskning, og for å gjøre grensekontroll mer pålitelig. Ifølge ICAO kan biometri brukes til å forbedre kvaliteten på bakgrunnssjekkene som utføres som del av søknadsprosessen for

[118]Secure Container Data Device Standardisation, PASR 2005
[119]ICAO MRTD Report Volume 1/Number 1 (2006)
[120]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*

pass, visa eller andre reisedokumenter, og biometri kan brukes til å styrke forbindelsen mellom reisedokumentet og personen det er utstedt til.[121]

Prosessen med å virkeliggjøre biometriske pass har også blitt drevet frem av USA. USA har insistert på at landene som ønsker å bruke Visa Waiver-programmet (hvor borgere ikke behøver å søke om visum for å komme inn i USA) må ha fått på plass et program for å plassere biometriske brikker i sine pass.[122]

De nye passene med integrerte kretser bør ikke ha en gyldighetstid på mer enn 10 år. ICAO anbefaler 5 år.

4.6.1 Komponentene i et biometrisk pass

Et biometrisk pass består av selve dokumentet, vanligvis i form av en liten bok, og en liten brikke.

Informasjonen i passet kan finnes på tre forskjellige steder:

- Den visuelle kontrollsonen (Visual Inspection Zone, VIZ). Dette området inneholder obligatoriske og valgfrie data i et oppsett som er bestemt av ICAO.
- Den maskinlesbare sonen (Machine Readable Zone, MRZ). Dette området inneholder elementer i en utforming og posisjon som er helt obligatorisk, i et standard format (OCR-B).
- Den integrerte brikkens logiske datastruktur (Locical Data Structure, LDS). Brikken inneholder obligatoriske og valgfrie data i en datastruktur som er bestemt av ICAO. Et symbol på passets forside viser at det inneholder en brikke.

I tillegg fungerer brukerens bilde som en visuell forbindelse mellom innehaveren og passet.

ICAO har utarbeidet et sett med kriterier for brikkene som skal brukes i passet.[123] De integrerte kretsene (brikkene) må være i henhold til ISO-standarden ISO/IEC 14443 (avstand mellom 0 og 10 cm) type A og B. Denne standarden har blitt valgt for å sikre global interoperabilitet og lesbarhet (dvs. at et pass skal kunne leses ved enhver grenseovergang). Brikken må også ha nok lagringsplass til å kunne romme den nødvendige informasjonen (se beskrivelsen av LDS senere i dette kapitlet).

ICAO har valgt å bruke en *kontaktløs brikke*, som betyr at den kan leses på avstand. Det kontaktløse systemet består av selve brikken, som integreres i reisedokumentet, og en leser. Leseren kommuniserer med brikken gjennom radiobølger, og kan ha enten kun lese- eller lese-/skrivefunksjon. Dersom det siste er tilfellet, kan brikken programmeres og deretter omprogrammeres via leseren. Leseren vil vanligvis være koblet til et datasystem.

---

[121] ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*
[122] Meints og Hansen (2006) *D 3.6 Study on ID Documents*
[123] ICAO (2004) *Use of Contactless Integrated Circuits in Machine Readable Travel Documents*

Frekvensen som brukes av ISO/IEC 14443-apparater er 13,56 MHz. Verken vann eller menneskelig vev absorberer radiobølger på denne frekvensen, så tilstedeværelsen av én eller flere mennesker, en hånd, fuktighet, osv. vil ikke påvirke leserens evne til å lese brikken. Lesing kan imidlertid forhindres ved å omslutte passet med metall, for eksempel aluminiumsfolie.

Den absolutt minste minnestørrelsen for å kunne bruke biometri i pass er 32K. Men fordi den teknologiske utviklingen på dette området skjer så fort, anbefaler ICAO at landene som utsteder biometriske pass bør ta høyde for brikker som er på 512K eller større.

Biometrien
ICAO har valgt *ansiktet* som det primære biometriske kjennetegnet som skal brukes i pass. Dette er obligatorisk og vil bli brukt verden over. *Finger* og *iris* anbefales som sekundære biometriske kjennetegn. Disse kan brukes dersom utstedelseslandet velger å gjøre det.

En rekke grunner oppgis til at ansiktet ble valgt som det primære biometriske kjennetegnet (se også kapittel 3.3): Ansiktsbildet er tilgjengelig for praktisk talt alle mennesker i verden. Ansiktet tillater også 100 % identitetsbekreftelse i kontrollprosessen, siden fotoet kan brukes ved maskinstøttede kontroller når et digitalt bilde ikke er tilgjengelig. Med fotoet kan dessuten ansiktsgjenkjenningen gjøres visuelt, selv når brikken, leseren eller behandlingssystemet ikke fungerer.

EU har valgt å basere sine anbefalinger for EU-passet på ICAO-standarden, med noen mindre justeringer. Ansiktet har blitt valgt som det primære biometriske kjennetegnet, og fingeren som det sekundære biometriske kjennetegnet. Iris er ikke del av EU-passet.[124]

Det primære fingeravtrykket som skal innlemmes i EU-passet er et vanlig avtrykk av den venstre og den høyre pekefingeren. Dersom det ikke lykkes å få gode avtrykk av disse fingrene, skal vanlige avtrykk av midtfingrene, ringfingrene eller tomlene registreres. Lagringsformatet er CBEFF (Common Biometric Exchange File Format).[124]

Én av hovedutfordringene med biometriske pass er interoperabilitet. Pass utstedes av mange ulike land, som bruker forskjellige leverandører, og alle pass må kunne leses ved enhver grenseovergang.[125]

Fordi globale standarder mangler for de biometriske verdiene som er valgt, har ICAO lagt ned påbud om å lagre selve bildet av det biometriske kjennetegnet i den logiske datastrukturen på brikken. Utstedelseslandet kan velge å lagre malen (se kapittel 3.1.2) i tillegg til dette, dersom de ønsker det.

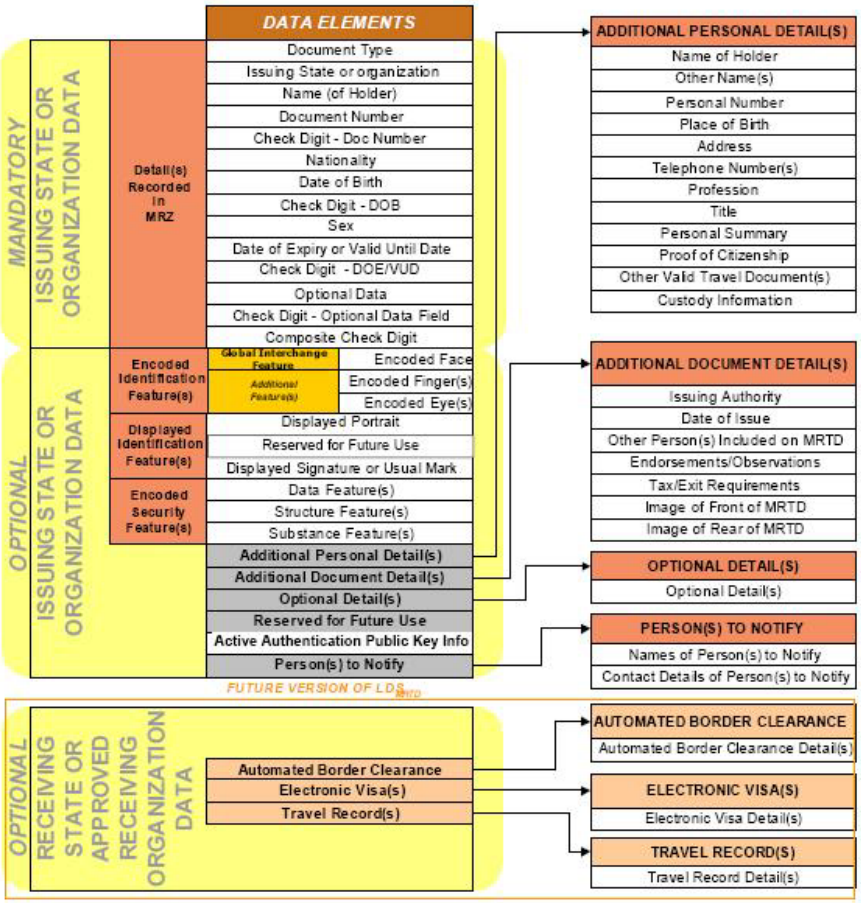
Av hensyn til personvernet anbefales det vanligvis at biometriske data bør kodes så snart som mulig etter at de registreres. Maler bør brukes istedenfor rådata, og rådata bør slettes så snart som mulig.[126] Ved å velge å lagre bildet fremfor en mal, fjerner ICAO (og EU)

[124]EU – Passport Specification (2006) *Biometrics Deployment of EU-Passports*
[125]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*
[126]Albrecht, A. (2003) BIOVISION: *Privacy Best Practices in Deployment of Biometric Systems*

grunnlaget for den personvernfremmende egenskapen til biometrisk teknologi, som er basert på bruken av maler og det at det opprinnelige kjennetegnet ikke kan gjenskapes.[127]

Den logiske datastrukturen (LDS)

Den logiske datastrukturen beskriver hvilke data som skal lagres i brikken, og på hvilken måte de skal lagres.[128]



Figur 2: Obligatoriske og valgfrie elementer for LDS v1.7

All data fra den maskinlesbare sonen (MRZ) er obligatoriske i den logiske datastrukturen, slik tilfellet er med passinnehaverens ansiktsbilde. I tillegg til disse dataene, er det påbudt med de sikkerhetsdata som trenges for å bekrefte passets integritet. De øvrige datafeltene er valgfrie, og noen er reservert for fremtidig bruk.

Den nåværende anbefalingen er at brikken bør kunne skrives til én gang. I fremtiden vil brikken måtte støtte anvendelser som krever overskriving. Blant slike anvendelser er:[129]

[127]Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informatization of the Body*
[128]Informasjonen i dette kapitlet er basert på ICAO (2004): *Machine Readable Travel Documents Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Tchknologies*

- Utstedelseslandet kan ønske å skrive en ny biometrisk verdi inn i LDS-en, for eksempel å oppdatere et ansiktskjennetegn som følge av plastisk kirurgi eller å legge til en ny type biometrisk verdi på et senere tidspunkt, for eksempel et irisbilde
- Landet som sjekker passet kan skrive en ny biometrisk verdi inn i LDS-en – for eksempel å legge til et nytt og oppdatert bilde av passinnehaveren
- Oppdatering av visumdata
- Oppdatering av data som ofte brukes om den reisende
- Lagring av informasjon om tidligere reiser
- Lagring av informasjon om automatiserte grensekryssinger

Dersom utstedelseslandet velger å legge til fingeravtrykk eller iris, må minst ett fingeravtrykksbilde eller irisbilde registreres.

4.6.2 Sikkerheten til biometriske pass

Det har vært mye debatt rundt biometriske pass, særlig i forhold til sikkerheten til biometriske data. Det fryktes at informasjonen kan fanges opp ved såkalt *skimming* (det å lese informasjonen på avstand uten at eieren er klar over det) eller avlytting (det å snappe opp informasjonen idet den overføres).

ICAO innrømmer at det er praktisk mulig med både avstandslesing og avlytting. For å ta tak i disse bekymringene, har ICAO utviklet og anbefalt en plan for tilgangskontroll (Basic Access Control, BAC) som utstedelseslandene skal bruke. Ved BAC bruker kontrollsystemet en "nøkkel" som avledes fra tall i MRZ-en til å "låse opp" brikken slik at systemet kan lese den. Passet må dermed være oppslått for at brikken skal kunne leses (hvis ikke data fra MRZ-en på en eller annen måte er kjent på forhånd), og innehaveren er sikret at dataene bare kan leses når passet er overlevert.[130] Denne metoden for tilgangskontroll er valgfri.[131] Dersom den iverksettes, kreves det at kommunikasjonskanalen til brikken er kryptert.

Organisasjoner som har pekt på visse personvern- og sikkerhetskrav som burde diskuteres når teknologier som RFID og biometri kombineres – som for eksempel Artikkel 29-gruppen vedrørende databeskyttelse – har ikke blitt hørt.

Data fra MRZ-en og fotografiet vil lagres i ukryptert tilstand i den logiske datastrukturen. Land som ønsker å begrense tilgangen til de valgfrie biometriske verdiene kan gjøre det ved å kryptere dem.

Sikkerhetsutfordringer i forbindelse med BAC
For å oppnå en vellykket autentisering, beregnes den opprinnelige passnøkkelen fra den maskinlesbare sonen. Til dette formålet brukes de delene som kan sjekkes mot et paritetsnummer (såkalt *key seed material*): passnummer, fødselsdato og utløpsdato.

---

[129]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*
[130]McMunn, M. K. (2006): *Machine Readable Travel Documents with biometric enhancement: The ICAO Standard*
[131]ICAO (2004) *PKI for Machine Readable Travel Documents offering ICC read-only access*

Den beregnede kryptografiske nøkkelstørrelsen på denne opprinnelige nøkkelen er ~56 bit:[132]

- passnummer: 10^9 muligheter (9 sifre)
- fødselsdato: 365*100 muligheter (~ 100 år)
- utløpsdato: 365*10 muligheter (~10 år)

På grunn av begrensninger i mulige fødsels- og utløpsdatoer, er det likevel mulig å avgrense noen av mulighetene: Fødselsdatoen 14. november 1965 omgjøres til sifferet 651114* ("*" står for kontrollsiffer). Fødselsdatoen 14. april 1965 omgjøres til sifferet 650414*. Det tredje og fjerde nummeret viser hvilken måned passinnehaveren ble født. Dette betyr at det tredje nummeret kan bare være 1 eller 0. Siden passet er gyldig i maksimum 10 år, er det også mulig å begrense de mulige numrene til gyldighetsdatoen. Utløpsdatoen 14.04.2016 skrives som 160414**. Det at den maskinlesbare sonens struktur er kjent reduserer dermed antall mulige varianter av *key seed material*.

Nederlandske sikkerhetseksperter presenterte en kryptografisk nøkkelstørrelse som var redusert til 35 bit, basert på ytterligere antakelser om passinnehaverens alder og passnummer som var avledet fra utstedelsesdatoen.[133] Med et såkalt *brute force*-angrep, dvs. et uttømmende søk av alle mulige kombinasjoner, var de i stand til å finne den riktige nøkkelen i løpet av noen timer.

4.6.3 Passdatabaser

Ulike europeiske land bruker ulike strategier for å håndtere og lagre passinformasjon: Sentrale databaser planlegges i Storbritannia, Nederland, Norge og Sverige (med lagring hos politiet). I Norge finnes det for tiden en sentralisert database for passinformasjon, og det har blitt foreslått å utvide databasen til også å inneholde fingeravtrykk når disse i fremtiden blir inkludert i passet. Både Teknologirådet og Datatilsynet har frarådet dette i sine svar til de offisielle høringene om emnet.[134] I Italia og Tyskland vil data som er nødvendig for pass, inkludert biometriske data, lagres desentralisert.[135]

En utfordring er at selv om en borger får et pass utstedt i et land hvor passopplysningene er håndtert i henhold til god personvernpraksis, er det ingen mulighet til å kontrollere hva som vil skje med dataene – for eksempel hvor og hvordan de lagres – når passet blir kontrollert på grensen i et land som har et annet syn på personvern.

En felleseuropeisk passdatabase har blitt diskutert, men det er for tiden ingen konkrete planer om en slik database.

---

[132] German Federal Office for Information Security (2005) *Common Criteria Protection Profile. Machine Readable Travel Document with „ICAO Anvendelse", Basic Access Control* og German Federal Office for Information Security (2005): *Digitale Sicherheitsmerkmale im elektronischen Reisepass*

[133] Heise Online (2006) *ePass-Hack im niederländischen TV demonstriert*

[134] Se http://www.teknologiradet.no/hringsuttalelse%20biometrisk%20pass_N-AIN.pdf.file og http://www.datatilsynet.no/templates/Page____1113.aspx

[135] Meints og Hansen (2006) *D 3.6 Study on ID Documents*

4.7 ID-kort

Grunnleggende teknologier: *RFID*
Lagringsteknologi
Biometri
Kommunikasjonsteknologier

De fleste EU-land har fått på plass en form for ID-kort – de eneste medlemslandene uten noen form for ID-kortsystem er Storbritannia, Irland, Danmark, Latvia og Litauen.[136] ID-kortsystemer har blitt innført på en rekke ulike måter: noen bruker RFID-teknologi, og det er antatt at biometri vil tas i bruk i nær fremtid.

ID-kort kan brukes i samspill med digitalisert informasjon (for eksempel biometri eller digitale signaturer). Disse muliggjør en entydig identifisering av et individ, og kan dermed for eksempel brukes til å forhindre bedrageri, kontrollere innvandring og bekjempe kriminalitet, samt også i anvendelser som ikke angår sikkerhet – f.eks. tilgang til tjenester fra offentlig og privat sektor.

Det har vært en opphetet debatt i Storbritannia – et av de ovennevnte landene som fremdeles ikke har et nasjonalt ID-kort – om regjeringens planer for ID-kort. I henhold til regjeringens nåværende plan skal ID-kort brukes i samspill med en biometrisk identifikator, som vil muliggjøre tilgang til over femti forskjellige typer informasjon om et individ, lagret i en sentralisert database. Denne omstridte planen har blitt beskrevet som et av de mest omfattende kortsystemer som hittil er blitt foreslått i Europa.[137]

En standard for et europeisk borgerkort (*European Citizen Card, ECC*) er for tiden under utvikling. Arbeidet gjøres av Den europeiske standardiseringskomitéen (CEN) og skulle etter planen publiseres i oktober 2006. I juli 2005 ble Artikkel 6-komitéen invitert av formannskapet i Rådet for Den europeiske union til å lage et utkast til felles sikkerhetsstandarder for nasjonale identitetskort. Komitéen ble særlig bedt om å fokusere på:[138]

- Bruken av biometri
- Felles standarder for kortgrensesnittet
- Tiltak for å sikre at data som er lagret på kortet er beskyttet, men kan leses av andre medlemsland. Dette inkluderer tiltak som *Enhanced Access Control* og *Public Key Infrastructure (PKI*)

Eksempel: Det belgiske ID-kortet[139]
Belgia var det første landet i Europa til å innføre digitale ID-kort. Kortet utstedes til alle borgere som er 12 år eller eldre. Kortet er på størrelse med et vanlig bankkort, og inneholder følgende informasjon:

---

[136]UK Home Affairs Committee Publication: *Home Affairs – Fourth Report*
[137]European Parliamentary Technology Assessment Network (2006) *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries*
[138]Council of the European Union (2005) *NOTE from Presidency to Strategic Committee on Immigration, Frontiers and Asylum: Minimum common standards for national identity cards*
[139]Meints og Hansen (2006) *D 3.6 Study on ID Documents*

- navn
- tittel
- nasjonalitet
- fødested og -dato
- nasjonalt nummer
- bilde
- underskrift
- underskrift til tjenestemannen som utstedte kortet
- gyldighetsdatoer
- kortnummer
- utleveringssted

Brikken på kortet inneholder den samme informasjonen, men inkluderer en adressefil i tillegg til ovennevnte informasjon.

Det belgiske kortet inneholder tre forskjellige 1024-bit RSA private signaturnøkler. For at borgeren skal kunne bruke nøklene til å lage en digital signatur, må en PIN-kode tastes inn. Dette gjøres gjennom pålitelig maskinvare, som f.eks. en smartkortleser.

Alle papirbaserte kort skal erstattes av det nye kortet innen utgangen av 2009.

Eksempel: INES-prosjektet (Frankrike)[140]
INES-prosjektet (Identité Nationale Electronique Sécurisée, sikker elektronisk nasjonal identitet) er et prosjekt som er ment å lage nye, obligatoriske, elektroniske ID-kort i Frankrike.

Det nåværende papirbaserte ID-kortet er ikke påbudt i Frankrike, og distribueres gratis. Dette har ført til et problem med identitetstyveri, da over 500.000 ID-kort ble meldt savnet i 2004. En av de foreslåtte løsningene på dette problemet er å påby det nye kortet, og å inkludere biometrisk informasjon i kortet. To biometriske kjennetegn har blitt foreslått: Ansiktet vil være det primære biometriske kjennetegnet. Det sekundære biometriske kjennetegnet kan være skannede fingeravtrykksbilder, men irisskanninger har ennå ikke blitt avskrevet som et alternativ.

I tillegg til å være et identitetskort, kan det nye elektroniske ID-kortet også brukes som en elektronisk signatur for e-tjenester i offentlig og privat sektor. Innehaverens personopplysninger og biometriske kjennetegn vil lagres i en kontaktløs RFID-brikke.

De samme personopplysningene som finnes i brikken vil lagres i en sentral database, og den tilsvarende biometriske informasjonen vil lagres anonymt i separate filer.

---

[140]IDABC: FR: *Future French eID card to become compulsory* og FR: *Future French electronic ID card to include two biometrics*

Kapittel 5 Datalagring

Datalagring er det å oppbevare data på et elektromagnetisk eller optisk medium, slik som en harddisk, et magnetisk bånd, en CD eller DVD, osv. *Tilgang* til dataene kan oppnås gjennom egnet utstyr, og avhengig av teknologien kan dataene *endres* eller *slettes*.

5.1 Databasesystemer

En database defineres som en organisert samling av data. I prinsippet kan dette også inkludere ikke-digitale data, som lister og kartotekkort, men i denne rapporten vil database henvise til organiserte data i digital form.

Databaser kan organiseres på ulike måter, men et fellestrekk er at dataene er organisert i dataelementer, som deretter kobles til hverandre. Den mest vanlige databasetypen er relasjonsdatabasen. I en slik database knyttes forskjellige informasjonsenheter (dataelementer) sammen med ett eller flere andre dataelementer. For eksempel kan *person* (navn) knyttes til én eller flere *adresser*, som igjen er knyttet til en bestemt *type* som beskriver forholdet – én adresse kan være hjemmeadressen og en annen kan være forretningsadressen. Forskjellige personer kan knyttes sammen gjennom kjennetegn som beskriver forholdets karakter (far/sønn, venn, kollega, osv.).

Denne måten å organisere data på gjør det lettere å knytte sammen informasjon og hente den fram igjen ved behov, og gjør det mulig å søke gjennom store datamengder for å finne relevant informasjon på en måte som var umulig med manuell arkivering. Databaser utgjør en vesentlig del av nesten ethvert datasystem, i spennet fra private CD-arkiver via kommersielle kunde- eller produktdatabaser til offentlige systemer som helsejournaler eller elektroniske saksmapper. Viktige databasesystemer som brukes til sikkerhetsformål i Europa er VIS (visumdatabasen), SIS (databasen til Schengen informasjonssystem) og EURODAC (database med informasjon om asylsøkere, se kapittel 3.5). Denne rapporten vil hovedsakelig fokusere på de sistnevnte systemene og bare komme inn på kommersielle databaser når de er relevante i forhold til sikkerhet (se kapittel 5.2.1).

5.1.1 Personvernutfordringer med databaser

En hovedutfordring ved håndtering av store datasett er datakvalitet. Det er viktig at alle opplysninger blir holdt oppdatert for at beslutninger om et individ skal treffes med tilstrekkelig nøyaktighet, relevans, hurtighet og fullstendighet. Ellers kan man risikere at en offentlig etat, et flyselskap eller annen part treffer beslutninger eller ekskluderer noen på grunnlag av unøyaktige, ufullstendige eller utdaterte opplysninger.[141] Det faktum at de fleste slike prosesser ikke er transparente for brukeren, gjør det umulig for en person å kontrollere hvorvidt hans eller hennes data er riktig behandlet.

Databasesystemer er også utsatt for såkalt formålsutglidning (*function creep*), som er bruken av data for noe annet det opprinnelige formålet. Et eksempel på slik formåls-

[141] United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*

utglidning var da utlendingsregistret – som også inneholder biometrisk informasjon som fingeravtrykk – ble åpnet for politiet til etterforskning av straffesaker.[142] Det opprinnelige formålet med databasen var å bidra til å fastslå identiteten til asylsøkere.

I forhold til biometrisk informasjon blir det ofte påpekt at det å lagre slik informasjon i sentrale databaser utgjør en større trussel enn det å lagre dataene lokalt, for eksempel på et kort med en integrert krets. Dette skyldes ikke bare den ovennevnte risikoen for formåls-utglidning, men også det at sentrale databaser er mer utsatt for sikkerhetsbrudd.[143]

5.2 Data retention

Med data retention mener vi det å ta opp og lagre data til ulike formål, som for eksempel fakturering, kundebehandling, osv. Personvernspørsmål med hensyn til slik oppbevaring av data er forbundet med lagringen av personopplysninger som ikke lenger er nødvendige for et praktisk formål, eller med at slike data lagres for en tidsperiode som er lenger enn nødvendig.

Den type data det er mest vanlig å snakke om i forbindelse med slik oppbevaring av data er IKT-data, som for eksempel trafikk- og lokasjonsdata for kommunikasjon som finner sted over mobiltelefoner, fasttelefoner, fakser, e-post, praterom, internett, osv.

Det å lagre trafikk- og lokasjonsdata er omstridt. Reglene varierer fra land til land, både med hensyn til hvor lenge dataene kan lagres, hvem som har ansvaret for dataene og hvem som skal dekke lagringskostnadene – myndighetene eller teleselskapene?

Andre områder hvor datalagring kan ses på som et sikkerhetstiltak, og dermed være påbudt ved lov, kan være: passering av bomstasjoner, flyselskapenes passasjerlister, bank- og kredittkorttransaksjoner, bibliotekets utlånsregistreringer, osv.

Eksempel: EUs Datalagringsdirektiv[144]
Bakgrunnen for Europaparlamentets og Rådets direktiv 2006/24/EF om lagring av data laget eller behandlet i forbindelse med tilveiebringelsen av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller elektroniske kommunikasjonsnettverk og om endring av direktiv 2002/58/EF er terrorangrepene i Madrid og London. Disse angrepene har ført til lokale initiativ om datalagring i de ulike medlemslandene, og direktivet forsøker å få de ulike praksisene til å stemme overens.

Det er også et resultat av den betydelige økningen i muligheter som elektronisk kommunikasjon gir. Data som benyttes i elektronisk kommunikasjon er særlig viktig og er derfor et verdifullt redskap til å avverge, etterforske, avsløre og straffeforfølge forbrytelser, særlig organisert kriminalitet.

---

[142]Kommunal- og regionaldepartementet (2003) *Rundskriv H19/03: Ikrafttredelse av endringer i utlendingsloven og utlendingsforskriften*
[143]Teknologirådet (2005) *Elektroniske spor og personvern*
[144]Informasjonen i dette kapitlet er basert på teksten til direktivet

Direktivet gjelder trafikk- og lokasjonsdata og beslektede data som er nødvendige for å identifisere abonnenten eller den registrerte brukeren. Innholdet av kommunikasjonen vil ikke bli lagret.

Data som vil bli lagret inkluderer:[145]

- Telefonnummeret eller, i tilfellet internettbruk, bruker-ID, pluss navn og adresse for den som ringer
- Oppringingens adressat (telefonnummer eller bruker-ID, pluss navn og adresse)
- Datoen, tidspunktet og varigheten til kommunikasjonen (start- og sluttidspunktene, eller alternativt tidspunktene for inn- og utlogging, pluss IP-adresse for internett-kommunikasjon)
- Type kommunikasjon (telefontjeneste eller internettjeneste)
- Hva slags utstyr som ble brukt (IMSI- og IMEI-nummer til både den som ringer og den som blir oppringt, dato, tidspunkt og celle-ID for anonyme anrop)
- Lokasjonene til mobilutstyret (celle-ID)

Direktivet slo fast at slike data skal lagres for ikke mindre enn seks måneder og ikke mer enn to år fra kommunikasjonsdatoen.

Eksempel: DNA-databaser
En DNA-database er en sentralisert database for lagring av individers DNA-prøver. Prøvenes karakter, samt reglene for hvilke prøver som kan registreres og når de kan registreres, varierer veldig fra land til land.

Det finnes mange ulike DNA-lagre, men for tiden blir de fleste ikke brukt til identifiserings-formål. Slike databaser inkluderer forskningsdatabaser, blodbanker og anlegg for lagring av vev.[146]

Vi vil her fokusere på systemer som lagrer DNA-prøver for å sammenligne dem med prøver samlet inn på åsted for forbrytelser. Land som for tiden har slike databaser inkluderer USA, Tyskland, Storbritannia, Norge, Finland, Belgia, Australia og Danmark.

Teknologien på dette området utvikler seg raskt. Der hvor tidligere DNA-prøver bare ble brukt til sammenligning av fingeravtrykk, er det nå i ferd med å bli praktisk mulig å utvikle starten på en faktisk profil (kjønn, etnisitet) fra selv den minste prøve av DNA-spor.[147]

Et viktig spørsmål med hensyn til å opprette og bruke DNA-databaser gjelder hvor omfattende prøvedatabasen skal være: Skal kun straffedømte forbrytere tas med, eller bør det tas DNA-prøver av alle som blir arrestert? Bør prøvene beholdes selv når straffesaken blir avvist eller den tiltalte blir frikjent? Bør det finnes en universell database som omfatter alle borgere?[148] I Europa har vi sett hvordan terskelen for å inkludere prøver blir senket gang på

[145]Se Kapittel 2 for forklaringer av de tekniske begrepene vedrørende telekommunikasjon
[146]OECD Working Party on Information Security and Privacy (2004) *Biometric-based technologies*
[147]Van der Ploeg, I. (2005) *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*
[148]Cole, S. A. (2004) *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*

gang. I Nederland ble kriteriet for påbudt avgivning av DNA endret fra mistenkte i straffesaker med 8-års strafferamme til mistenkte i straffesaker med 4-års strafferamme.[149] I Norge har en komité nedsatt av Justis- og politidepartementet foreslått at alle straffedømte skal avgi DNA til den sentrale DNA-databasen. Tidligere har bare forbrytere dømt for mord, voldsforbrytelser og alvorlige narkotikaforbrytelser måttet avgi DNA.[150]

Et annet spørsmål er hvorvidt bare et DNA-"fingeravtrykk" (bare nok informasjon til å kunne brukes til identifisering) skal lagres, eller om selve DNA-prøven bør beholdes, noe som gjør ytterligere analyse i fremtiden mulig.

5.2.1 Kommersiell datalagring

Grunnleggende teknologier: *Kommunikasjonsteknologier*
Datalagring
Databaser
Datautvinning

De fleste kommersielle aktører ønsker å lagre så mye data som mulig om kundene sine, til bruk i interne FoU-formål og som et markedsføringsredskap. I hvilken grad det er lov å bruke dette til målrettet markedsføring varierer fra land til land. I etterkant av slike aktiviteter har vi imidlertid sett en økende tendens til at kommersielle data brukes til sikkerhetsformål, ikke minst i USA etter 11. september 2001.

De amerikanske Department of Homeland Security, Justis- og Utenriksdepartementet, samt Social Security Administration (trygdeforvaltningen) meldte i 2005 at de hadde kjøpt personopplysninger fra såkalte *informasjonsformidlere* for rundt $30 millioner. Rundt 91 % av dette gikk til politiarbeid (69 %) eller antiterrorisme (22 %).[151]

Informasjonsformidlere er selskaper som samler inn og kobler sammen personopplysninger fra flere kilder og gjør dem tilgjengelige for kundene sine (se også Kapittel 6 for en beskrivelse av *data mining*). Kildene kan være offentlige registre, informasjon som er allment tilgjengelig (for eksempel på internettet) og informasjon fra proprietære kilder som for eksempel private selskaper.

Det finnes også eksempler på at politietater henvender seg direkte til selskaper for å få tilgang til kundedataene deres. I USA leverte det amerikanske Justisdepartementet en begjæring til en føderal domstol der de søkte om å få en rettskjennelse som ville tvinge Google til å overlevere et tilfeldig utvalg av én million URL-er fra Googles database, samt en datafil med teksten til alle søkestrenger som ble lagt inn på Googles søkemotor i løpet av én uke (unntatt informasjon som identifiserer de som la inn søkene).[152] Andre søkemotorer, som Yahoo og MSN, har mottatt og etterfulgt den samme anmodningen fra Justisdepartementet.

---

[149] Van der Ploeg, I. (2005) Biometric Identification Technologies: Ethical Implications of the Informization of the Body
[150] Justis- og politidepartementet (2005) *NOU 2005:19: Lov om DNA-register til bruk i strafferettspleien*
[151] United States Government Accountability Office (2006) *PERSONAL INFORMATION Agencies and Resellers Vary in Providing Privacy Protections*
[152] United States District court for the northern district of California, San Jose division (2006) *Gonzales vs. Google*

På denne måten kan polititjenestemenn få tilgangsrettigheter til data fra selskaper i etterforskningsøyemed. Tyske politimyndigheter, for eksempel, har rett til å få tilgang til data som kontrolleres av juridiske enheter, for å kunne underbygge eller utelukke en konkret mistanke om en forbrytelse.[153]

Det er mulig å differensiere hvilken tilgang som gis til data fra virksomheter basert på kriterier for mistanke. Når politimyndigheter får tilgang til slike data, kan det være basert på en konkret mistanke om at en person har begått en forbrytelse. Alternativt kan politimyndigheter søke tilgang til informasjon for å etterforske en mulig og allestedsnærværende fare, for eksempel faren for terrorangrep. Slike etterforskninger er ikke basert på en konkret mistanke, men er en del av politimyndighetenes forsøk på å avsløre organisert kriminalitet. I denne sammenheng er ikke den potensielt mistenkte kjent av myndighetene. For å drive slik etterforskning, forsøker politimyndighetene å samle inn og analysere informasjon om personer som svarer til en viss profil som indikerer deres evne og vilje til å begå slike alvorlige forbrytelser. Datascreening som metode for å forhindre terrorangrep[154] inkluderer per definisjon gjennomsøking av personopplysninger fra en stor gruppe mennesker. Det er dermed høyst relevant for personvern, særlig siden data fra uskyldige personer blir behandlet.

Truslene mot personvernet er opplagte dersom data som er samlet inn av forretningsforetak aksesseres av politimyndigheter med sikte på datascreening. Mange forretningsforetak har kundebehandlingsprogrammer (CRM) som inkluderer opprettesen av en kundeprofil. Profilen inneholder oppsamlet informasjon om kundenes preferanser og vaner, og selv data som opprinnelig er irrelevante får dermed uventet betydning. Å koble sammen data som er tilgjengelig i en rekke selskapers datavarehus kan gi politimyndigheter tilgang til detaljert informasjon om borgere. De fleste mennesker etterlater elektroniske spor i ulike forretningsmiljøer uten særlig bekymring. På grunn av risikoen for å krenke den grunnleggende retten til personvern, må tilgang til slike data for etterforskninger som ikke er basert på mistanke følge særskilte og begrensede lover.[155]

5.3 Grensekontrollsystemer

Grunnleggende teknologier: *Databasesystemer*
Biometri
Kommunikasjonsteknologier

Dette avsnittet tar for seg ulike systemer som brukes ved grensekontroll for å vurdere hvorvidt individer er den de gir seg ut for å være og har adgangsrett til landet eller regionen som utfører kontrollen. Slike systemer baserer seg vanligvis på bruken av databaser og biometrisk identifisering.

Fordi maskinlesbare reisedokumenter (MRTD), eller *biometriske pass,* er mer forbundet med RFID og sensorteknologier, ble spørsmål vedrørende denne teknologien – inkludert passdatabaser – diskutert i kapittel 4.6.

---

[153]Regulert i artikkel 161a i tysk strafferett.
[154]I Tyskland ble datascreening (såkalt Rasterfahndung) underlagt en kjennelse fra Den tyske grunnlovsdomstolen. For mer informasjon se D 3.2. Se også Achelpöhler, W. og Niehaus H. (2004) *Data Screening as a Means of Preventing Islamic Terrorist Attacks in Germany*
[155]For flere detaljer, se *D 3.2 Legal Report*

Eksempel: SIS II
Den opprinnelige Schengen-avtalen ble gjort i 1985 mellom Belgia, Frankrike, Luxembourg, Nederland og Tyskland. Idéen var (og er) å fjerne grensekontroll mellom deltakerlandene, og å oppveie for dette ved å kontrollere Schengenområdets yttergrenser og øke politisamarbeidet mellom medlemslandene.[156]

SIS (Schengen informasjonssystem) er et felles informasjonssystem som tillater nasjonale politimyndigheter innen Schengen å få tilgang til og utveksle informasjon. Det opprinnelige systemet ble innført i 1995. SIS omfatter for tiden 13 EU-land, i tillegg til Norge og Island, men forventes å bli utvidet. SIS II er en oppdatert utgave av SIS og planlegges iverksatt i 2007.

Gjennom dette systemet vil politimyndighetene få informasjon i forbindelse med alarmer knyttet til personer eller gjenstander. Denne informasjonen brukes til å samarbeide om kriminalsaker, kontrollere mennesker på grensene eller utstede visa eller oppholdstillatelser. Det er seks forskjellige varslingskategorier i SIS II:[157]

1) *varsler om personer som burde nektes innreise til Schengenområdet*;
2) *varsler om personer som det er utstedt arrestordre på (med sikte på overgivelse eller utlevering);*
   Informasjon som kan ligge inne i systemet inkluderer: identiteten og nasjonaliteten til den ettersøkte og informasjon om lovbruddet og dommen.

   Informasjonen kan aksesseres av politiet og grensekontrollører, nasjonale rettsmyndigheter og påtalemyndigheter, Det europeiske politikontor (Europol) og Eurojust.[158]

   Informasjonen beholdes i systemet inntil den ettersøkte har overgitt seg eller blitt utlevert. Varsler om arrestasjonen og tilleggsdata blir automatisk slettet etter 10 år.
3) *varsler om personer for å sikre beskyttelse eller avverge trusler;*
   Varsler kan sendes ut om savnede personer som må plasseres under midlertidig politibeskyttelse, enten for deres egen sikkerhet eller for å avverge trusler, og om savnede mindreårige.

   Informasjonen kan aksesseres av politiet og grensekontrollører, samt nasjonale rettsmyndigheter og påtalemyndigheter.

   Varslene skal slettes så snart personen er plassert under politibeskyttelse. Varslene blir automatisk slettet etter 10 år.
4) *varsler om personer som er ettersøkt i forbindelse med rettergang;*
   Varsler kan sendes ut om vitner, personer som er innkalt av en nasjonal rettsinstans

[156] Rieker, P. og Knutsen, B. O. (2003) *EUs "nye" sikkerhetspolitikk: Bekjempelse av terrorisme og internasjonal kriminalitet*
[157] Det følgende er hovedsakelig basert på: European Commission Press Release *MEMO/05/188, Schengen: from SIS to SIS II* og Commission of the European Communities *Proposal for a council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*
[158] Den rettslige samarbeidsenheten til Den europeiske union, http://eurojust.europa.eu/

eller som må forkynnes en domsavsigelse eller som må avtjene en dom.

Informasjonen kan aksesseres av politiet og grensekontrollører, nasjonale rettsmyndigheter og påtalemyndigheter, og Eurojust.

Varsler vil slettes så snart oppholdsstedet til den aktuelle personen har blitt fastslått. Varslene blir automatisk slettet etter 10 år.

5) *varsler om personer og gjenstander for diskret overvåking eller målrettet kontrollering;* For å avverge trusler mot den offentlige sikkerhet, kan varsler sendes ut om personer eller kjøretøy, båter, luftfartøy eller containere for at de skal settes under diskret overvåking eller målrettet kontrollering. Dette kan gjøres når det finnes klare bevis for at den aktuelle personen har til hensikt å begå eller er i ferd med å begå flere og meget alvorlige lovbrudd, eller hvor en helhetsvurdering gir grunn til å anta at personen vil begå slike lovbrudd i fremtiden.

   Informasjon om personer som ligger inne i systemet inkluderer: navn og mulige alias, fødested og -dato, kjønn og nasjonalitet, fotografier, fingeravtrykk og fysiske kjennetegn, hvorvidt personen er bevæpnet, er voldelig eller er på rømmen, og detaljer om selve varselet, inkludert lenker til andre varsler.

   Informasjonen kan aksesseres av politiet og grensekontrollører, nasjonale rettsmyndigheter og påtalemyndigheter, og Eurojust.

   Varsler om personer blir automatisk slettet etter 3 år.

6) *varsler om gjenstander som skal beslaglegges eller brukes som bevis i en rettsprosess*

SIS-databasen rommer for tiden over 13 millioner registreringer, hvorav 1/10 er i tilknytning til ettersøkte personer.[159]

Noen av de viktigste nye egenskapene til SIS II vil være sentrallagring av den europeiske arrestordren og utleveringsinformasjon, og lagring av biometriske data som fingeravtrykk og fotografier. Dette er en vesentlig endring sammenlignet med dagens situasjon, hvor informasjon kun utveksles bilateralt. Det nye systemet vil også gi muligheten til å legge inn informasjon om personer hvis identitet har blitt misbrukt, dette for å unngå ytterligere ubehageligheter forårsaket av feilidentifiseringer. Slik praksis vil være avhengig av samtykke fra den berørte personen.[160]

SIRENE
For å sikre at politiet og andre myndigheter utveksler alle potensielt nødvendige tilleggs-

[159] Article 29 Data Protection Working Party (2005) *Opinion 6/2005 on the Proposal for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for Regulation of the European Parliament and of the council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final)*

[160] Commission of the European Communities (2005) *Proposal for a council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*

opplysninger, må hvert medlemsland opprette et SIRENE-kontor (Supplementary Information Request at the National Entry). SIRENE består av representanter fra nasjonale og lokale politimyndigheter, tollinspektører og rettsvesenet.[161] SIRENE-kontoret skal også bekrefte kvaliteten til informasjonen som er lagt inne i SIS II. I Norge vil SIRENE-kontoret være tilknyttet KRIPOS.

Eksempel: VIS
VIS (Visuminformasjonssystemet) vil være et system for å utveksle visumdata mellom medlemslandene. For tiden forvalter alle medlemslandene sine egne visumsystemer. Borgere fra 134 land trenger et visum for å reise inn i EU. Hittil har det vært mulig for en søker som har blitt avslått av ett konsulat å gå videre til det neste (såkalt "visumshopping").

Et viktig mål for det nye systemet er å hindre dette. Informasjon om tidligere søknader og avslagsgrunnene vil være sentralt tilgjengelig. Andre mål inkluderer muligheten til å kontrollere at visuminnehaveren er den samme person som visumet er utstedt til, og til å bidra til å identifisere og dokumentere ulovlige innvandrere som ikke tidligere er dokumenterte.[162]

Følgende data vil bli inkludert i systemet:

1) alfanumerisk data om søkeren og om visa som er søkt om, utstedt, avslått, annullert, tilbakekalt eller forlenget;
2) fotografier;
3) fingeravtrykksdata;
4) lenker til andre anvendelser eller databaser hvor personen kan være registrert, som for eksempel SIS.

VIS vil være basert på en felles teknisk plattform med SIS II. Det vil bestå av en sentral struktur og nasjonale grensesnitt. Grensesnittene vil suppleres med lenker til konsulater og grenseposter. Data vil samles inn av de ulike medlemslandenes konsulater og deretter overføres til den sentrale databasen, hvor det vil være tilgjengelig for alle medlemsland. Systemets yteevne er anslått – særlig med hensyn til biometriske data – til å være i stand til å inneholde data om rundt 20 millioner visumsøknader i året, noe som vil resultere i 70 millioner fingeravtrykk som skal lagres i systemet i løpet av en 5-årsperiode.[163]

Artikkel 29-gruppen vedrørende databeskyttelse påpeker at *det må utføres en særlig streng kontroll dersom disse biometriske data skal lagres i en sentralisert database, siden dette i stor grad vil øke risikoen for at data vil brukes på en måte som er uforholdsmessig eller uforenlig med det opprinnelige formålet som de ble samlet inn for.*

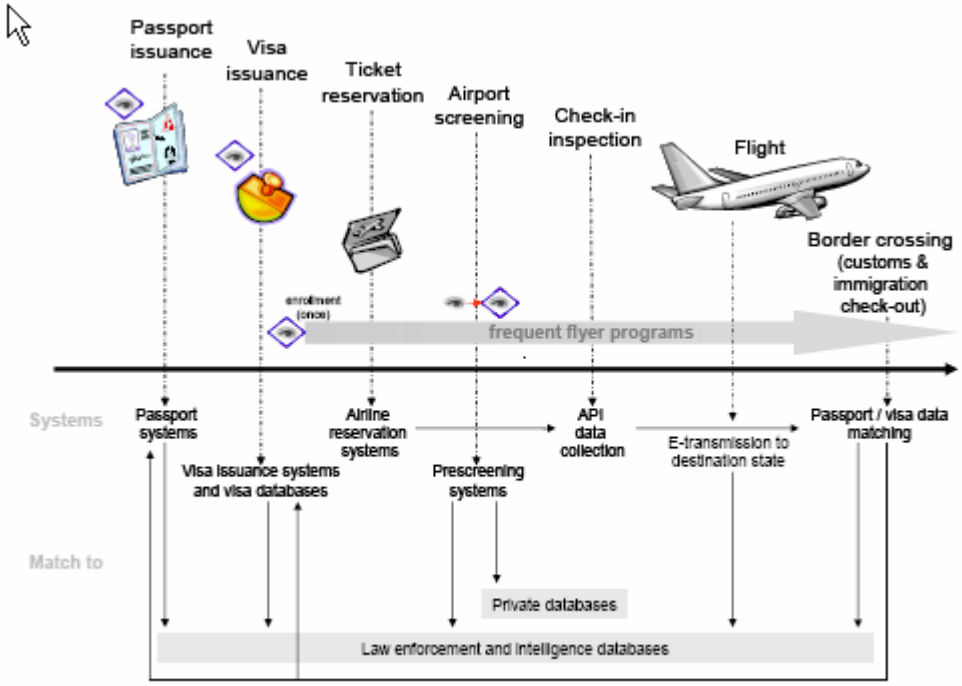
[161] Fra www.oasis.gov.ie
[162] Forslag til en forordning fra Europaparlamentet og Rådet vedrørende Visuminformasjonssystemet (VIS) og mellomstatlig utveksling av data vedrørende tidsbegrensede oppholdsvisa
[163] Article 29 Data Protection Working Party (2005) *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas*

Det sies i forslaget til forordningen at data ikke bør beholdes lenger enn nødvendig. Den hensiktsmessige perioden er satt til fem år, for å være i stand til å ta i betraktning data om tidligere visumsøknader når man vurderer nye visumsøknader. Etter femårsperioden bør dataene slettes. Data kan slettes tidligere dersom det er grunner til dette.

5.4 Utvekslingen av passasjerinformasjon ved utenlandsreiser

Grunnleggende teknologier: *Databasesystemer*
Kommunikasjonsteknologier
MRTD

Det er ulike typer systemer som er basert på utvekslingen av passasjerinformasjon ved utenlandsreiser:[164]



Figur 3: Systemkategorier på en kronologisk akse (OECD)

5.4.1 Screening på flyplassen

Systemer for screening på flyplassen (eller forhåndsscreening) gjør det mulig for de som er ansvarlige for flyplassikkerheten (for eksempel for tilgang til flyene og avgangssonene) å gjøre screeningen av passasjerene på en mer effektiv måte. Istedenfor å velge ut tilfeldige passasjerer for en grundigere undersøkelse, bruker forhåndsscreeningssystemer profilering til å velge ut en passasjer hvis det er behov for en grundigere undersøkelse. Forhånds-screeningssystemer behandler vanligvis:

[164] OECD Working Party on Information Security and Privacy (2004) *Background material on biometrics and enhanced network systems for the security of international travel*

- Data som er tilknyttet passasjerens identitet, slik den er gitt av flyselskapenes bestillingssystemer eller via maskinlesbare reisedokumenter.
- Data som er lagret i forskjellige databaser hvor det er informasjon om den gitte passasjeren. Dette kan omfatte politiets databaser eller databaser brukt til privat markedsføring.
- Ulike kriterier for å avgjøre om et individ kan gå gjennom vanlig innsjekking, grundigere innsjekking eller skal nektes innsjekking.

API-systemer
API-systemer (*Advance Passenger Information*) forsøker å gjøre det mulig for toll- og/eller innvandringsmyndigheter å organisere behandlingsprosessen sin før et fly lander. Avhengig av det enkelte land, kan API-systemer gjøre det mulig å behandle API-data før ombordstigning. Slike systemer behandler informasjonen som er samlet inn av flyselskapet under innsjekkingsprosessen. Denne informasjonen, kalt passasjermanifestet, kan samles inn automatisk fra maskinlesbare reisedokumenter (pass, visa eller andre dokumenter).

Informasjonen overføres elektronisk fra flyselskapet til de relevante myndigheter. De innsamlede dataene kontrolleres mot databaser med mistenkte, og kan også selv mate andre systemer, for eksempel til sporings- eller profileringsformål.

I tillegg til API-data, har USA påbudt flyselskapene å overføre data som er hentet fra PNR-mappen (*Passenger Name Record*). PNR-mappene lages av flyselskapene når en passasjer bestiller en reise, og lagres i flyselskapenes bestillings- og avgangskontrolldatabaser. PNR gjør ulike aktører, som reisebyråer, automatiske bestillingssystemer (CRS-systemer), flyselskaper eller deres stedlige representanter på flyplassen i stand til å kjenne igjen enhver passasjer og få tilgang til all relevant informasjon knyttet til hans eller hennes reise. Dette kan være avgangs- og returflyvninger, flyforbindelser, spesialtjenester som er nødvendige om bord på flyet (kosher eller vegetarmat, eventuell fysisk hjelp som er nødvendig, osv).[165]

APP-behandling
APP (*Advance Passenger Processing*) er en metode for å samle inn API som gjør at passasjerinformasjonen kan overføres og behandles før ombordstigning. En screeningprosess resulterer i et statusflagg for ombordstigning/ingen ombordstigning. APP gjør flyselskapene i stand til å kontrollere passasjerer ved innsjekking. Dette gjør det mulig å samle inn passasjerdata og overføre dataene til reisemålets grensekontroll forut for ankomst. APP sender en elektronisk melding til flyselskapet og bekrefter at passasjerer som trenger det har et gyldig visum. Hele prosessen gjøres i sanntid.

Det største fokuset på API-systemene har vært på utvekslingen av PNR-data fra flyselskaper som betjener det europeiske markedet til USA. Den forrige avtalen mellom EU og USA om utveksling av PNR-data løp ut 30. september 2006. Den ble erstattet av en ny avtale, som slo fast at USAs Department of Homeland Security kan få tilgang til PNR-data fra flyselskapenes

[165]European Commission Airline passenger data transfers from the EU to the United States (Passenger Name Record)

bestillingssystemer. Dataene vil deretter håndteres i henhold til amerikanske lover og krav i den amerikanske grunnloven.[166]

Passasjerdata er også av interesse for europeiske myndigheter. I Storbritannia har politiet tilgang til nettbaserte personopplysninger om alle passasjerer som reiser inn og ut av landet.[167] Det er meningen å utvide systemet til også å omfatte innenlandsflyvninger. Også Danmark har foreslått at politiet, med tanke på påbudt screening, burde gis tilgang til flyselskapenes informasjon om alle passasjerer som reiser til eller fra landet.

En ny fransk innvandringslov inkluderer opprettelsen av en database over fingeravtrykk og ansiktsbilder for søknader om oppholdskort og ulovlige innvandrere, samt for visumsøkere, for å muliggjøre verifisering ved innreisestedene.[168]

Artikkel 29-gruppen vedrørende databeskyttelse har påpekt at instanser som Den internasjonale organisasjonen for sivil luftfart (ICAO), Verdens tollorganisasjon (WCO) og Det internasjonale lufttransportforbund (IATA) har utviklet entydige definisjoner av API-data for å oppnå samstemte standarder og lik praksis. De avtalte retningslinjene sier at API-data består av de opplysningene som eventuelt finnes i reisedokumentenes maskinlesbare sone. PNR-data går langt utover dette.[169]

[166]The European Union (2006) *AGREEMENT between the European Union and the United Stats of America on the prosessing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security*
[167]Bunyan, T. (2005) *While Europe sleeps...*
[168]OECD Working Party on Information Security and Privacy (2004) *Background material on biometrics and enhanced network systems for the security of international travel*
[169]Article 29 Data Protection Working Party (2006) *Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data*

Kapittel 6 Analyse- og beslutningsstøtte

Analyse- og beslutningsstøtte er nært forbundet med databaser. Det er den stadig økende datamengden i både kommersielle og offentlige databaser som har gjort analysen av slik data til både en blomstrende næring og til en del av enkelte lands sikkerhetsstrategier.[170]

6.1 Personvernutfordringer i forbindelse med analyse- og beslutningsstøtte

Det er allment kjent at når forskjellige informasjonsfragmenter om en person kobles sammen, avslører det mer om vedkommende enn når informasjonen ses på hver for seg. Et viktig personvernsprinsipp i forbindelse med databaser som inneholder personopplysninger er derfor at bare informasjon som er nødvendig for å oppfylle systemets formål skal samles inn, og at slik informasjon skal slettes når den ikke lenger trenges (formålsprinsippet).

I det siste har vi sett en trend hvor myndigheter ønsker å koble databasesystemer sammen av grunner som avviker fra databasesystemenes opprinnelige formål. Hensiktene med en slik strategi kan være økt effektivitet (for eksempel i Storbritannia[171]) eller sikkerhet (som forslaget om forbedret interoperabilitet mellom SIS II, VIS og EURODAC[172]).

Datautvinning (*data mining*) er den mest anvendte teknikken for analyse- og beslutningsstøtte. Utfordringene i forbindelse med datautvinning er stort sett de samme som med databaser (se kapittel 5.1). Sammenkobling av data resulterer i mer informasjon om individer, og i de fleste tilfeller vet ikke den registrerte at denne sammenkoblingen foretas – og langt mindre hvilke databaser det gjelder.

Spørsmålet om datakvalitet er en utfordring i forbindelse med alle databaser. Når data samles inn fra en rekke forskjellige kilder – noen offentlige, noen kommersielle – blir kvalitetssikring enda vanskeligere.

6.2 Datautvinning

Datautvinning er en fellesbetegnelse for teknologier som finner nyttige mønstre og regler i store datamengder. Som en indirekte følge fører disse teknologier til opprettelsen av store datavarehus, som ikke kan analyseres på en effektiv måte ved hjelp av tradisjonelle metoder.[173] Gjennom å bruke matematiske, eller rettere sagt statistiske teknikker, blir det mulig å søke gjennom meget store datamengder etter sammenhenger som produserer en ny kunnskap.[174]

Datautvinningsteknologiens styrke i forhold til sikkerhetsformål ligger i dens mulighet til å trekke frem i lyset ikke-opplagte mål for etterforskning eller identifisere terrortrusler. Dette

---

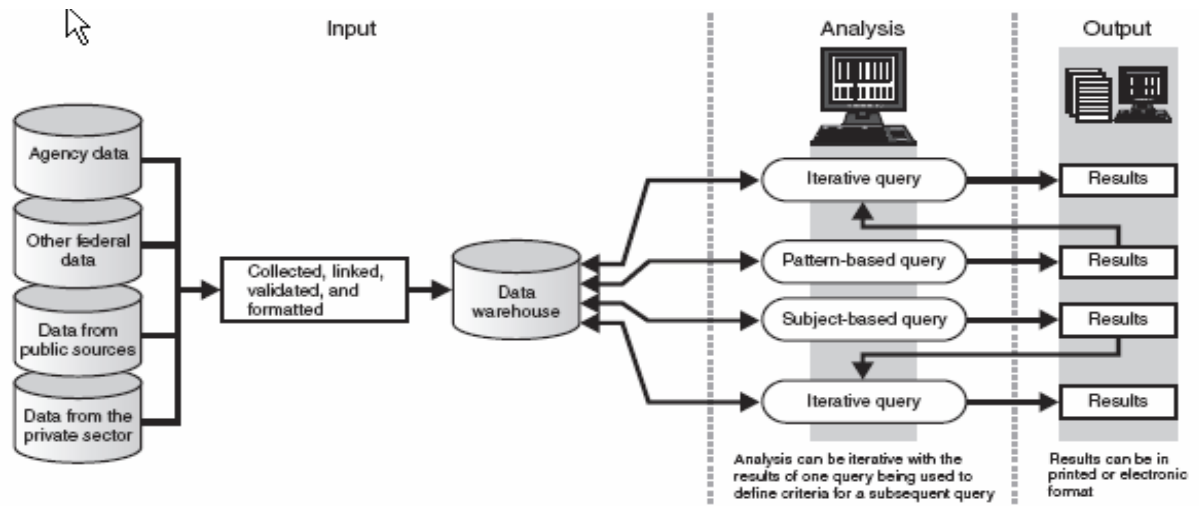
[170] Se for eksempel kapittel 6.3 om TIA (Total Information Awareness).
[171] OPM (2005) *Research into the use of personal data sets held by public sector bodies*
[172] Article 29 Data Protection Working Party (2004) *Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)*
[173] EPTA (2006) *ICT and Privacy in Europe – A report on different aspects of privacy based on studies made by EPTA members in 7 European countries*
[174] Hildebrandt og Backhouse (2005) *D 7.2 Descriptive analysis and inventory of profiling practices*

gjøres gjennom logiske slutninger avledet fra desentraliserte datasett spredt rundt hele verden via internettet. Mange anser at mulighetene som denne teknologien tilbyr er nødvendige for å holde tritt med nye sikkerhetstrusler, men den legger også mye makt til å overvåke i hendene til de som har tilgang til teknologien i mye større grad enn tidligere.[175]

Datautvinning består vanligvis av tre prosesser:[176]

- *datainnputt*
  I denne fasen blir data samlet i et sentralt datavarehus, validert og formattert for bruk i datautvinning.
- *dataanalyse*
  I denne fasen søkes det typisk etter data gjennom en forespørsel. De to mest vanlige forespørselstyper er mønsterbaserte forespørsler og emnebaserte forespørsler. Mønsterbaserte forespørsler søker etter dataelementer som svarer til eller avviker fra et forhåndsdefinert mønster (f.eks. uvanlige erstatningskravsmønstre i et forsikringsprogram). Emnebaserte forespørsler søker etter all tilgjengelig informasjon om et forhåndsdefinert emne ved å bruke en spesifikk identifikator. Dette kan være personopplysninger, som for eksempel en personlig identifikator (f.eks. et ID-nummer eller personnavnet)
- *resultatdata*

Følgende figur illustrerer prosessen:



Figur 4: høyytelses datautvinning[176]

[175]Weitzner et al. (2006) *Transparent Accountable Data Mining. New Strategies for Privacy Protection*
[176]United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*

Eksempel: FBIs Foreign Terrorist Tracking Task Force[177]
I kjølvannet av terrorangrepet den 11. september 2001, har datautvinning i økende grad blitt brukt som et redskap til å avdekke terrortrusler gjennom å samle inn og analysere data fra offentlig og private sektor. Arbeidet FBIs Foreign Terrorist Tracking Task Force gjør innen datautvinning søker å hjelpe føderale politi- og etterretningsetater med å oppspore utenlandske terrorister og deres støttespillere i USA.

Rapportene fra systemet spenner fra lister over individer som kan svare til en viss profil, til detaljert informasjon om en bestemt mistenkt. Slike rapporter vil typisk inneholde personopplysninger. Rapportene deles med feltetterforskere, feltkontorer og andre føderale etterforskere.

Disse systemene bruker informasjon som etaten samler inn selv, samt informasjon som er gitt av andre etater, som for eksempel Social Security Administration (trygdeforvaltningen), og kilder fra privat sektor, som for eksempel kredittkortselskaper. Systemet bruker 30 offentlige kilder, 11 kommersielle kilder og 4 internasjonale kilder, inkludert etterretningsdata og savnede eiendeler som meldes til Interpol.

Eksempel: Å forutsi atferd[178]
I en studie fra 2004-2005 ble 100 ansatte og studenter ved Massachusetts Institute of Technology (MIT) utstyrt med spesielle mobiltelefoner. Anropslogger, bluetooth-apparater i nærheten og kommunikasjons- og brukeratferd ble registrert. Totalt rundt 450.000 timer med data ble samlet inn (MIT Reality Mining datasettet).

Ved å bruke denne informasjonen, har forskere identifisert noen byggeklosser i et individs atferd (kalt *eigenbehaviors)* og bruker så dette til å foreta sin analyse. Forskerne hevder at hvis de får vite en persons atferd i døgnets første halvdel, kan de forutsi personens videre atferd med en nøyaktighet på 79 %. Denne teknikken kan også brukes til å karakterisere gruppeatferd, og å identifisere hvor nært et individ er knyttet til en gruppe. Idéen bak studien er at dersom du fort kan karakterisere mennesker, sammenligne dem med lignende mennesker og forutsi deres atferd i den nære fremtid, kan du lage grensesnitt som gjetter brukerens preferanser, sosiale forbindelser og daglige planer.

6.3 Søketeknologi

Søketeknologi har utviklet seg voldsomt de seneste år, og enkelte hevder nå at søking i ustrukturert tekst snart vil erstatte databaseteknologi som den fremste teknologien for å finne informasjonsforbindelser og -mønstre.

Mer og mer informasjon, både om individer og selskaper, er nå tilgjengelig på internettet og i ulike offentlige og private databasesystemer som er koblet til internettet. En søkemotor vil systematisk gå gjennom (*crawl*) internettet og indeksere sidene den finner (dvs. enten lage en kopi av siden eller registrere de viktigste nøkkelordene).[179]

---

[177] United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*
[178] Basert på Eagle og Pentland (2006) *Eigenbehaviours: Indentifying Structure in Routine*
[179] Battelle, J. (2005) *The Search – How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*

Det å kombinere informasjon fra en rekke kilder kan bidra til å identifisere mistenkelige profiler. Ved å bruke slik søketeknologi er det mulig å opprette automatiske søk som går kontinuerlig gjennom forskjellige databaser og allment tilgjengelige kilder, i søket etter mønstre som har blitt observert i tidligere kriminalsaker.

En teknologi som er forventet å forbedre søket etter terrorister på internettet er *den semantiske webben*. Det semantiske nettet dreier seg om *data* fremfor *dokumenter*. Mye av motivasjonen er knyttet til det å få tilgang til informasjon som i dag ligger gjemt i forskjellige proprietære databaser. For at dette skal fungere, må informasjonsenhetene "merkes" på samme måte av alle. Idéen er å sørge for et felles rammeverk som gjør at data kan deles og gjenbrukes på tvers av ulike anvendelser, virksomheter og samfunn. Arbeidet med dette er et samarbeid ledet av W3C, med deltakelse fra en rekke forskere og næringslivsaktører.[180] Ulike e-forvaltningsinitiativ representerer liknende tiltak. Storbritannia har for eksempel utviklet et felles vokabular for offentlig sektor (Integrated Public Sector Vocabulary).[181]

Det er kjent at USAs Nasjonale sikkerhetsråd (NSA) har brukt logger over teletrafikk for å danne et grunnbilde av aktuelle personers kontaktnett. Grupperinger av mennesker innenfor et større kontaktnett blir dermed synlige, og det gjør også mennesker med få forbindelser som synes å opptre som mellommenn mellom slike grupper. Idéen er å se hvor mange ledd eller "grader" som skiller noen fra, for eksempel, et medlem av en svartelistet organisasjon.

Ved å supplere teletrafikkalysene sine med data fra sosiale nettverk på internett, kan NSA knytte sammen mennesker på dypere nivåer, gjennom felles aktiviteter, som for eksempel å ta flytimer.[182] I mange tilfeller kan implisitt og/eller eksplisitt informasjon finnes i slike sosiale nettverk. Det sosiale nettverket LinkedIn.com består for eksempel av mange mennesker fra ulike deler av IT-sektoren. MySpace.com, Friendster og Hi5 inneholder store datamengder om sosiale nettverk (per august 2006 hadde MySpace 100 millioner medlemmer).[183] Det semantiske nettet er en metode for å kunne koble sammen informasjon fra alle slike nettsteder i letingen etter nettverk. Forskning på dette området finansieres av NSA.[182]

Søk i såkalt rike medier er et annet viktig felt hvor søk kan brukes som sikkerhetsteknologi. Alle medier konverteres til slutt til råtekst eller tekst som beskriver innhold (meta data) eller egenskaper. En avansert søkeplattform vil kunne identifisere forbindelsesmønstre gjennom en såkalt "on-the-fly" regresjonsanalyse og deretter bruke disse mønstrene til å utløse visse hendelser eller advarsler. Søk i rike medier kan forbedres ved å integrere talegjenkjenning som gjør tale (fra videoer og taleopptak) om til tekst, hvorpå teksten indekseres av søkemotoren.[184]

---

[180] World Wide Web Consotium (W3C): *Sematic web*, http://www.w3.org/2001/sw/
[181] www.esd.org.uk/standards/ipsv
[182] Marks, P. (2006) *Pentagon sets its sights on social networking websites*
[183] Aleman-Meza et al. (2006) *Semantic Analysis on Social Networks: Experiences in Addressing the Problem of Conflict of Interest Detection*
[184] FAST Search Best Practices TM (2006) *Searching Rich Media*

Eksempel: Total Information Awareness

Total Information Awareness (TIA) var et program utviklet av det amerikanske forsvarsdepartementets forskningsenhet DARPA. TIA-programmet inneholdt tre typer verktøy: oversettelse mellom språk, datasøk og mønstergjenkjenning, og avanserte verktøy for samarbeid- og beslutningsstøtte.[185]

Målet med TIA var å forutsi terrorangrep før de inntraff. Systemet var ment å skanne private og offentlige databaser, samt internett, for transaksjoner som kunne forbindes med et terrorangrep. Kongressen i USA stanset finansieringen av TIA i september 2003.

[185]US Department of Defense (2003) *Total Information Awareness (TIA)*

Referanser

Bøker og artikler

Achelpöhler, W. og Niehaus, H. (2004) Data Screening as a Means of Preventing Islamic Terrorist Attacks in Germany. *German Law Journal,* **Vol. 05 (**No. 05), s. 495-513

Agre, P. E. (2003) *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places.* University of California, Los Angeles

Albrecht, A. (2003) *Privacy Best Practices in Deployment of Biometric Systems.*

Aleman-Meza et al. (2006): *Semantic Analysis on Social Networks: Experiences in Addressing the Problem of Conflict of Interest Detection.* Edinburgh: WWW 2006

Article 29 Data Protection Working Party (2003) *Working document on biometrics.* Brüssel

Article 29 Data Protection Working Party (2004) *Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS).* Brüssel

Article 29 Data Protection Working Party (2005) *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas.* Brüssel

Article 29 Data Protection Working Party (2005) *Opinion 6/2005 on the Proposal for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for Regulation of the European Parliament and of the council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final).* Brüssel

Article 29 Data Protection Working Party (2005) *Working document on data protection issues related to RFID technology.* Brüssel

Article 29 Data Protection Working Party (2006) *Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data.* Brüssel

Article 29 Data Protection Working Party (2006) *Working document on data protection and privacy implications in eCall initiative.* Brüssel

Battelle, J. (2005) *The Search – How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture.* London: Nicholas Brealey Publishing

Berg et al. (2004) *Autonomous sensor systems. Communication needs for independent sensors.* Kjeller: Forsvarets forskningsinstitutt

Bolkcom, C. (2005) *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*, *CRS Report for Congress,* oppdatert 7. februar 2005. Washington: The Library of Congress

Bunyan, T. (2005) While Europe sleeps... *ELCN Essays* (no. 11)

Cabinet Office, eGovernment Unit (2006) *IPSV-Integrated Public Sector Vocabulary, version 2.00.*

Campbell, D. (1999) Interception Capabilities 2000, i: Holdsworth D. (red.) (1999) *Development of surveillance technology and risk of abuse of economic information (An appraisal of technologies for political control)*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme

Cole, S. A. Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate i: Lazer D. (red.) (2004) *DNA and the Criminal Justice System: The Technology of Justice,* MIT Press, s. 63-89

Commission of the European Communities (2005) *Proposal for a council decision on the establishment, operation and use of the second generation Schengen information system (SIS II).* Brüssel

Committee on the Judiciary, The United States Senate (2001) *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age. Testimony of James X Dempsey (pp 47-61).* Washington: US Government Printing Office

Council of the European Union (2005) *NOTE from Presidency to Strategic Committee on Immigration, Frontiers and Asylum: Minimum common standards for national identity cards.* Brüssel: DG Justice and Home Affairs

Det danske Udenrigsministeriet (2004) *En verden i forandring - nye trusler, nye svar. Redegørelse fra regeringen om indsatsen mod terrorisme.* København: Det danske Udenrigsministeriet

D-G Energy and Transport [lesedato: 22.02.2007] *Galileo – Satellite Navigation System.*

Eagle og Pentland (2006) *Eigenbehaviours:* Identifying Structure in Routine, submitted to: *Ubicomp '06*. September 17-21. Orange County. CA

EPIC (2005) *Carnivore page.* http://www.epic.org/privacy/carnivore/

EPIC (2005) Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, *Spotlight on Surveillance* (August 2005).

ESSTRT (2005) *Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"*

European Commission (2003) *Airline passenger data transfers from the EU to the United States (Passenger Name Record).* Brüssel
http://ec.europa.eu/comm/external_relations/us/intro/pnrmem03_53.htm

European Commission, Information Society and Media (2006) *eCall – saving lives through in-vehicle communication technology.* Brüssel

European Commission, Justice and Home Affairs (2006) *EU – Passport Specification Biometrics Deployment of EU-Passports* Working Document (EN) – 28/06/2006.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2005) *Proposal for a regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between members on short stay-visas.* Brussels

European Parliamentary Technology Assessment Network (2006) *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries.* Oslo: Teknologirådet

FAST Search Best Practices TM (2006) Searching Rich Media, *Search 360* (februar 2006).

Finkenzeller, K. (2003) *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* 2. utgave. München: Carl Hanser Verlag

Gasson et al. (red.)(2005) *D 3.2, A study on PKI and biometrics.* FIDIS consortium

German Federal Office for Information Security (2005) *Common Criteria Protection Profile. Machine Readable Travel Document with „ICAO Application", Basic Access Control* Version 1.0. Bonn: BSI

German Federal Office for Information Security (2005) *Digitale Sicherheitsmerkmale im elektronischen Reisepass.* Bonn: BSI

German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems.* Bonn: BSI

Hegghammer, T. (2006) *Terrorisme og ny kommunikasjonsteknologi.* Kjeller: Forsvarets forskningsinstitutt

Heinrich, C. (2005) *RFID and beyond. Growing your business through real world awareness.* Indianapolis: Wiley Publishing

Hellevik, O. (1995) *Sosiologisk metode,* Oslo: Universitetsforlaget

Hempel og Töpfer (2004) *CCTV in Europe.* Berlin: Technische Universität Berlin

Henderson, Bruce og Burton (2001) Matching faces of Robbers captured on Video*, Applied Cognitive Psychology* **15**, s. 445-464,

Hildebrandt og Backhouse (2005) *D 7.2 Descriptive analysis and inventory of profiling practices.* FIDIS consortium

ICAO (2004) Annex 1 Use of Contactless Integrated Circuits In Machine Readable Travel Documents*, Biometrics Deployment of Machine Readable Travel Documents, Technical Report* v.2.0 Version 4.0. International Civil Aviation Organization (ICAO)

ICAO (2004) *Machine Readable Travel Documents Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies*, Version 1.7. International Civil Aviation Organization (ICAO)

ICAO (2006) *ICAO MRTD Report* **Volume 1** (Number 1). Montreal: International Civil Aviation Organization (ICAO)

ICAO TAGMRTD/NTWG (2004): *Biometrics Deployment of Machine Readable Travel Documents, Technical Report* v.2.0. International Civil Aviation Organization (ICAO)

Institute for Prospective Technological Studies (IPTS) (2005) *Biometrics at the Frontiers: Assessing the impact on Society.* European Communities

Jain, Bolle og Pankanti (1999) *Personal Identification in Networked society.* Norwell, Massachusetts: Kluwer Academic Publisher

Justis- og politidepartementet (2005): *NOU 2005:19. Lov om DNA-register til bruk i strafferettspleien.* Oslo: Statens Forvaltningstjeneste Informasjonsforvaltning

Justis- og politidepartementet (2005): *Ot.prp. nr. 60 (2004-2005): Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet).* Oslo: Justis- og politidepartementet

Kinnegig, T. A. F. (2004): *PKI for Machine Readable Travel Documents offering ICC read-only access* v 1.1. International Civil Aviation Organization (ICAO)

Kommunal- og regionaldepartementet (2003): *Rundskriv H19/03*: *Ikrafttredelse av endringer i utlendingsloven og utlendingsforskriften.* Oslo: Kommunal- og regionaldepartementet

Lyon, Hardenberg (2001) Warum Neugeborene mehr wissen als Grosse manchmahl ahnen*, GEO* (7), s. 27-42, Hamburg

McMunn, Mary K. (2006) Machine Readable Travel Documents with biometric enhancement: The ICAO Standard, *ICAO MRTD Report* **Volume 1 (**Number 1). Montreal: International Civil Aviation Organization (ICAO)

Meints og Hansen (2006) *D 3.6 Study on ID Documents.* FIDIS consortium

Naylor og Attwood (2003) *Annotated Digital Video for Intelligent Surveillance and Optimised Retrieval.* The ADVISOR Consortium

Norris, McCahill og Woods (2004) *Editorial. The Growth of CCTV: A global perspective in the international diffusion of video surveillance in publicly accessible space*. Surveillance & Society

OECD Working Party on Information Security and Privacy (2004) *Background material on biometrics and enhanced network systems for the security of international travel*. Paris: OECD

OECD Working Party on Information Security and Privacy (2004) *Biometric-based technologies.* Paris: OECD

Office for Public Management (OPM) (2005) *Research into the use of personal data sets held by public sector bodies.* Final report for Council for Science and Technology (draft). London: OPM

Parliamentary Office for Science and Technology (POST) (2002) *Postnote number 175: CCTV*. London: POST

Ratha, Connell og Bolle (2001) Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal* **Vol 40** (no 3)

Rejman-Greene, M. (red.) (2003): *Biovision Roadmap* issue 1.1. Ipswich: BIOVISION

Rieback et al. (2006) *Is Your Cat Infected with a Computer Virus?* Amsterdam

Rieker, P. og Knutsen, B. O. (2003) *EUs "nye" sikkerhetspolitikk: Bekjempelse av terrorisme og internasjonal kriminalitet.* Oslo: Forsvarets forskningsinstitutt og Norsk utenrikspolitisk institutt

Riksaasen, T. (1993/94) *Telematikknett.* Trondheim: NTNU

Safety Support (2006) *eCall: Saving a life every four hours!*

Sarma, Weis, Engels (2003): RFID Systems and Security and Privacy Implications, i: B.S. Kaliski Jr. et al. (Red.) (2003) *CHES 2002* s. 454-469. Berlin: Springer-Verlag

Tekonologirådet (2005): *Elektroniske spor og personvern.* Oslo: Tekonologirådet

Temporary Committee on the ECHELON Interception System *(2001) Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098 (INI)).* Brüssel: European Parliament

Texas A&M Research Foundation *Employee's guide to security responsibilities. Bugs and Other Eavesdropping Devices* http://rf-web.tamu.edu/security/SECGUIDE/Home.htm

Thalheim et al. (2002) Body Check*, c't* (11/2002), s. 114

The European Union (2006) AGREEMENT between the European Union and the United Stats of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security*, Official Journal of the European Union* **Vol 69** (No 131), s. 41543

The European Union (2006) DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public

communications networks and amending Directive 2002/58/EC, *Official Journal of the European Union*

The House of Lords (1998) *Fifth report of the House of Lords Science and Technology Select Committee*. London: Science and Technology Committee Publications

UK Home Affairs Committee Publication: *Home Affairs – Fourth Report* 2003-04 (ID Cards)

United States District court for the northern district of California, San Jose division (2006) *Gonzales vs. Google*, *No. CV 06-8006MISC JW*.

United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain.*, Washington: GAO

United States Government Accountability Office (2006) *PERSONAL INFORMATION Agencies and Resellers Vary in Providing Privacy Protections*. *Statement of Linda D. Koontz, director, before the Subcommittee on Commercial and Administrative Law and the Subcommittee on the constitution, Committee on the Judiciary, House of Representatives*, April 4 2006. Washington: GAO

US Department of Defense (2003): *Total Information Awareness (TIA)* Update February 2003. http://www.defenselink.mil/Releases/Release.aspx?ReleaseID=3625

US Department of Defense (2006): *Dictionary of Military and Associated Terms*, *Joint Publication 1-02*, med tilføyelser frem til 8. august 2006. DoD

Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*, utkast mars 2005. BITE project

Weitzner et.al (2006): *Transparent Accountable Data Mining. New Strategies for Privacy Protection*. Cambridge, MA: MIT CSAIL

Wilson, D. H. (2005): *How to survive a robot uprising. Tips on defending yourself against the coming rebellion*, London: Bloomsbury Publishing Plc

Wood, D. M. (red.) (2006) *A Report on the Surveillance Society*. Surveillance Studies Network For the Information Commissioner

Wright, S. (1998): *An appraisal of the Technologies of Political Control*. Luxembourg: European Parliament, Directorate General for Research, Directorate B, The STOA Programme

Nyhetsartikler

BBC News (2007) World's tiniest RFID tag unveiled, *BBC News,* 23. februar 2007 http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6389581.stm

Datatilsynet (2007) *Statens Vegvesen holdt tilbake viktig AutoPASS-informasjon.* 1. mars 2007

European Commission Press Release (2005) *MEMO/05/188, Schengen: from SIS to SIS II.* Brüssel, 1. juni 2005

FOX News (2005) FBI Ditches Carnivore Surveillance System. *FOX News* 18. januar 2005, http://www.foxnews.com/story/0,2933,144809,00.html

Gadher, D. (2004) Plane passengers shocked by their X-ray scans*, The Sunday Times*, 7. november 2004 http://www.timesonline.co.uk/article/0,,2087-1348172,00.html

Halvorsen, F. (2006) SAS får benytte fingeravtrykk*, Teknisk Ukeblad*, 29. april 2006 http://www.tu.no/nyheter/ikt/article51090.ece

Heise Online (2006) ePass-Hack im niederländischen TV demonstriert, *Heise Online* http://www.heise.de/newsticker/meldung/69127 .

IDABC: FR: Future French eID card to become compulsory, *eGovernment news*, 14. april 2005. http://europa.eu.int/idabc/en/document/4100

IDABC: FR: Future French electronic ID card to include two biometrics, *eGovernment news*, 3. september 2004 http://ec.europa.eu/idabc/en/document/3249/335

Love, D. (2004): Progressive's Black Box: Is Big Brother Good for the Industry*, Insurance Journal*, 6. desember 2004. http://www.insurancejournal.com/magazines/southeast/2004/12/06/features/50322.htm

Marks, P. (2006): Pentagon sets its sights on social networking websites*, New Scientist*, juni 2006 http://www.newscientisttech.com/channel/tech/mg19025556.200-pentagon-sets-its-sights-on-social-networking-websites.html

McCullagh, D. (2007): FBI turns to broad new wiretap method, *CNET News*, 30. januar 2007, http://news.com.com/FBI+turns+to+broad+new+wiretap+method/2100-7348_3-6154457.html

Petrie, E. (2002): Iceland places trust in face scanning*, BBC News*, 24. januar 2002 http://news.bbc.co.uk/1/hi/sci/tech/1780150.stm

Reichgott, M. (2005): Chicago Pairing Surveillance Cameras with Gunshot Recognition Systems, *Security Info Watch.com* http://www.securityinfowatch.com/online/CCTV--and--Surveillance/Chicago-Pairing-Surveillance-Cameras-with-Gunshot-Recognition-Systems/4628SIW427

RFID Journal (2003): Hitachi Unveils Smallest RFID Chip *RFID Journal,* http://www.rfidjournal.com/article/view/337/1/

Strande M. (2006) Ingen finger-id på norske flyplasser*, Teknisk Ukeblad,* 3. oktober 2006 http://www.tu.no/data/article60056.ece

Sweetman, B. (2005): Mini UAVs – the next small thing? *Jane's International Defence Review*, 11. mai 2005

Tendler, S. (2005): "Smart" CCTV could fight terrorist threat in stations*, The Times*, 15. november 2005 http://www.timesonline.co.uk/article/0,,2-1872083,00.html

The Royal Society *Superhuman vision – seeing with terahertz* http://www.royalsoc.ac.uk/exhibit.asp?id=4661&tip=1

The Sunday Times (2006): Word on the street ... They're listening, *The Sunday Times*, 26. november, 2006 http://www.timesonline.co.uk/article/0%2C%2C2087-2471987%2C00.html

Wessel, R. (2006) Airport monitoring system combines RFID with video*, RFID Journal.* 18. september 2006 http://www.rfidjournal.com/article/articleprint/2658/-1/1

Appendiks A – Intervjuer og intervjuguide

Om intervjuene

Både i forberedelsene til og arbeidet med dette dokumentet, har eksperter fra forsknings-institusjoner og meningsdannere blitt intervjuet. Intervjuene ble utført på en uformell måte, basert på en guide som ble utformet på forhånd. Dette åpner for at intervjueren kan komme over informasjon i løpet av intervjuet som ikke tidligere ble vurdert, men som likevel inviterer til videre diskusjon.[186]

På grunn av intervjuenes uformelle karakter, kunne et intervjuobjekt også foreslå andre eksperter som kunne tenkes å bidra og som derfor burde intervjues. Følgende personer ble intervjuet i forbindelse med arbeidet med denne rapporten:

Magnar Aukrust
Magnar Aukrust er avdelingsdirektør i Justis- og politidepartementet, i Politiavdelingen. Han jobber særlig med internasjonalt politisamarbeid, biometriske pass og nasjonale ID-kort. Han har vært medlem i en rekke offentlige råd knyttet til det militære og politiet.

Christophe Birkeland, PhD
Christophe Birkeland er avdelingsdirektør for NorCERT, som er en del av Nasjonal sikkerhets-myndighet (NSM).

Heidi Mork Lomell, PhD
Heidi Mork Lomell er forsker ved Institutt for kriminologi og rettssosiologi (UiO). Som en del av Urbaneye-prosjektet, som ble støttet av Europakommisjonen, har hun forsket på bruken av videoovervåking og på allmenne oppfatninger av videoovervåking. Lomell deltar for tiden i prosjektet *For whom the bell curves*, hvor hun forsker på bruken av kriminalstatistikk i politiarbeid.

Svein Y. Willassen,
Svein Y. Willassen skriver for tiden sin doktorgradsavhandling om digitale bevis ved NTNU. Forut for det jobbet han som spesialetterforsker ved Politiets datakrimsenter (PDS). Willassen har deltatt i internasjonalt arbeid, blant annet med å utforme Interpols *Computer Crime Manual* og trekke opp retningslinjer for digital bevisanalyse hos Den internasjonale organisasjon for databevis (IOCE).

Ove Skåra
Ove Skåra jobber som informasjonsdirektør ved Datatilsynet.

Hanne P. Guldbrandsen
Hanne P. Guldbrandsen jobber som seniorrådgiver ved Datatilsynet, Juridisk avdeling. Hun er i tillegg medlem av Artikkel 29-gruppen vedrørende databeskyttelse.

---

[186] Hellevik, Ottar (1995): *Sosiologisk metode*

Isabel Münch
Isabel Münch er avdelingsleder for IT-Grundschutz ved Bundesamt für Sicherheit in der Informationstechnik (Tyskland).

Intervjuguide

Intervjuet bør innledes med en kort beskrivelse av PRISE og PASR, og våre kriterier for relevante sikkerhetsteknologier bør presenteres.

Intervjuobjektet bør informeres om all informasjon fra prosjektet vil publiseres i en *ugradert* rapport.

Bakgrunnsinformasjon om intervjuobjektet
I tillegg til intervjuobjektenes navn og organisasjon, kan interessant informasjon være:

- Hva er hans eller hennes profesjonelle bakgrunn?
- Hvilket område innenfor sikkerhetsteknologi jobber han eller hun med?
- Er han eller hun involvert i noen prosjekter (nasjonale eller internasjonale) som kan være relevante for PRISE?
- Er han eller hun involvert i noen offentlige utvalg, osv., som kan være relevante for PRISE?

Teknologier og teknologisk utvikling
Disse er noen nøkkelord for å sikre at så mye relevant informasjon som mulig kommer ut av intervjuet. Det er imidlertid viktig å følge opp interessante emner som intervjuobjektene trekker frem.

1) Innenfor det gitte teknologiområdet, hvilke sikkerhetsteknologier finnes i dag som er relevante for PRISE-prosjektet?
2) Hvordan brukes teknologien/systemet i praksis (dersom dette er relevant)?
3) Hvem bruker eller kommer til å bruke teknologien?
4) Hvorfor har det blitt iverksatt/forsket på/planlagt?
5) Hvordan ser intervjuobjektet for seg den fremtidige utviklingen innenfor sitt fagfelt?
6) På hvilken måte kan teknologien brukes til å identifisere individer eller avsløre tilleggsinformasjon om identifiserte individer?
    a) Lagres informasjonen i en database?
    b) Dersom det er tilfellet, hva slags informasjon blir lagret?
    c) Hvem har tilgang til informasjonen? Under hvilke forhold?
    d) Blir informasjonen utvekslet? Hvordan?

Avslutningsspørsmål
Det er viktig å forsikre seg om at det er tid til noen avslutningsspørsmål på slutten av intervjuet:

- Kan intervjuobjektet gi oss noen form for dokumentasjon som kunne være relevant for prosjektet?

- Finnes det noen andre eksperter som vi ikke har kontaktet og som kan ha informasjon som er relevant for prosjektet? Internasjonale ressurser er av særlig interesse.
- Er det i orden hvis vi ringer tilbake med oppfølgingsspørsmål eller hvis vi trenger å oppklare noe?