Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Rapport

Elektroniske spor

Rapport

Rapportnr 1008

Forfattere Jerker Danielsson, Arne-Kristian Groven, Thor Kristoffersen, Hans Jakob Rivertz, Åsmund Skomedal

Dato 6. juni 2005

ISBN ISBN-13 : 978-82-53-90516-7
ISBN-10 : 82-539-0516-5

Forfatterne

Jerker Danielsson, MSc., Konsulent, Mnemonic.

Arne-Kristian Groven, Cand. Scient, Seniorforsker, NR

Thor Kristoffersen, Dr. scient., Seniorforsker, NR

Hans Jakob Rivertz, Dr. Scient, Seniorforsker, NR

Åsmund Skomedal, Dr. ing., Forskningssjef, NR

Norsk Regnesentral

Norsk Regnesentral (NR) er en privat, uavhengig stiftelse som utfører oppdragsforskning for bedrifter og det offentlige i det norske og internasjonale markedet. NR ble etablert i 1952 og har kontorer i Informatikkbygningen ved Universitetet i Oslo. NR er et av Europas største miljøer innen anvendt statistikk. Det jobbes med svært mange forskjellige problemstillinger slik som estimering av torskebestanden, finansiell risiko, beskrivelse av geologien i petroleums-reservoarer og overvåking av klimaendringer. NR er også ledende i Norge innen utvalgte deler av informasjons- og kommunikasjonsteknologi. Problemstillinger kan være overvåke inntrengning i datasystemer, e-læring i skole og næringsliv, bruk av datateknologi i markedsanalyser samt anvendelser av multimedia på forskjellige plattformer. NRs visjon er forskningsresultater som brukes og synes.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Tittel	**Elektroniske spor**
Forfattere	**Jerker Danielsson, Arne-Kristian Groven, Thor Kristoffersen, Hans Jakob Rivertz, Åsmund Skomedal**
Dato	6. juni
År	2005
ISBN	ISBN-13 : 978-82-53-90516-7
	ISBN-10 : 82-539-0516-5
Publikasjonsnummer	1008

Sammendrag

Denne rapporten er utarbeidet på oppdrag fra Datatilsynet og Justisdepartementet i april og mai 2005.

Når funksjoner i samfunnet som tidligere ikke brukte teknologi erstattes med informasjonsteknologi åpnes nye muligheter for å samle inn elektroniske spor. F. eks. når man kun brukte kontanter for å betale med var det vanskelig å fange informasjon om hvem som kjøpte hva, men ved betaling med kredittkort er dette relativt enkelt rent teknisk sett.

Elektroniske spor kan deles opp i to typer; hendelsesdata/trafikkdata og innholdsdata. De oppstår generelt i ulike situasjoner og de mest vanlige er:

- *Autentisering og bruk av Digitale identiteter*
- *Adgangs og tilgangs kontroll*
- *Betaling*
- *Sporing av utstyr og mennesker*
- *Sensor datafangst*

Det brukes en rekke ulike teknologier som genererer elektroniske spor. Denne rapporten oppsummerer bredden i disse teknologiene og er primært ment å være et teknisk grunnlag for andre vurderinger av elektroniske spor. Det fokuseres i denne rapporten mest på hvor og hvordan elektroniske spor oppstår, bearbeides og lagres. Et bredt spekter fra telefoni og datanettverk til webtjenester, biometrisk identifisering og videoovervåkning dekkes av rapporten. I korte trekk beskrives også anonyme alternativer til dagens løsninger og den framtidige utvikling vurderes.

Emneord	Elektroniske spor, sikkerhet, personvern
Målgruppe	Offentlige myndigheter, tilsyn, forskningsinstitutter, universiteter og høyskoler
Tilgjengelighet	Åpen
Prosjektnummer	324006
Satsningsfelt	Informasjonssikkerhet
Antall sider	65

Forord

Norsk Regnesentral har på oppdrag fra Datatilsynet og Justisdepartementet utarbeidet denne rapporten om elektroniske spor og bruken av disse i samfunnet. Rapporten er en kartlegging av hva slags elektroniske spor som genereres, bearbeides og lagres i ulike tekniske systemer.

Arbeidet har hovedsakelig blitt utført i april og mai 2005. Forfatterne retter også en stor takk til deltagerne i referansegruppen for deres kommentarer og konstruktive innspill underveis.

Innhold

Figuroversikt

1 Introduksjon

1.1 Oppsummering

Når funksjoner i samfunnet som tidligere ikke brukte teknologi erstattes med informasjonsteknologi åpnes nye muligheter for å samle inn elektroniske spor. F. eks. når man kun brukte kontanter for å betale med var det vanskelig å fange informasjon om hvem som kjøpte hva, men ved betaling med kredittkort er dette relativt enkelt rent teknisk sett.

Elektroniske spor kan deles opp i to typer; hendelsesdata/trafikkdata og innholdsdata. De oppstår generelt i ulike situasjoner og de mest vanlige er:

- Autentisering og bruk av Digitale identiteter
- Adgangs og tilgangs kontroll
- Betaling
- Sporing av utstyr og mennesker
- Sensor datafangst

Det brukes en rekke ulike teknologier som genererer elektroniske spor. Denne rapporten oppsummerer bredden i disse teknologiene og er primært ment å være et teknisk grunnlag for andre vurderinger av elektroniske spor. Det fokuseres i denne rapporten mest på hvor og hvordan elektroniske spor oppstår, bearbeides og lagres. Et bredt spekter fra telefoni og datanettverk til webtjenester, biometrisk identifisering og videoovervåkning dekkes av rapporten. I korte trekk beskrives også anonyme alternativer til dagens løsninger og den framtidige utvikling vurderes.

Generelt kan det oppsummeres at det blir stadig flere elektroniske spor og at utviklingen ikke kommer til å bremse særlig med det første. I de aller fleste systemer som behandler elektroniske spor er det mye større muligheter enn det som det gis rom for i forhold til for eksempel personopplysningsloven og begrensninger må dermed iverksettes. At disse begrensningene må ivaretas av (arbeids)rutiner for bruk av teknologien, og ikke i særlig grad ivaretas av teknologien selv, er en problemstilling som bør belyses ytterligere.

1.2 Formål

Denne rapporten er utarbeidet på oppdrag fra Datatilsynet og Justisdepartementet i april og mai 2005.

Formålet med rapporten er å kartlegge hvilke elektroniske spor som den enkelte potensielt etterlater seg. Dette er et omfattende spørsmål og denne rapporten vil derfor gi en *oversikt* over temaet. Arbeidet har fokusert på å kartlegge bredden av kilder til elektroniske spor. Derfor vil den enkelte kilde ikke beskrives så utførlig som kan være ønskelig for andre formål, som for eksempel en reell vurdering av om en tekologi innebærer brudd på personopplysningsloven eller lage veiledninger for at en teknologi ikke skal medføre ulovelig bruk.

En slik kartlegging kan angripes fra forskjellige perspektiv. De perspektiv som har blitt brukt i arbeidet med denne rapporten og som brukes for å presentere resultatet av arbeidet beskrives i

kapittel 2. Forhåpentlig kan det rammeverket disse perspektivene utgjør være til nytte for ytterligere kartlegging og vurdering av kilder der mer detaljert dokumentasjon er viktig.

Kartleggingen som presenteres i denne rapporten fokuserer på hvilke elektroniske spor om den enkelte som *potentielt* kan samles inn med eksisterende teknologi i motsetting til hva som i realiteten samles inn. Dette valget er tatt ettersom både legitim og ikke legitim innsamling, samt kriminell innsamling av elektroniske spor, er av interesse for personvernet. Det har heller ikke været ønskelig med en streng avgrensning til dagens situasjon men også ønskelig å se på hvilke muligheter som finnes i nærmeste framtid. Det er også en glidende overgang for når informasjon kan defineres som et elektronisk spor avhengig av om den slettes "umiddelbart", etter noen sekunder, dager eller uker. Ofte er det slik at en teknologi kan brukes slik at den går fra en modus med "umiddelbar sletting" til lagring ved enkle grep og det er opp til prosedyrene som styrer bruken av teknologien hva som skjer – ikke teknologien selv.

Generering og innsamling av elektroniske spor kan være kjent eller ikke kjent for den som det samles inn data om. Dette blir ofte kalt aktiv respektive passiv generering/innsamling av elektroniske spor. Denne rapporten søker å fokusere hovedsakelig på passiv genereringen og innsamlingen av elektroniske spor, dvs. den del som brukeren ofte er ikke er klar over. Tradisjonelt er det antatt at passivt genererte opplysninger utgjør størst trussel mot personvernet ettersom brukeren ikke er klar over innsamlingen og derfor ikke har mulighet å beskytte seg og benytte de rettigheter lovgivingen gir den enkelte.

Elektroniske spor som samles inn av utstyr uten at det nødvendigvis er kjent for brukeren eller den som eier utstyret (brukeren og eieren kan være samme person, men de trenger ikke å være det) er av spesielt interesse. Det blir eksempelvis stadig vanligere at elektronisk utstyr er utstyrt med harddisk og på disse kan det lagres elektroniske spor uten at det er kjent for brukeren eller eieren av utstyret.

Aktivt genererte (brukergenererte) opplysninger kan selvsagt også utgjøre en personvernsrisiko, særlig hvis de holdes opp mot opplysninger i andre systemer. Passivt genererte opplysninger kan, sammen med aktivt genererte opplysninger, også brukes som grunnlag for detaljerte personprofiler på brukere av et system.

Rapporten vil også beskrive noe om alternativer til dagens teknologi som ikke alltid er like hensiktsmessig med tanke på hva slags spor og hvor mange som genereres. Spesielt teknologi som støtter anonymitet er av interesse.

1.3 Avrensninger

Denne rapporten behandler ikke utveksling av elektroniske spor mellom virksomheter, kun direkte innsamling av elektroniske spor. Politiets innsamling av elektroniske spor er ikke heller behandlet i denne rapporten.

Det er heller ikke lagt vekt på å vurdere graden av kobling mellom sporene og den enkelte person. Kvaliteten på denne koblingen varierer i ulike tilfeller og ytterligere analyser av disse aspektene kan være hensiktsmessige.

Denne rapporten vurderer heller ikke om noen elektroniske spor er mer sensitive enn andre.

2 Elektroniske spor

2.1 Beskrivelse

Overgangen til "IT alderen" har stor betydning for samfunnet på flere måter. Det følgende beskriver endringer vedrørende sporbarhet.

"To be in cyberspace is to be recorded. Digital activities and objects are nothing but an ensemble of traces and records. Each electronic action in cyberspace implies the creation of tread marks; digitalization involves the generation of representations, more or less permanent. Those digital footprints can be, by nature, reconstituted, recreated and saved indefinitely. Where a vast number of activities in traditional space are inherently non-traceable, cyberspace actions are the traces themselves."[1]

Et spor kan være et objekt (f. eks. et dokument) eller dokumentasjon av en hendelse (f. eks. signatur på at en pakke har blitt mottatt). Alle objekt og hendelser i den elektroniske verden representeres av bitstrenger. Disse bitstrengene er i seg selv elektroniske spor som kan lagres. Kopier er i tillegg identiske og kan distribueres raskt og effektivt til andre. Det samme gjelder ikke i den fysiske verden. Der må aktiviteter ofte fanges av en observatør, et menneske eller teknologi og kopier er ikke alltid like originalen.

Et elektronisk spor kan fortelle om at en hendelse har skjedd og innholdet i selve hendelsen. Eksempelvis kan et elektronisk spor kan fortelle at en e-post har blitt sent mellom to e-postadresser og det kan fortelle om hva som stod i selve e-posten.

De elektroniske spor som vi primært er interessert i her er de som kan knyttes til en enkeltperson, altså elektroniske spor som forteller noe om den enkeltes handlinger, lokasjon, etc.

Disse elektroniske sporene faller inn under begrepet personopplysninger slik det er definert i personopplysningsloven. Denne definerer personopplysninger som: "opplysninger og vurderinger som kan knyttes til enkeltperson".

I forhold til personvernet antas det at påliteligheten for den knytning som gjøres mellom opplysningene og en person er et sentralt tema. På den ene siden finnes spor som beviselig ikke har noen tilknytning til en person, altså anonyme transaksjoner, og på den andre siden juridisk bindene dokumenter signert med digitale signaturer. De fleste elektroniske spor vil befinne seg et sted imellom disse to ytterpunkter og hvordan denne knytningen konkretiseres i faktiske systemer og hvordan vi forstår og resonerer rundt dens kvalitet antas å være viktig for personvernet.

Denne rapporten vil ikke gå særlig inn på vurderinger av hvor enkelt eller vanskelig det er å knytte et elektronisk spor til en enkeltperson. Elektroniske spor som i dag ikke knyttes til identifiserte personer fordi teknikken foreløpig ikke er tilstrekkelig utviklet, men som i nær fremtid vil kunne tenkes å bli identifisert, er derfor også relevante i denne sammenheng.

[1] M. H. Barrera og J. M. Okai, Digital Correspondence: Recreating Privacy Paradigms, International Journal of Communications Law and Policy, nr. 3 1999.

Et annet aspekt ved personopplysninger er selve bruken av informasjonen. Det er fullt mulig for en leverandør å samle kundeinformasjon med det formål å få betalt for og levert en vare for deretter å gjøre "gjenbruk" av informasjonen til å sende reklame. Dette vil ofte oppfattes som effektivt og dermed hensiktsmessig, men det er ikke noen automatikk i at det dermed er lovelig. Informasjon som samles inn for ett formål skal normalt ikke brukes for andre formål uten brukers "informerte samtykke". Det er viktig å påpeke at vi gjennom eksempler og lignende i denne rapproten ikke tar stilling til hvorvidt gjeldene praksis er innenfor lovverket eller ikke. Det påpekes tilfeller der slike muligheter finnes og at økte informasjonsmengder øker den totale sannsynligheten for misbruk.

2.2 Kartleggingsperspektiv

Arbeidet med å kartlegge de elektroniske spor som den enkelte etterlater seg kan angripes fra forskjellige perspektiv.

De perspektiv som har bruktes i utarbeidning av denne rapport er:

- Typer av elektroniske spor
- Teknologier som genererer og/eller brukes for å samle inn elektroniske spor
- Lagringssteder for elektroniske spor
- Generering og innsamling av elektroniske spor i forskjellige samfunnssektorer, situasjoner og scenarier.

Sammenhengen mellom disse perspektiv kan oppsummeres som:
Forskjellige *teknologier* anvendes i forskjellige *samfunnssektorer* og *situasjoner/scenarier* for å generere og samle inn *elektroniske spor av forskjellige typer*. Disse elektroniske spor *lagres på forskjellige steder*. (Fokus på teknologier for generering og innsamling av elektroniske spor).

I utarbeidelsen av denne rapporten har alle disse perspektiv blitt brukt for å fange opp så mange relevante tilfeller som mulig av elektroniske spor som den enkelte etterlater seg. Forhåpentlig kan denne strukturen inspirere andre å identifisere elektroniske spor som ikke er behandlet i denne rapport. Resultatet presenteres også utefra disse perspektiv:

- Kapittel 3 presenterer forskjellige typer av elektroniske spor.
- Kapittel 4 presenterer en rekke generelle situasjoner hvor elektroniske spor genereres og samles inn.
- Kapittel 5 behandler forskjellige teknologier som genererer elektroniske spor og som brukes til å samle inn elektroniske spor.
- Kapittel 6 gjennomgår ulike steder der elektroniske spor lagres.
- Kapittel 7 omhandler noen scenarier fra hverdagen.
- Til slutt presenterer Kapittel 8 teknologi for anonyme tjenester og Kapittel 9 ser på tendenser og fremtidig utvikling.

3 Typer av elektroniske spor

Et elektronisk spor kan beskrive en hendelse (f. eks. at en e-post har blitt sendt eller at noen har åpnet et elektronisk dokument) og/eller et elektronisk spor kan inneholde selve innholdet i hendelsen (innholdet i e-posten eller dokumentet).

Beskrivelsen av en hendelse kalles ofte *trafikkdata/kommunikasjonsdata* i tilfellet hvor hendelsen er en form for kommunikasjon eller mer generisk *hendelsesdata* for all typer av hendelser. En hendelse har typisk attributter som tid, sted og involverte personer knyttet til seg.

Selve innholdet kalles ofte *innholdsdata*. Innholdsdata kan inneholde forskjellige typer av informasjon f. eks. helseinformasjon, informasjon om et salg.

For visse hendelser trenger det ikke å være relevant å skille mellom hendelsesdata og innholdsdata. F. eks. for hendelsen at noen passerer bomringen er det kanskje ikke hensiktsmessig å ta med alle innholdsdata (hvilket bilmerke, bilde av sjåfør, osv), men bare hvilken type kjøretøy det var som passerte (personbil, lastebil).

Hendelsesdata og innholdsdata kan innholde flere typer av informasjon. Tabell 1 lister noen relevante informasjonstyper.

Type	Beskrivelse	Eksempler på spor og teknologi
Identifiserende informasjon	***Informasjon som direkte identifiserer en person***	***Personnummer***
Identitetsinformasjon	***Informasjon om seksuelle legning, ekteskapelig status, etnisk tilhørighet etc.***	***Ugift***
Lokasjonsinformasjon	***Informasjon om hvor vi befinner oss i den fysiske verden og i den elektroniske ved gitte tidspunkter.***	***Mobiltelefoni GPRS***
Helseinformasjon	***Informasjon om den enkeltes helse, sykdom, sykemelding medisinering, behandling etc.***	***Elektroniske pasient-journaler Overvåkning av pasienter i hjemmet***
Kundeinformasjon	***Informasjon om kunder***	***Kredittkortnummer***
Medlemskapsinformasjon	***Informasjon om medlemskap i foreninger og partier***	

Biometrisk informasjon	***Informasjon om en personlig egenskap / karakteristikk***	***Biometriske pass med Fingeravtrykk eller ansiktsgeometri***
Adgangs og tilgangsinformasjon	***Informasjon om fysisk adgang og logisk tilgang***	***Filsystemlogger Besøkslister Passering i bomring***
Ytringer	***Meninger distribuert on-line til større grupper av personer***	***e-post til distribusjonslise news***
Betalingsinformasjon	***Informasjon om kjøp***	***Betalingstransaksjon med bankkort***

Tabell 1 Eksempler på informasjonstyper

Et elektronisk spor innholder ofte flere typer av informasjon. Et elektronisk spor som forteller om et innkjøp innholder naturligvis betalingsinformasjon men også ofte indirekte lokasjonsinformasjon (betalingen ble utført på et visst tidspunkt på et gitt sted) og kanskje også helseinformasjon (det var medisiner som ble kjøpt).

På samme måte kan lokasjonsinformasjon avledes fra adgangs og tilgangsinformasjon.

4 Situasjoner

Elektroniske spor genereres i mange forskjellige situasjoner. I dette avsnittet presenteres noen generelle situasjoner der elektroniske spor genereres og samles inn. For hver situasjon gis det eksempler på hvordan situasjonen oppstår i forskjellige samfunnssektorer og scenarier.

Autentisering, betaling og adgangskontroll henger ofte sammen. Ditt betalingskort kan være knyttet til en digital identitet og denne identiteten er knyttet til ditt personnummer. Når du betaler med kortet så autentiserer du deg ved at du har kortet og ofte ved at du i tillegg kan PIN-koden som bekrefter bruken. Når du har betalt får du en kontrollert eller avgrenset tilgang til tjenesten.

Sporing og sensor datafangst har det felles at de dreier seg om informasjonsinnsamling fra et objekt (ting eller menneske). Ulovelig innsamling av elektroniske spor behandles i seksjon 4.6.

Når det gjelder vurderinger av hvilke av disse situasjonene som generer de mest interessante sporene er det vanskelig å si noe konkret om hver enkelt. Det er derimot viktig å påpeke at med en stor mengde elektroniske spor og mange ulike kilder er det økende fare for effektiv samkjøring av ulike informasjonsklider og databaser. I slike tilfeller er det mulig å bruke informasjonen effektivt og til helt andre formål enn det opprinnelige og denne muligheten representerer en utvikling som bør følges nøye.

4.1 Autentisering og digitale identiteter

Autentisering av brukere er prosessen med å verifisere at brukeren virkelig har den digitale identitet (f. eks. et brukernavn) som han/hun hevder å ha.

En digital identitet skapes av en utsteder ved registrering. Den digitale identitet som lages kan være knyttet til en fysisk person, eksempelvis gjennom personnummer. En slik identitet identifiserer deg direkte. En identitet trenger likevel ikke å være direkte knyttet til deg. F.eks. kan man tenke seg at en kan registrere en e-post konto på Internett uten å oppgi navn, adresse etc. (hvis utsteder spør om det, kan en alltid oppgi falske opplysninger). Et lignende eksempel fra den papirbaserte veden hvor en ikke trenger å oppgi identifiserende opplysninger ved registrering er hvis en åpner en anonym bankkonto i Sveits.

I de tilfeller hvor den digitale identiteten skal knyttes til en fysisk person så må en som bruker på en eller annen måte "bevise" at du virkelig er den du hevder. Brukerens identitet må dokumenteres gjennom å fremvise "gyldig offisiell legitimasjon". I tillegg må denne dokumentasjonen verifiseres og relateres til den person som møter opp fysisk. Ofte er det krav til at dokumenter og spor fra registreringen lagres. I tilknytning til eSignaturloven [2] er det for kvalifiserte sertifikater satt krav til lagring av dokumentasjonen fra verifiseringsprosessen ved det personlige oppmøtet på 10 år. Det er altså svært viktig at autentiseringen ved registrering er korrekt, ellers oppstår mulighet for identitetstyveri.

Til den digitale identiteten som skapes knyttes "authentication credentials" eller akkreditiver. Denne informasjonen brukes senere av personen som har blitt tildelt den digitale identiteten for å bevise at han/hun er den som innehar identiteten.

Autentisering kan baseres på tre typer av akkredititver eller "faktorer":

- Noe du *vet* (en hemmelighet, f.eks. passord)
- Noe du *har* (en gjenstand f. eks. adgangskort)
- Noe du *er* (en egenskap, f. eks. fingeravtrykk)

Den siste typen av autentisering, noe du *er*, kalles ofte biometrisk autentisering. Denne typen autentisering skiller seg fra de andre da den er direkte knyttet til deg som person. Passord og adgangskort kan byttes ut fordi de er frikoblet fra deg som individ. Et fingeravtrykk kan ikke byttes uten at du må igjennom en operasjon.

Flere typer autentiserings metoder kombineres ofte for å øke styrken på autentiseringen.

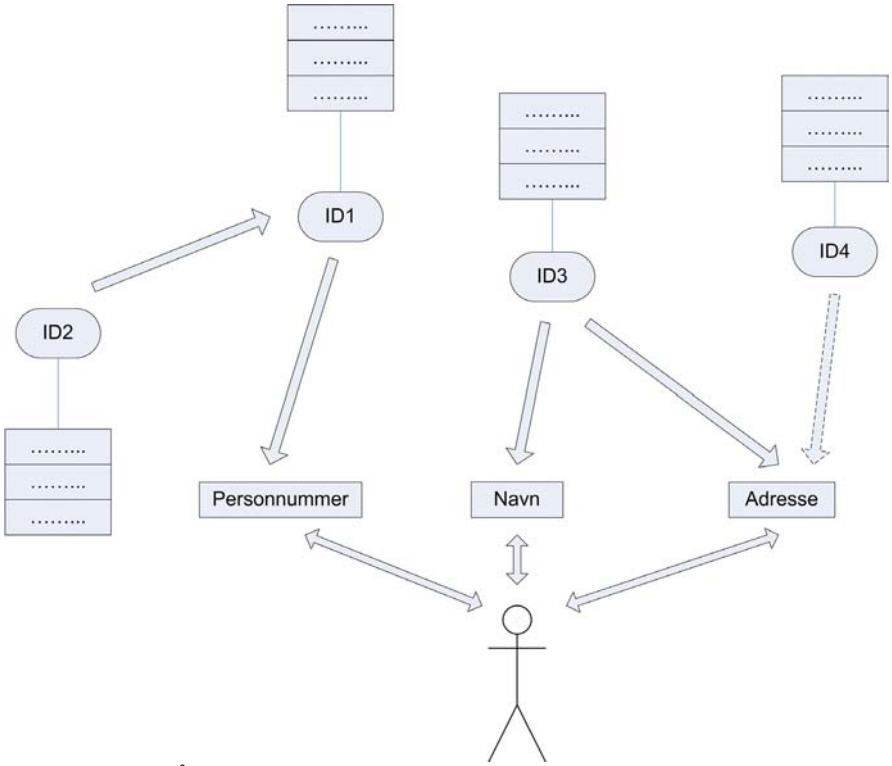
- Når du tar ut penger fra en minibank autentiserer du deg som eieren til din konto gjennom å både taste inn en PIN-kode (noe du vet) og ved å sette inn ditt kort (noe du har) i minibankautomaten.
- Såkalte Biometriske Pass er planlagt innført til høsten 2005 i Norge. Disse skiller seg fra de gamle ved at de inneholder en lesbar elektronsk representasjon av en eller flere "biometrier" tilhørende innehaveren og dette styrker verifiseringen ved bruk. Biometri innebærer at en ved utstedelse av passet må registrere en egenskap som eksempelvis fingeravtrykk og at det produseres en elektronisk referanse av denne.

[2] e-Signaturloven, http://www.lovdata.no/all/hl-20010615-081.html

Ved kontroll av passet vil en igjen avlese biometrien fra innehaveren og sammenligne denne med referanseverdien som leses elektronisk fra passet. Det er her en viktig diskusjon om referanseverdiene skal lagres andre steder enn i passene. Foreløpig vil løsningen i Norge ikke lagre disse referansene sentralt. Hva som skjer videre forstår vi at ikke er avklart per i dag, men det er svært viktig i forhold til elektroniske spor.

- Når du logger inn på et datasystem bruker du typisk (bare) noe du vet, ditt passord
- For å få adgang til kontoret trenger du ofte bare å dra ditt adgangskortkort (noe du har) gjennom en leser. Sent på kvelden og i helgene trenger du ofte også å taste inn en PIN-kode (noe du vet).

Digitale identiteter trenger som sagt ikke å være identifiserende. En digital identitet kan være en såkalt pseudonym ved at den ikke går an å koble direkte til den fysiske brukerens navn eller personnummer. Likevel er det viktig å være klar over at en slik digital identitet muligens *kan* kobles til ditt personnummer senere gjennom at andre data koblet til den digitale identiteten samkjøres med andre registre hvor du er registrert. Det kan også være slik at etter at du har brukt den digitale identiteten en stund finnes det så mye informasjon koblet til denne at det går ann å utlede informasjon som mer eller mindre identifiserer deg. Eksempelvis er det betydelig sannsynlighet for at en person kan identifiseres unikt hvis en kjenner fornavn og postkode for vedkommende.



Figur 1 Eksempel på forholdet mellom en persons digitale identiteter

Figur 1 viser et eksempel på hvordan en persons ulike digitale identiteter kan forholde seg til hverandre og at det til hver identitet er det koblet informasjon om personen. Når de digitale identitetene ID1 og ID3 ble registrert ble personens personnummer, respektive navn og adresse registret. Den digitale identiteten ID2 er koblet til den digitale identiteten ID1. Den som har kjennskap til både denne kobling og koblingen mellom ID1 og personens personnummer kan

dermed koble sammen ID1 og personens personnummer. Den digitale identiteten ID4 er ikke direkte koblet til personen, men det finnes en mulighet å utlede personens postnummer og muligens adresse om man analyserer de data som er knyttet til ID4.

I visse tilfeller finnes det ikke noen grunn til at din digitale identitet skal være identifiserende, andre ganger finnes det gode grunner til det. Det er gode grunner til at bankene trenger å knytte enkelte transaksjoner til enkeltpersoner, men det er ikke like gode grunner til at din lokale kiosk skal kunne knytte dine innkjøp til deg. Dette tar vi for gitt i den fysiske verden, men mye tyder på at vi ikke vil kunne handle anonymt i framtidens elektroniske kiosk.

Bruk av Identiteter
Ekte anonymitet er ofte ikke praktisk mulig og i mange situasjoner heller ikke ønskelig. Likevel bør det være et prinsipp at i et fritt samfunn tillates generelt individer å velge om når, til virken grad, og i hvilket omfang de vil bli identifisert i forskjellige situasjoner. Å kreve at folk må identifisere seg når det ikke er noe saklig behov for identifisering er å krenke personvernet. Det vurderes slik at det er reell fare for at nettopp dette i økende grad skjer i elektroniske løsninger. Som individer vil vi bli avkrevd vår digitale identitet uten å ha særlig kontroll på når, i hvilket omfang og med hvilken grunn autentisering kreves. Altså blir det svært viktig at de som avkrever en digital identitet gjør dette bare når behovet er reelt. Riktige vurderinger her vil være vanskelige og krever spesiell kompetanse. Det stilles spørsmål ved om denne kompetansen finnes i tilstrekkelig grad.

Det er en trend at forskjellige digitale identiteter knyttes opp mot hverandre og at samme digitale identitet brukes i mange forskjellige sammenhenger. Begrep som ”Single-sign-on” og ”Federated Identity” representerer uttrykk for denne utvikling. ”Single-sign-on” og ”Federated Identity” innebærer at du ikke trenger å logge inn på hver enkelt tjeneste for seg. Du logger inn en gang og siden skjer autentisering mot de ulike tjenestene du bruker i bakgrunnen. Dette innebærer at dine forskjellige digitale identiteter knyttes sammen eller at de erstattes med en felles digital identitet. Denne type av teknologi kan både brukes lokalt og på Internett. Når den brukes lokalt har den ikke så store konsekvenser for personvernet siden brukerens ulike digitale identiteter (f. eks. Windows og e-post brukernavn) allerede er kjente lokalt. Dette er derimot ikke tilfelle på Internett. Den digitale identitet du bruker på et websted er i utgangspunktet ikke kjent for et annet websted.

Denne utvikling drives av behovet av å forenkle for brukene. I dag trenger brukere å håndtere flere forskjellige passord, PINs, og kort. De fleste ser det intuitivt som noe positivt om man kunne redusere dette. Fra tjenestetilbyderes side er ”Single-sign-on” og ”Federated Identity” en mulighet å tilby integrerte tjenester (”one-stop-shops”). Du kan for eksempel logge inn på siden til et flyselskap og kan uten at du trenger å logge inn på nytt bestille hotell og leiebil fra andre leverandører. Dette virker umiddelbart som en god idé, men det kan ha betydning for personvernet hvis ikke brukeren informeres om hva som faktisk skjer. Bruk av PKI baserte identiteter er beskrevet i kap. 5.5.

4.2 Betaling

Det finnes ingen elektronisk ekvivalent til kontanter som per i dag er i kommersiell bruk i Norge. Det nærmeste vi kommer er antagelig den Mondex baserte løsningen som brukes av Norsk Tipping og BuyPass. Kontanter har den fordelen at de tilbyr en måte å betale på som er

helt anonym. At en elektronisk ekvivalent ikke er allment tilgjengelig fører til at alle elektroniske kjøp i utgangspunktet er sporbare til den enkelte.

I denne sammenheng bør det nevnes at den europeiske sentral banken skal ha planer (eller ha hatt planer) om å innføre RFID brikker, se kapittel 5.9, i sedler med høy valør for å gjøre det vanskeligere å forfalske dem[3]. Men en slik teknologi kan også brukes til å spore hvor enkelte sedler har blitt brukt. Dette er et eksempel på en aktivitet som tidligere etterlot seg minimalt med spor som endres av ny teknologi og nå kan bli en aktivitet som generer elektroniske spor.

Betalingsinformasjon er en rik kilde til informasjon om den enkelte. Betalingsinformasjon gir i utgangspunkt informasjon om:

- Hva har du har kjøpt
- Hvor mye du har betalt
- Din lokasjon ved kjøpsøyeblikket

Fra denne informasjonen kan annen informasjon avledes avhengig av hva du kjøpt, f. eks.:

- Hva du spiser - om du vegetarianer eller ikke
- Hva du leser
- Hvilke medisiner du bruker og dermed hvilke sykdommer du har
- Hva du har av fritidsinteresser

Betaling er ofte koblet til fysisk adgang og logisk tilgang. Du betaler for adgang/tilgang direkte eller så betaler du for et bevis som gir deg adgang/tilgang flere ganger eller over en bestemt tidsperiode. Ofte er det mulig å knytte et slikt bevis til betlingsinformasjonen knyttet til innkjøp av beviset.

Elektronisk betaling skjer oftest ved bruk av en form for betalingskort eller kredittkort. I disse tilfellene har butikken/butikkjeden mulighet å registrere hva hver kunde kjøper av butikken/butikkjeden. Mens banken/kredittkortselskapet har mulighet å registrere alle innkjøp dens kunder gjør elektronisk i alle butikker.

Det er nå også og mulig å betale mindre beløp med mobiltelefonen. Du betaler da dine innkjøp gjennom "e-cash", mikrobetalinger eller over mobiltelefonfakturaen. Din mobiltelefonoperatør har da mulighet til å registrere dine innkjøp. Det finnes også forskjellige løsninger for mikrobetalinger på Internett.

En del butikkjeder har også kundekort/bonuskort som kunden kan bruke for å registrere eller betale for innkjøpene i butikkjeden. Kunden får bonus på sine innkjøp og butikken får økt lojalitet og mulighet for å registrere hva hver kunde kjøper. Butikkjeden har også mulighet å skape kundeprofiler og dermed skreddersy tilbud til forskjellige kundegrupper.

4.3 Fysisk adgangskontroll og logisk aksesskontroll

Autentisering i en eller annen form er en forutsetting for adgangskontroll og logisk aksesskontroll. All fysisk adgangskontroll og logisk tilgangskontroll kan generere logger over hvem som har forespurt adgang/tilgang til hver tid.

[3] Security Technology: Where's the smart money?, The Economist, 9. februari 2002.

Logisk aksesskontroll regulerer ikke bare lese og skrive tilgang til filer eller dokument. Samme mekanismer brukes også til å regulere aksess til applikasjoner, funksjonalitet i applikasjoner, felt i en database, aksess til Internett, skrivere, e-post, installasjon av program etc.

I alle tilfeller hvor adgang og tilgang kontrolleres er det mulig å generere logger som innholder informasjon som svarer på spørsmålene hva, hvem, hvorfra og når. Adgang og tilgangslogger er per definisjon adgangs og tilgangsinformasjon og det er ofte mulig å avlede lokasjonsinformasjon fra denne informasjon.

Ofte brukes samme digitale identitet for regulere både fysisk adgangskontroll og logisk tilgangskontroll. En bedrift kan samkjøre disse loggene.

Tilgangskontroll og betaling
I mange tilfeller er adgangs og tilgangskontroll kombinert med betaling. Du betaler for et bevis (en billett) som gir adgang eller tilgang. Betaling og adgangs/tilgangs kontroll er i enkelte tilfeller kombinert i en transaksjon. F. eks. du betaler med ditt kredittkort som også blir din billett.

Dette er tilfelle på flytoget mellom Oslo og Gardermoen. Der har du muligheten at kjøpe en papirbillett kontant eller ved å betale med kredittkort. Du kan også reise billettløst ved å betale og bruke ditt kredittkort som billett. Du har også mulighet at registrere ditt kredittkort og din e-post adresse på Internett, slik at du kan få kvitteringen tilsendt elektronisk.

Av disse tre alternativ etterlater løsningen med kontant betaling ikke noen elektroniske spor som kan knyttes til en enkelt individ. Alternativet med papir billett betalt med kredittkort etterlater seg potentielt et elektronisk spor som forteller at passasjeren antagelig har reiset med flytoget på et gitt tidspunkt (lokasjonsdata). Fra denne informasjon og en flyrutetabell kan du potentielt utlede hvor passasjeren har reist videre. Det siste alternativet hvor du har registret din e-post adresse på Internett lager ytterligere elektroniske spor. Nå har bedriften som driver flytoget din e-post adresse som de kan koble til ditt kredittkort. Ettersom kvitteringen sendes ut på e-post lagres din reise også som et elektronisk spor i den e-post server passasjeren bruker og muligheten er tilstede for at e-posten har blitt fanget opp og/eller lagret på vei til din postkasse.

Det er ikke bare på flytoget som du kan bruke kredittkort som billett. Det forekommer også at du kan bruke kredittkort som flybillett og P-hus billett. Andre eksempler finnes sikkert også.

Bomstasjoner
Bomstasjoner er annet eksempel på kombinasjon av betaling og adgangskontroll. Dette eksemplet likner mye foregående eksempel. Også her er det mulig å betale kontant (med få unntak), men det mest praktiske er å kjøpe et abonnement for en viss tidsperiode. På oppdrag for Samferdselsdepartementet har Transportøkonomisk institutt (TØI) utarbeidet rapporten "Makt, beslutning og integritet - om IKT og personvern i transport". Denne rapporten etterlyser klare regler for bruk av IKT i samferdselssektoren. Se forøvrig også [4].

Et annet tilfelle hvor en etterlater seg et elektronisk spor ved adgang er når du registrerer deg som besøker hos mange virksomheter. Denne registrering foregår ofte elektronisk.

[4] Noen vet alltid hvor du kjører, http://www.forbruker.no/bil/article812902.ece

En problemstilling som ofte er knyttet til logisk aksesskontroll er et karv til etterrettelighet eller sporbarhet. Dette gjelder spesielt i arbeidslivet fordi bedrifter må beskytte sine systemer mot interne og eksterne trusler og eneste måten å kunne finne et sikkerhetsbrudd eller forhindre nye angrep på er å logge nok informasjon til å kunne vite med god presisjon hva som har skjedd. Formålet med alle disse sporene er altså "sikkerheten", men det er fristende å bruke denne informasjonen til andre ting, spesielt ved konflikter på arbeidsplassen. Se for øvrig artikkelen "Ikke lek med jobbens PC" 5 på VG Nett.

4.4 Sporing av utstyr og mennesker

Teknologier som mobiltelefoni, RFID og GPS gjør det mulig å fysisk spore utstyr og mennesker. Disse teknologiene beskrives nærmere i kap. 5.9, men her nevnes enkelte eksempler på anvendelser av sporningsteknologi.

Det finnes tjenester som tilbys av mobiloperatørene der man kan spore sine venner. Netcom Buddy[6] er et eksempel på en slik tjeneste. For at noen skal kunne spore din mobiltelefon må du godta en invitasjon fra den som vil kunne spore deg. Denne type teknologi kan misbrukes ved at du låner en annens mobiltelefon og melder den inn eller ved at du plasserer en mobiltelefon f. eks. i bilen til den som du vil spore[7].

Det finnes flere eksempel av sporing av ting som i varierende grad kan kobles til enkeltpersoner. For eksempel sporing av stålne biler og annet stålet utstyr. Muligheten til å spore en ting etter at noe har blitt stjålet innebærer også at det er mulig å missbruke denne funksjonaliteten når det sporbare utstyret ikke er stjålet.

Et annet eksempel på anvendelse av sporingsteknologi er så kalt "fleet management" som brukes for å optimalisere transport, f. eks. styring av drosjer og lastebiler. Indirekte fører dette til at sjåføren til det sporede kjøretøy også er sporbar.

En annen anvendelse er å bruke sporingsteknologi for å beregne forsikringspremier[8]. Sporingsteknologi kan gjøre det mulig for forsikringsselskapet å vite hvor du kjører og når. Dette kan siden anvendes som grunnlag for å beregne din forsikringspremie. Samme tekniske løsning kan også brukes for å beregne veiskatt eller veitoll.

Ofte er objektet klar over at han/hun spores. Men teknologien kan også brukes uten at objektet er bevisst dette f.eks. hvis noe som personen bærer på seg spores (mobiltelefon eller klær med RFID brikker).Jon Bing har skrevet følgende om dette tema:

"Likevel er dette bare begynnelsen. Man har eksempler på bruk av adgangskontroll for å øke bevegelsesfriheten til pasienter som har vanskelig for å gjøre rede for seg – i stedet for å låse dem inne, bærer de en ankelring eller lignende som gjør det mulig å lokalisere dem og finne dem igjen ved hjelp av satellittbasert posisjoneringssystemer. Lignende utstyr tilbys integrert i barneklær så foreldre skal kunne finne igjen barn som vandrer av sted på egen hånd. Ikke mye fantasi skal til før man kan tenke seg at slikt

[5] Ikke lek med jobbens PC, http://www.vg.no/pub/vgart.hbs?artid=101837

[6] https://netcom.no/tjenester/fleretjenester/nytteogunderholdning/buddy.html

[7] Reagerer på mobil-overvåking, Aftenposten, 26. august 2002, http://www.aftenposten.no/nyheter/nett/article387527.ece

[8] Bruker GPS til å beregne bilforsikring, 7. september 2004, http://www.digi.no/php/art.php?id=110512

utstyr blir påbudt som fjellvettregel nr 11 for å unngå unødvendig dyre leteaksjoner." Elektroniske spor, Jon Bing [9].

4.5 Datafangst med sensorer

Det utvikles stadig nye sensorer og mindre sensorer. Sensorer samler inn innholdsdata som kan være svært rik på informasjon.

Sensordataene sendes ofte over en form for trådløs kommunikasjon. Dette øker risikoen for at sensordataene fanges opp. Kommunikasjonen kan krypteres men krypteringen, er ofte svak ettersom sensorer har begrenset beregningskapasitet og batterikapasitet.

Vanligvis er objektet klar over at han/hun er tilknyttet sensorer, men sensorer kan selvfølgelig missbrukes. Sensorer kan brukes til å overvåke mennesker, f. eks. innsamling av helseinformasjon [10]. Sensorer brukes også ofte til å overvåke installasjoner/maskiner;

- biler med utstyr for automatisk diagnostikk og rapportering til verkstedet
- innbruddslarmer

Det er i slike systemer en risiko for at overskuddsinformasjon som forteller noe om individer samles inn, men hvis systemene er godt laget og tar hensyn til personvernet vil dette normalt ikke være et problem. En faktor er i hvilken grad informasjon prosesseres lokalt og sendes eller om det meste prosesseringen skjer sentralt. Ved lokal prosessering kan utstyret innholde sensitiv informasjon.

GPS teknologi er som nevnt også foreslått brukt i forbindelse med bilforsikringer. Dette kan ha sine fordeler, men har utvilsomt også implikasjoner for personvernet.

4.6 Kriminell aktivitet

Alt utstyr som lagrer elektroniske spor er et mulig mål for kriminell aktivitet. Det kan være utro tjenere som misbruker elektroniske spor som virksomheten har et legitimt behov at lagre eller det kan være eksterne som stjeler utstyr som innholder elektroniske spor eller en form for datamaskininnbrudd fra eksterne. Virus og ormer kan installere program på PCer som fanger opp og leser elektroniske spor og sender disse sporene til den som laget ormen eller viruset. Denne type av spionprogrammer kalles ofte "spyware".

Hva som lagres på forskjellige steder behandles i kapitlet om lagringssteder. Privat utstyr, som hjemme-PCer, inneholder ofte store mengder med elektroniske spor. Databaser av spesiell interesse kan være kundedatabaser og databaser med kredittkortsinformasjon.

Elektroniske spor kan også fanges opp når de sendes over kommunikasjonsinfrastrukturer som for eksempel Internett eller mobilnettet.

Stort sett all teknologi som er utviklet med gode intensjoner kan også brukes for kriminelle formål. Bruken av teknologi gjør samfunnet mer effektivt, men det samme gjelder for kriminell aktivitet – den blir også mer effektiv. F. eks. kan kriminelle også bruke diverse sporingsutstyr

[9] Elektroniske spor, Jon Bing, 2003.

[10] *Wireless health and care*, prosjekt, http://www.wshc.no/index.php

som GPS og RFID. Et annet eksempel er ”Phising”, angrep mot brukere der man forsøker lure brukere å oppgi kredittkortinformasjon eller brukernavn/passord på falske websider ved først å sende falsk e-post.

Kriminelle kan bruke kunnskap om navn, adresse, kredittkortnummer, personnummer etc. for å utføre transaksjoner i andres navn f. eks. bestille varer eller åpne en konto. Dette kalles identitetstyveri. Kriminelle kan få tak i denne type av informasjon gjennom ”phising”, avlytting av ukryptert informasjon, innbrudd i kundedatabaser eller bestikkelse av ansatte i virksomheter som håndterer slik informasjon. Identitetstyveri har alltid forekommet, men det kan tenkes at det er enklere og gjennomføre i dag når transaksjoner ofte er elektroniske (man trenger ikke å møte opp ansikt mot ansikt) og det skjer på globalt nivå. Det at man kan misbruke identiteten til personer som lever på andre siden av jordkloden medfører også at det ofte er vanskelig å få tatt de skyldige og selv om det lykkes kan det være vanskelig å få etablert nok bevismaterial til at de blir tiltalt og dømt.

At flere og flere transaksjoner utføres over Internett øker effektiviteten i samfunnet men det gjør det også enklere for kriminelle å utføre illegitime transaksjoner.

5 Teknologi og elektroniske spor

Teknologi brukes i denne sammenheng slik at den genererer, kommuniserer, lagrer og bearbeider elektronisk informasjon.

Det primære formålet med en teknologi kan være å samle inn spor. Slik teknologi kaller vi innsamlingsteknologi og beskrives i kap. 5.11. Eksempler på slik teknologi inkluderer: Spyware, Tracking cookies, web bugs og utstyr for telefonavlyttning.

Det primære formålet med teknologi er normalt ikke å samle in elektroniske spor. Likevel vil nesten alle teknologiske løsninger generere elektroniske spor relatert til den funksjonalitet teknologien tilbyr. Legitime grunner til at det genereres elektroniske spor kan være flere, eksempelvis;

- betaling: transaksjoner kobles til bankkonto og må kunne etterprøves
- bokføring: en tjeneste koster avhengig av omfang og type bruk
- autentisering: behov for å identifisere bruken
- aksess kontroll: behov for a kontrollere tilgang til spesielle funksjoner,
- en ”side effekt” av hvordan teknologien fungerer, etc.

Eksempler på teknologier i den siste gruppen inkluderer: Digital Rights Management (DRM) teknologi, elektroniske betalingstjenester, ”bomringteknologi” etc. Teknologi som i utgangspunktet ikke er laget primært for å samle in elektroniske spor kan selvfølgelig brukes for det formålet hvis sporene lagres og ikke slettes slik de burde.

En annen distinksjon mellom ulike teknologier er om de genererer elektroniske spor som dokumenterer hendelser i den elektroniske verden (f. eks. pakkesniffers og DRM) eller de som anvendes for å fange opp hendelser i den fysiske verden (f. eks. videoovervåkning og RFID).

Lagring av digitale spor
Det er viktig å ta hensyn til at når et digitalt elektronisk spor en gang har vært lagret sentralt er det vanskelig å få det slettet og det er enda vanskeligere å vite med sikkerhet at det virkelig er slettet. Dette skyldes at det i mange tilfeller ikke finnes noen full oversikt over alle kopiene som automatisk genereres av et elektronisk spor. Virksomheten som først samlet inn det elektroniske sporet har ofte flere kopier på ulike filer og databaser, på forskjellige disker, backup-taper og det elektroniske sporet kan ha blitt overført til andre virksomheter.

I det følgende presenters noen utvalgte teknologier.

5.1 Talekommunikasjon

All elektronisk kommunikasjon er i seg selv elektroniske spor (trafikkdata og innholdsdata) som kan lagres. Hvis ikke kommunikasjonen er kryptert så er det mulig for alle direkte involverte aktører å fange den opp mellom sender og mottager. Kommunikasjonen passerer ofte gjennom mange nettverk som kontrolleres av forskjellig operatører.

Tele og datakommunikasjon er organisert i funksjonelle lag. Elektroniske spor kan samles inn fra alle disse lagene og det relativt uanhengig av hverandre. Det samme gjelder datasystemer generelt – hardware, operativsystem, databaser, applikasjoner. Informasjonsinnholdet øker høyere opp i lagene.

5.1.1 Fasttelefoninettet

Med dette mens det "gamle" telenettet som har gjennomgått en evolusjon fra å være helt analogt i 1986 til å være 100 % digitalt ca 1997. Dette er en fundamental endring i en kritisk samfunns infrastruktur som har skjedd på relativt kort tid. I og med at de fleste typer telefoni fortsatt eksisterer er det hensiktsmessig å se på disse under ett.

Beskr / Type	Periode	Telefon sentral	Abonnement	Lagring av trafikkdata	Lagring av innhold	Takster
Analog	- 1956	Operatør	Fast pris	Nei	Nei	Lokal, Riks, Utland
Analog	Ca 1950 – ca 1975	Elektro-mekanisk	Fast pris + hele tellerskritt (eks á 3 min.)	Bare antall påbegynte tellerskritt	Ved fysisk tilkobling	Lokal, Riks, Utland
Analog	1986 mar -	Digital	Fast pris + pris per min. (og etter hvert; sek.)	Samtale start og stopp tid, A-nr + B-nr (tape, disk)	Ved aktivering i sentral	Lokal, Riks I, Riks II, Utland
ISDN	1990 jan -	Digital	Fast pris + pris per sek.	Samtale start og stopp tid , A-nr + B-nr (tape, disk)	Ved aktivering i sentral	Variable
xDSL	2003 -	Digital	Fast pris er vanlig	Antatt: status på forbindelsen	Usikket	Ikke vanlig

Trafikkdata
Hvis en ser på utviklingen over de siste 20 år har det skjedd en utvikling hvor infrastrukturen er blitt mer "intelligent". Det vil si; den husker primært mye mer over lengere tid og kan bearbeide den informasjonen som ligger der. Et eksempel på dette er "Familie og venner" tjenester som gir rabatterte samtaler til et antall forhåndsdefinerte abonnenter. Dette fungerer fordi operatøren lagrer hvem du tror du kommer til å ringe mye til og bruker dette for å gi rabatter basert på de trafikkdata som samles inn.

Trafikkdata lagres for å beregne den betaling tjenesteleverandøren skal ha for de tjenester som er brukt iht. de avtaler som er gjeldene. Når betaling er gjennomført er det ikke lenger behov for opplysningene om trafikkdata og disse skal slettes i henhold til angitte friste, normalt 3 til 5 måneder.

Den type trafikkdata som normalt lagres i en moderne telefonsentral er: tidspunkt for start og slutt av samtalen, hvilket nr. det blir ringt fra (A-nr) og hvilket nr. det blir ringt til (B-nr). Denne informasjonen vil så videreformidles til et drifts og regnskapssystem.

Innholdsdata / avlytting
Lagring av innholdsdata, dvs. telefonavlytting, er noe som normalt ikke gjøres. Dette er ikke et sentralt tema i denne rapproten, men nevnes da dette er en kjent problemstilling for telefoni. Hvis innholdsdata lagres så skal det være etter en rettslig kjennelse, men det også en konsekvens at en slik kjennelse må kunne effektueres av en operatør. Altså, det er en ringvirkning av denne praksis at alle telefonisystemer har innebygd funksjonalitet for avlytting. Denne funksjonaliteten kan normalt aktiveres for alle kunder fra en sentral driftssentral uten ekstra fysisk tilkobling spesielt til kundens telefonlinje. Det blir da viktig at de som utvikler, produserer og bruker systemet gjør det korrekt iht. regelverket og at dette kontrolleres på forsvarlig måte.

5.1.2 Mobil telefoni

	Periode	Telefon sentral	Abonnement	Lagring av trafikkdata	Lagring av innhold	Lagring av lokasjon
Analog (NMT)	198x –	Analog / Digital	Fast pris + pris per min. (og etter hvert; sek.)	Samtale start og stopp tid, A-nr + B-nr	Ved tilkobling	Basestasjon, Tel nr.
Digital (GSM)	Ca 1992 -	Digital	Fast pris + pris per sek.	Som over	Ved aktivering i sentral	Lokasjons omr., Cell, IMEI, CCID, Tel. nr.
Digital (3G / UMTS)	2004 -	Digital	Fast pris + pris per sek.	Som over	Ved aktivering i sentral	Lokasjons omr., Cell, IMEI, CCID, Tel. nr.

IMEI - unique International Mobile Equipment Identity number; serienummer på telefonen
ICCID - Integrated Circuit Card ID; serienummer på SIM brikken på 19 eller 20 siffer
SIM - Subscriber Identity Module; smartkort som inneholder abonnentens "brukerprofil"

Cell - Dekningsområde for en "radiosender" i basestasjonen. Disse grupperes til lokasjons områder på ca 50 celler.

Trafikkdata.
Utviklingen av mobiltelefoni har siden 80-tallet vært ganske lik som for fasttelefoni. Kapasiteten i infrastrukturen til å lagre informasjon har økt slik at det kan lagres elektroniske spor med mer presisjon og eventuelt over lengre tid. Den type trafikkdata som normalt lagres i en telefonsentral for mobiltelefoni er tilsvarende som for fasttelefoni: tidspunkt for start og slutt av samtalen, hvilket nr. det blir ringt fra (A-nr) og hvilket nr. det blir ringt til (B-nr). Denne informasjonen vil også videreformidles til et sentralt drifts og regnskapssystem. Som for fasttelefoni skal disse data slettes i henhold til angitte friste, normalt 3 til 5 måneder.

Lokasjonsdata
Den viktigste forskjellen vedrørende elektroniske spor er at det i mobilnettet lagres informasjon om *hvor* mobiltelefonen befinner seg. For å opprette en samtale med en mobiltelefon må den ha en trådløs "radioforbindelse" til en sender/mottaker som kalles en basestasjon. Over denne forbindelsen vil det opprettes datakommunikasjon som formidler trafikkdata og taledata. For dagens GSM-nett vil basestasjonen motta informasjon om serienummer på telefonens SIM kort (ICCID), telefon nummeret etc. og bruke dette for å kontrollere at telefonen er i bruk av en betalende abonnent. Basestasjonen vil be om oppkobling av en taleforbindelse for innholdsdata til en sentral som videreformidler denne når en ringer.

Basert på signalstyrken fra basestasjonene vil mobiltelefonen vurdere om den valgte basestasjon er egnet til å fortsette å fungere som "radiostasjon" for telefonen eller om den bør be om å bytte til ane annen celle. Hvis telefonen beveger seg vekk fra stasjonen, f.eks. i en bil, er den til slutt utenfor rekkevidde og en annen celle/basestasjon vil måtte overta. Mobiltelefonen vil da be om overføring til en ny celle og når en ny basestasjon overtar vil denne på nytt samle inn elektroniske spor fra telefonen. Nettverket lagrer til enhver tid hvilken celle en telefon er "aktiv" i og spør aktivt etter telefonen ("pager") hvis det ikke har vært noen endringer de siste (6) timer.

I det en telefon skrues av eller overføres til en annen celle vil normalt informasjon om oppkoblingen slettes fra basestasjonen. Telefonsentralen vil normalt lagre informasjon om hvilket lokasjonsområde (bestående av ca 50 celler) der telefonen sist var aktiv. Årsaken til denne løsningen antas å være blant annet at det skal gå raskere å få kontakt med nettet igjen hvis forbindelsen med basestasjonen faller bort i en kortere periode.

Alt dette betyr at datasystemene til en mobiloperatør har følgende elektronisk spor når en har skrudd på mobiltelefonen:

- Hvilken telefon du bruker (for eksempel din egen, en du har lånt eller stjålet)
- Hvilken SIM brikke du bruker (for eksempel din egen eller en som er lånt fra jobben)
- Hvilket mobilnummer SIM brikken har blitt tildelt
- Hvilken celle du befinner deg i

Størrelsen på en celle er variabel, men ettersom det er flere og kort mellom basestasjoner i byene antas det å kunne gi en presisjon på 2-300m. Utenfor byene vil en celle kanskje gi 3-4 km presisjon eller mindre.

Lokasjonsdata kan brukes aktivt for å lage nye tjenester. Et eksempel på dette er såkalte ”buddy” tjenester. Se for øvrig kap. 5.4.2.

I tillegg til trafikk og lokasjonsdata lagrer mobilnettet informasjon om ditt abonnement. Dvs. hvilke tjenester/funksjoner du abonnerer på ut over taletjenesten. Dette kan være tjenester for talepostkasse, viderekobling, dataoverføring, etc. og nettverket vil avvise forespørsler til tjenester som ikke er betalt for.

5.2 Datakommunikasjon og datanettverk

Med datakommunikasjon menes en kommunikasjonsforbindelse for overføring av digitale data mellom to enheter, for eksempel overføring av en datafil over en telefonlinje mellom to modem. Med datanettverk menes sammenkobling av flere forbindelser for datakommunikasjon. Et datanettverk gir mulighet for logisk tilkobling til ett eller flere andre datasystemer i det samme nettverket. En bruker har ofte bare (fysisk) kontroll over den kommunikasjonsforbindelsen som er tilkoblet ens eget utstyr. Brukeren av et utstyr har dermed varierende kontroll med hvilke andre enheter som er koblet til nettverket en kommuniserer med. I et ”hjemmenettverk” kan en ha god kontroll mens en på Internett ikke har noen kontroll med nettverket selv. Dette medfører at en bruker selv har høyst varierende grad av kontroll over hvor og hvordan elektroniske spor behandles og lagres i datanettverk.

5.2.1 Aksessteknologi for datakommunikasjon

For å koble seg til et nettverk trenger utstyret en fysisk og logisk forbindelse som forbinder det med et ”aksesspunkt” i nettverket, når flere aksesspunkter av samme type kobles sammen omtales dette ofte som et aksessnett. I de fleste tilfeller bruker datamaskiner en egen fysisk enhet, et modem (modulator – demodulator) for oppkobling til et aksesspunkt over en telelinje, tv-kabel eller lignende. Informasjonen som overføres over en forbindelse vil normalt ikke lagres i modemet da dette ikke er beregnet for lagring, men overføring av data. Rent teknisk er det selvsagt mulig å kopiere all informasjonen som overføres til et sted der den lagres, men det antas at dette ikke forekommer da det må kunne sidestilles med telefonavlyttning.

Det brukes mange ulike typer teknologier for tilkobling til aksesspunkter og her nevnes noen av de mest brukte.

Oppringt Modem

Dette er en analog punkt til punkt forbindelse til et annet modem, en sentral eller en server. Modemet kobler opp og oppretter dataforbindelsen som datamaskinen kan bruke. Typisk er dette en dataforbindelse til en ISP tjeneste som gir mulighet til å koble videre til Internett. Den informasjon som lagers er tilsvarende trafikkdata som for de senere års analog fasttelefoni, se kap 5.1.1. I tillegg vil aksess til en ISP tjeneste normalt medføre lagring av noe informasjon, se kap 5.2.3.

Data over ISDN

Dette er tilsvarende som over, men modemet overfører data digitalt, noe som gir mulighet for noe høyere overføringskapasitet enn for analoge modem, typisk opp til 122 kb/s.

xDSL

Denne betegnelse brukes oftest for å dekke SHDSL og ADSL. Begge disse er punkt til punkt forbindelser som brukes for å koble til et annet modem og da gjerne over en kabel som allerede

brukes til et annet formål som telefoni eller kabel-tv. Disse modemene er "høyhastighets" digitale modem som typisk gir overføringskapasitet på 1-10 Mb/s og brukes ofte for oppkobling til Internett. Hos noen leverandører vil også her tidsforbruket av ISP tjenesten lagres for faktureringsformål. Normalt er dette ikke nødvendig ettersom tjenesten ikke prises etter bruk, men har fast pris.

5.2.2 Telekommunikasjon - stamnett

Som for aksessnettet, beskrevet tidligere, er stamnettet etablert ved bruk av flere ulike teknologier. Stamnettets oppgave er å knytte aksessnettene sammen. Sammenkoplingen av aksessnettene gjennom stamnettet gjør at alle abonnenter til en hvilken som helst operatør, uavhengig av teknologisk aksessløsning, kan komme i kontakt med en hvilken som helst annen abonnent uavhengig av geografi. Hovedsakelig består stamnettet i Norge av fiber som fysisk medium, på grunn av topologiske forhold er det benyttet radiolinje på flere steder. Coax-kabel, som tidligere var hovedkomponenten, og som det fremdeles finnes en del av, er i stor grad byttet ut med fiberoptisk kabel.

Stamnettets fysiske oppbygging er helt nøytralt i forhold til elektroniske spor. Elektroniske spor oppstår i intelligente stamnettfunksjoner som styrer og overvåker overføringen av informasjon mellom aksessnettene og abonnentene. Hvilken informasjon som lagres i stamnettfunksjonene med hensyn til abonnentene vil altså variere. Spesielt kan abonnentens såkalte CoS (class of service), hvilke tjenester og sikkerhet som er avtalt med operatøren, være avgjørende.

5.2.3 Internett – åpent IP nettverk

Det som normalt omtales som Internett er det globale og åpne nettverket basert på IP protokollen spesifisert i IETF standarden "Internet protocol"[11]. IP protokollen binder ulike dataforbindelser og nettverk sammen og oppretter en ende til ende forbindelse mellom to av enhetene/datamaskinene i nettverket. Protokollen ruter eller styrer data gjennom nettverkene som "datapakker" som mellomlagres i koblingspunktene ("nodene") i nettet. Normalt vil alle datapakker slettes så snart de er videreformidlet, men de vil til en viss grad "bufres" i utstyret som kommuniserer. Igjen er det selvsagt teknisk mulig å lage utstyr koblet til Internett som kopierer den mellomlagrede informasjonen og lagrer den mer permanent. I hvilken grad dette gjøres er ikke lett å anslå, men rent teknisk kan det ikke utelukkes. Internett er basis for et utall datatjenester som alle genererer elektroniske spor. Hvis ikke trafikken er beskyttet spesielt (kryptert) mellom klient og server kan, som nevnt over, mye av den informasjonen som lagres på server siden også bli lagret av mellomledd, for eksempel ISPer. Selv om muligheten er der, er det lite trolig at akkurat lagring av IP trafikk skjer i særlig grad.

Ved tilkobling til åpent internett via en ISP kreves normalt kontroll av bruker-id og passord som lagres hos tjenesteleverandøren. Bruken av en bruker-id vil normalt også lagres i en viss periode.

5.2.4 Kablet og trådløst *lokalt* nettverk (LAN og WLAN)

Lokale nettverk (LAN) basert på tradisjonell bruk av kabler er normalt sikret mot innsyn og lekkasje av elektroniske spor ved fysisk sikring av lokalene der kabelen er lagt. Dette gir god sikkerhet så lenge en har oversikt over kablingen, det vil si kompleksiteten er liten eller dokumentasjonen er god. For privat bruk i hjemmet vil dette normalt fungere uten problemer.

[11] Internt protocol, http://www.ietf.org/rfc/rfc0791.txt

Trådløse lokale nettverk (WLAN) har derimot et en sårbarhet som kan gi svært dårlig kontroll med elektroniske spor. Problemet ligger i at mange ikke vet at de må beskytte sin trådløse kommunikasjon mot innsyn og ofte kreves en aktiv konfigurasjon av utstyret for at det skal sikres. Hvis et WLAN ikke har noen sikkerhetsmekanismer aktivert kan dette sammenlignes med å legge fysisk nettverkskabler inn hos alle naboene dine, legge ut 4-5 kabler til nærmeste gatehjørne og til slutt reklamere for det hele med plakater på alle lyktestolpene i nabolaget. Som et apropos kan det nevnes at en undersøkelse [12] antyder at opp mot halvparten av alle trådløse rutere som settes opp i norske hjem ikke har noen sikkerhetsmekanismer aktivert.

Et ubeskyttet WLAN vil i seg selv ikke generere elektroniske spor, men det er en reell trussel fordi andre med tvilsom motivasjon kan bruke et WLAN for å generere spor som tilsynelatende kommer fra en bestemt husstand (og dermed en eller noen få personer), men slett ikke gjør det. Det gjør det selvsagt også enklere med datainnbrudd og lekkasje av elektroniske spor fra PCene på hjemmenettet når en får fri tilgang til nettverket.

5.2.5 Personlige data nettverk

Ny teknologi går i retning av stadig mer sammenkobling av ulike typer personlig og mobilt utstyr. Dette resulterer i at vi får nettverk som vi "tar med oss". Eksempel på dette er kopling mellom mobiltelefon og en bluetooth "øreprope" og mellom mobiltelefonen og en bærbar PC. På dette området er det grunn til bekymring for en utvikling der fleksibilitet settes så mye foran sikkerhet at disse løsningene ikke får praktiske tiltak som skjermer godt mot innsyn. Igjen, dette er primært ikke teknologi som generer elektroniske spor, men teknologi som er sårbar for innbrudd og lekkasje av eksisterende elektroniske spor.

5.2.6 Annen trådløskommunikasjon

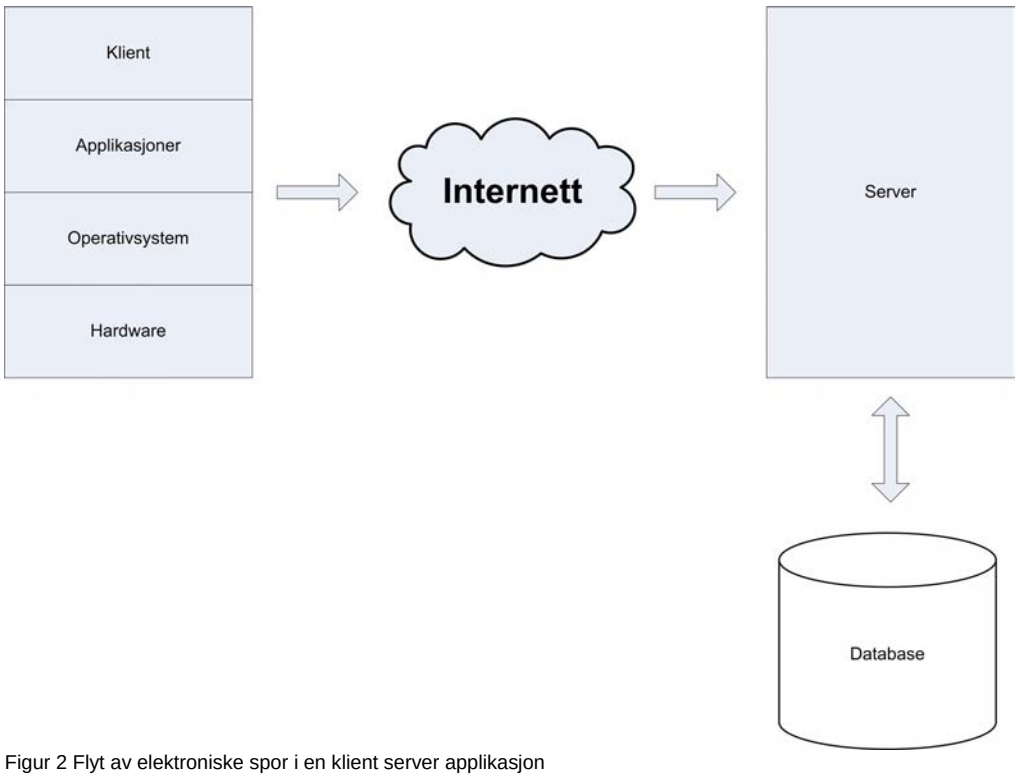
Mobiltelefoner tilbyr ulike tjenester for trådløs kommunikasjon. Det er primært fire typer teknologi som tilbys:

1) SMS meldinger: disse mellomlagres i mobilnettet og slettes etter noe tid. For disse lagres sender, mottaker, innhold og tidspunkt.
2) Mobil data: tilbyr overføring av data, for eksempel en modemfunksjon til en PC.
3) Wap: forenkelt web format for mobil telefoner. Elektroniske spor oppstår på tilsvarende måte som for vanlige web tjenester, se kap 5.3.1.
4) Web: full http støtte i mobiltelefonen. Se kap 5.3.1.

5.3 Internett tjenester

Å surfe websider er sammen med **e-post** de tjenestene på internett som er mest anvendt. De tjenestene som beskrives her vil normalt måtte basere seg på en av de kommunikasjonstjenestene som er beskrevet i kap. 5.1 og 5.2 og dermed vil bruk av en tjeneste etterlate spor på *både* kommunikasjons og tjenestenivå.

[12] Lever farlig i trådløst nett, Aftenposten, 4.april 2005, http://www.aftenposten.no/nyheter/nett/article1008438.ece



Figur 2 Flyt av elektroniske spor i en klient server applikasjon

Det er i denne sammenhengen viktig at tenke på at all informasjon som fylles inn i rubrikker/skjema på websider og "sendes" til en webserver faktisk går gjennom flere delsystemer hvor den behandles og potensielt lagres før den mottas av selve tjenesten der dataene behandles og potentielt lagres. Disse delsystemene inkluderer: Applikasjonene selv, operativsystemet – som kan sikkerhetskopiere filer, kommunikasjonssystemet – som mellomlagrer data og maskinvare som kopierer data for "cashing".

Cookies

HTTP som er protokollen som brukes for å hente websider fra en webserver er en tilstandsløs protokoll. Det innebærer at det ikke finnes noen mekanisme i HTTP som gjører at det går å koble to websideforespørsler til hverandre. Informasjonskapsler ("cookies") løser dette problemet gjennom å lagre informasjon på klient siden. Første gangen man henter en webside fra en web server lagrer den ofte en informasjonskapsel på klient siden (i brukerens PC). Når klienter senere laster ned websider fra webervern sender den med informasjonskapselen og webserveren har mulighet å sende tilbake en oppdatert informasjonskapsel.

Praktisk så brukes informasjonskapsler typisk for å sørge for at brukere bare trenger å logge in en gang og ikke en gang for hver webside de henter ned fra websiden eller for å spare brukeres innstilninger til en webtjeneste.

Informasjonskapsler kan også brukes med formålet å spore brukere og lagre informasjon om hvordan hver enkelt bruker et websted. Problemet med IP adresser for sporingsformål er at de kan endres. Når en brukere kobler seg på Internett er det ikke sikkert at han får samme IP adresse som forrige gang han logger på (dynamiske IP adresser). Brukeren kan også sitte bak en brannmur som gir all utgående samme avsender adresse (Network Address Translation eller NAT).

Web Proxy, Web Filter
Ettersom det krever mer og mer båndbredde å betjene brukere med internett tilgang er det for mange (større) bedrifter besparende med tiltak som reduserer behovet for båndbredde på eksterne kommunikasjonslinjer. Det en kan gjøre er å følge det samme prinsippet som for RAM cashing i PCer, men nå tilpasset lasting av informasjon fra Internett. Det vil si, man introduserer en mellomliggende tjener på vei ut av bedriften og ”bufrer” opp de websidene som brukerne laster ned. Dette betyr at neste gang den samme siden lastes ned av en (annen) bruker vil denne overføres fra ”proxyen” lokalt og ikke fra den reelle webtjenesten. Over tid vil det bygges opp statistikk over hvilke websider som leses ofte og disse vil lagres i Proxyen. Med relativt beskjedne midler og en god strategi for bufring vil en kunne redusere ekstern trafikk ut av bedriften med 70-80%. Dette gjør at en kan betale for atskillig mindre båndbredde enn uten en proxy.

Dette har også en opplagt ulempe knyttet til elektroniske spor. Per definisjon vil en slik proxy inneholde nesten all informasjon om hvilke maskiner, representert ved IP adresser, som laster ned hvilke websider. Altså vil en proxy kunne inneholde en mengde informasjon som kan brukes til å overvåke de ansattes bruk av webtjenester, kanskje også uten at de er direkte klar over at dette foregår.

Et web filter vil har mye av samme funksjonaliteten, men denne innholder regler og ”signaturer” på webtjenester som brukere ikke skal få tilgang til. Så i stedet for å formidle bufrede sider vil et web filter blokkere nedlasting av uønskede websider. Dette kan for eksempel være sider for spill, gambling eller pornografisk materiale. Igjen betyr dette at en slik funksjonalitet innholder spor fra brukerne vedrørende deres bruk av webtjenester.

Brannmurer
Fordi en tilknytning til internett i utgangspunktet åpner for at svært mange applikasjoner i en datamaskin skal kunne nås, også fra Internett, er det nødvendig å begrense aksess fra eksterne maskiner til et minimum. Det er normalt bare et fåtall applikasjoner som skal kunne nås fra det åpne Internettet og en brannmur har regler for kommunikasjonen mellom maskiner. Normalt gjøres dette basert på at en applikasjon må oppgi en ”port” for å informere om hvilken applikasjonsprotokoll den vil benytte. Brannmuren håndhever dermed regler for hvilke IP adresser som kan benytte hvilke porter både for inngående og utgående kommunikasjon. Fordi svært mye av trafikkdataene logges, og som et minimum alle brudd på reglene, vil en brannmur også inneholde svært mange elektroniske spor. Et felles trekk ved proxyer, filtre og brannmurer er at det er opp til bedriftens interne prosedyrer å sørge for at informasjon/spor de har lagret ikke blir misbrukt.

5.3.1 World Wide Web tjenester

Hver gang en bruker laster ned en webside kommuniserer brukerens nettleser eller ”browser” (f. eks. Internet Explorer) med en webserver. En websideforespørsel innholder informasjon om brukerens IP adresse, nettleser og adressen til den side som brukeren sist besøkte. Normalt vil denne informasjonen lagres på webserveren som underlag for statistikk over hvilke IP-adresser og områder (domener) som besøker tjenesten.

Internett søk er et eksempel på en nyttig tjeneste på internett. Potentielt kan disse søkemotorene skape brukerprofiler gjennom å koble de søkebegrepene som brukes til den IP-adresse og den cookie som browsern har for søketjenesten. Disse brukerprofilene kan være

ganske personlige og sensitive ettersom det en søker etter på internett sier en god del om en slev som person. Følgende er et utdrag ur Googles personverns policy[13] (04.05.2005):

"Når du besøk Google første gang, sender Google en informasjonskapsel ("cookie") til datamaskinen din. En informasjonskapsel en datafil som identifiserer deg som en unik bruker. Google bruker informasjonskapsler til å forbedre kvaliteten på tjenesten, og til å forstå brukergrunnlaget bedre. Dette gjør Google ved å lagre brukerinnstillinger i informasjonskapsler og å spore brukertrender og mønstre for hvordan personer søker."
"Google samler ikke inn unik informasjon om deg (for eksempel navnet ditt, e-postadressen og så videre) bortsett fra når du spesifikt og vitende oppgir slik informasjon. Google noterer og lagrer informasjon om tidspunktet, weblesertypen, weblesерspråket og IP-adressen ved hvert søk. Denne informasjonen brukes til å kontrollere våre rapporter og for å kunne tilby mer relevante tjenester til brukerne. Google kan for eksempel bruke IP-adressen eller weblesерspråket til å fastslå hvilket språk som skal brukes til å vise søkeresultater eller annonser."
"Google kan velge å vise søkeresultatene i form av viderekoblinger av webadresser. Når Google bruker en viderekobling av en webadresse, sendes informasjon om klikket til Google hvis du klikker en webadresse fra et søkeresultat, og Google sender deg deretter til webområdet du klikket. Google bruker denne webadresseinformasjonen til å forstå og forbedre kvaliteten til Googles søketeknologi. Google bruker for eksempel denne informasjonen til å finne ut hvor ofte brukerne er tilfreds med det første søkeresultatet, og hvor ofte de går videre til andre resultater."

Sett fra tjenesteleverandørens ståsted er dette kanskje ikke en urimelig policy, det tar vi ikke standpunkt til her, men - det er betimelig å stille spørsmål ved i hvilken grad brukerne faktisk er inneforstått med (1) hvor mye informasjon som samles inn om den enkelte og (2) i hvilken grad brukeren har og forstår sin kontroll over denne informasjonen.

Hjemmebank
Hjemmebank er en av de mest utbredte web tjenestene per i dag. Dette resulterer i at det ligger spor om det aller meste av den enkeltes banktransaksjoner, ikke bare hos banken, men også elektronisk på ens egen PC. Det er her ikke eksistensen av sporene (som bankene er pålagt å ha) som er problemet, men antall kopier og kontrollen på disse.

Chatrooms
Dette er en populær type webtjenester hvor brukerne tilbys en "oppslagstavle" eller et "chatroom" der brukere "melder seg på" og deretter kan sende tekstmeldinger som med en gang vises på tavla til alle i rommet. Dette gjør det mulig å "skravle" relativt "anonymt" og uforpliktende med andre. Det er ofte ikke noen form for autentisering til disse tjenestene – en kan fritt velge sin identitet – dette omtales som et nickname eller "nick".

Pengespill / Gambling
I Norge er antagelig (antagelig) bare Norsk Tipping og Rikstotto som har lisenes til å drive pengespill på Internett. Det er i utgangspunktet ikke tillatt innenfor lotteriloven å tilby denne form for tjenester uten spesiell tillatelse og for nettbaserte pengespill er det gitt dispensasjon til begrenset drift for disse aktørene. Disse tjenestene er pålagt å lagre alle transaksjoner og spill sentralt. I prinsippet genererer all aktivitet på en slik tjeneste elektroniske spor som lagres sentralt. Dette er tilsvarende som for "registrerte spillere" tidligere og det føres tilsyn med

[13] http://www.google.no/privacy.html

driften fra Lotteritilsynet. Alle brukere må være norske statsborgere og gevinster utbetales til norske bankkonto.

Internett "scanning" / arkivering
Nasjonalbiblioteket har lovlig rett til å arkivere alle "publikasjoner", antagelig også de som er websider. Dette betyr at mange websider i Norge i utgangspunktet etterlater elektroniske spor som aldri slettes. Hva som omfattes av dette og hvem som har tilgang til informasjonen bør undersøke nærmere.

Andre tjenester også i utlandet, er spesielt laget for å kunne finne tilbake til tidligere versjoner av websider. Disse tjenestene kan selvsagt ikke lagre all informasjon fra alle websider, men de lagrer svært mye og om "nesten alle" tjenester. Ved søk på et webdomene kan en få en historisk oversikt over tidspunkt websidene er kopiert på og deretter se på det som er lagret. Altså er det ikke slik at noe som er publisert og slettet fra en tjeneste på Internett forsvinner, det kan ligge elektroniske kopier lagret "for evig og alltid" på mange andre tjenester rundt om i verden. Se for eksempel tjenesten på "archive.org". [14]

Web-mail
Det er etter hvert mange som bruker webbaserte tjenester til e-post, såkalt "webmail". Hotmail er den mest kjente, men også Yahoo og andre har et stort antall brukere, og de fleste ISPer tilbyr sin egen løsning for webmail til sine kunder. Googles "Gmail" tjeneste har fått ekstra oppmerksomhet i forhold til personvern. Mange av bekymringene gjelder antagelig alle webmail tjenester, men disse er gjort ekstra synlig av Gmail fordi en del av deres tjenestetilbud tydelig illustrerer hvilke muligheter en slik e-postleverandør faktisk har.

Det er opplagt at operatøren, som med tradisjonelle e-posttjenere, har tilgang til e-posten som er lagret. Til forskjell fra POP-servere ligger ikke bare innkommende post på leverandørens maskin, men også all annen arkivert e-post som ikke er eksplisitt slettet eller flyttet ut av tjenesten. Dette gjelder forøvrig også tradisjonelle e-posttjenere som bruker IMAP protokollen.

Gmail
Et særtrekk ved Gmail er at den viser tilpasset reklame basert på nøkkelord i innholdet i den enkelte e-posten du leser. Det blir dermed synlig og opplagt for brukerne at tjenesten faktisk "åpner" e-posten og prosesserer innholdet i den. Det kan også se ut som om tjenesten lager profiler av brukerne og dette er kanskje hovedårsaken til mye av oppmerksomheten tjenesten har fått. I følge Gmail selv er annonseutvalget basert på nøkkelord i den enkelte e-post som vises og ikke på noen profil, og de sender ikke fra seg noe informasjon om brukerne til annonsørene. Allikevel, en e-post om helgens sykkeltur i marka kan gi deg reklame om terrengsykler. Stemmer det at informasjon om brukere ikke sendes til andre kan en kanskje si at annonsørmatchingen teknisk sett ikke særlig annerledes enn at tjenesten også sjekker e-post for virus og spam, slik så å si alle webmail systemer og de fleste andre e-postoperatører gjør. Et annet særtrekk er at Gmail tilbyr rask søking i e-post som et sentralt element og legger opp til å bruke det fremfor å bla i lister og hierarkier. Det blir dermed tydelig at e-posten er søkeindeksert og at det er lett å finne fram i den. Teknisk sett er det ingen vesentlig forskjell i sporbarhet: alle store webmail leverandører tilbyr søking i e-post selv om det er plassert mindre sentralt grensesnittet.

[14] Archive.org, http://www.archive.org/

En reell forskjell med Gmail er den store lagringsplassen, tjenestedesignet og brukerinstruksjonene oppfordrer brukeren til å ikke slette e-post når den er lest, men bare arkivere den. Å fjerne en melding helt krever en eksplisitt handling utover typisk daglig bruk. Nytteaspektet ved å ha gammel e-post tilgjengelig uten å være i veien, koblet med kraftige søkemuligheter gjør at mange brukere følger dette mønsteret. Det resulterer i at en mye større mengde korrespondanse ligger lagret og søkbart enn det som har vært typisk hos andre webmail leverandører. På dette området følger imidlertid mange andre tilbydere etter og tilbyr større lagringskvoter slik at samme bruksmønster og massiv lagring blir mulig også der. Hos noen av dem gjør grensesnittet det litt lettere og mer naturlig å slette lest post, men man må regne med at mange brukere uansett ikke "rydder" før det er fullt.

Webmail åpner for utvidet mulighet for søking og "scanning" av e-post og dermed en mer tvilsom bruk eller mulig misbruk av innholdet i e-post. I hvilken grad dette faktiske skjer eller ikke tar vi ikke stilling til, det bare påpekes at de tekniske løsningene legger til rette for en noe annen bruk enn ved tradisjonell e-post med POP tjenere. Webmail går som andre webtjenester over det åpne og globale Internett og er regulert av de lokale lover i det landet operatøren drifter sin tjeneste. I tillegg vil operatøren normalt ha en selvregulering gjennom sin "Privacy Policy", for Gmail se [15]. Det anbefales å lese - og forstå - det denne type tjenester publiserer vedrørende personverns policy.

En vurdering av i hvilken grad disse policyene er gode eller dårlige, tilpasset norsk lovgivning eller hvordan de etterleves av operatørene vil igjen kreve betydelige undersøkelser som ikke er mulig å inkludere her. Det viktige er å være klar over at det kan være forskjell på sentrale områder i forhold til personvern mellom webmail og den e-post tjenesten din arbeidsgiver tilbyr.

5.3.2 E-post

I utgangspunktet så lagres og arkiveres alle meldinger i sin helhet av den e-post tjenesten sender og mottaker er tilknyttet og blir et elektronisk spor. Ettersom sender og mottaker bør har en viss kunnskap om og tillit til sine tjenesteleverandører er dette kanskje ikke det viktigste problemet med e-post. Likevel, slik tillit kan endre seg over tid. Det at e-post lagres hos mottagers sentrale tjeneste medfører at hvis du sender og mottar privat e-post på jobben lagres også denne selv om den er privat. En ringvirkning er at e-post ofte kan finnes igjen på bedriftens e-posttjenere flere år etter det at du har sluttet i jobben og tillitsforholdet er et annet.

En større utfordring med e-post er antagelig de e-posttjenerne som ligger mellom sender og mottager og videreformidler posten; disse har ingen av partene direkte kontroll med og det er ikke mulig å vite hvilke servere som vil være involvert eller hva disse gjør med e-posten. Teknisk sett er det ikke noe problem å kopiere all e-post som formidles og all ubeskyttet e-post bør antas å gi ubegrenset innsyn for tredjepart.

Er en e-post først kopiert kan den scannes og lagres og i ettertid brukes til en rekke formål. Det som muligens har forhindret dette fra å skje i særlig omfang er kostnaden for lagringskapasitet. Når denne nå faller øker risikoen for lagring, scanning og tvilsom bruk av e-post hos tredje parter. Dette er likevel "gamle" problemstillinger knyttet til bruk av e-post. Det som gjør at disse problemstillingene nå bør vurderes i et annet lys er at e-post er i ferd med å gå fra å være

[15] http://gmail.google.com/gmail/help/privacy.html

formidling av "postkort" til å være en formidler av offisielle brev mellom bedrifter samt mellom myndigheter og innbyggerne. Det bør være innholdet som setter kravene til beskyttelse og ikke teknologien - selv om den er effektiv. Kravene til beskyttelse av (sensitiv) personinformasjon som sendes fra en etat via e-post er, og bør absolutt være, rimelig strenge. Likevel, hvordan dette skal løses i praksis er fortsatt et tema. En rekke anvendbare teknologier som Kvalifiserte Sertifikater, Digitale Signaturer, Tidsstempling og Notarius tjenester er tilgjengelig, men disse er ikke videre utbredt i Norge per i dag. e-Forvaltnings forskriften [16] er etablert, men om det er tatt i bruk gode rutiner og løsninger for å etterleve denne og annen lov/forskrift som regulerer det offentliges behandling av e-post og dokumenter i elektronisk form antas det å være grunnlag for å undersøke nærmere.

5.3.3 Betaling på internett

Det finnes et stort antall ulike betalingsinstrumenter som kan benyttes på Internett for å betale for produkter og tjenester. Det er ikke hensiktsmessig å lage en uttømmende liste så dette avsnittet er avgrenset de til de mest vanlige betalingsinstrumentene i Norge.

Kredittkort

Kredittoppgjøret skjer i to steg; brukersted (web butikken) – kreditor og kreditor – bruker. Både dialogen bruker til brukersted og brukersted til kreditor vil normalt etterlate elektroniske spor som inneholder all informasjon om selve kjøpet/varen. Kreditor lagrer det samme som for andre transaksjoner. Brukerstedet vil også normalt lagre all informasjon om kundens kredittkort (serie nr. og utløpsdato) elektronisk. Denne informasjonen er tilstekkelig til å kunne belaste kunden for varer som denne ikke har kjøpt, men i tilfelle vil ikke kunden betale umiddelbart ved eventuelt misbruk.

Debetkort

Direkte debet fra konto. Eks. VISA. Denne type transaksjoner skjer også i to faser, men brukerens konto belastes umiddelbart. Transaksjonene skjer mellom brukersted – brukerstedets bank og kundens bank. Informasjonen som lagres av brukersted er tilsvarende som for kredittkort, men behovet for å lagre det over tid er ikke det samme da oppgjøret skjer umiddelbart. Informasjonen som lagres av bankene er normalt avgrenset til et pengebeløp, et trans nr, en id for brukerstedet og en id for brukeren, men ikke noe om selve varen som er kjøpt.

"e-purse"

Med dette begrepet menes en sentralt lagret lommebok funksjon som en bruker mindre beløp fra ved kjøp av småvarer. Eksempler på slike løsninger er Telenor Mobil sin M-handels løsning SmartPay og Payex fra eSolutions Group. Felles for disse løsningene er at kunden oppretter en "konto" hos leverandøren og overfører penger (f.eks 500 kr) til denne og kan overvåke sin saldo. Når en betaler med en slik løsning vil e-purse leverandøren ta rollen til både brukerstedets og brukeren sin bank og på den måten vil informasjonen om et kjøp ikke fordeles til like mange aktører. På den annen side; disse løsningene leveres ikke av banker, men fra leverandører av betalingstjenester.

e-cash

Dette er en betegnelse for lokalt lagret elektroniske kontanter, normalt benyttes smartkort for å

[16] e-forvaltnings forskriften, http://www.lovdata.no/for/sf/mo/xo-20040625-0988.html,

ivareta sikkerheten i slike løsninger. Eks.: Norsk Tipping med Mondex e-cash og bankenes tester med Proton løsningen. For å overføre penger til ditt kort må du involvere din bank, men ikke nødvendigvis for å betale til en nettbutikk. I Mondex løsningen skjer overføring av elektroniske penger direkte mellom er forbrukers smartkort og butikkens smartkort uten at banken eller andre er involvert i det hele tatt. Dette gjør Mondex ganske likt kontanter i og med at disse pengene er "ihendehavers" og bare eksisterer i ett smartkort om gangen. Spor etter hvordan penger flyttes lagres bare hvis pengeoverføringen går feil. Proton vil normalt kreve interaksjon med med en tredje part for "clearing", i Norge BBS.

Uavhengig av e-cash teknologi vil ofte andre sikkerhetsmekanismer som generer spor bli brukt for å sikre "kontrakten" mellom bruker og nettbutikk. Disse etterlater i så fall spor vedrørende kjøpet i nettbutikken, men ikke nødvendigvis om selve betalingen eller identiteten til kunden.

5.3.4 Katalog og oppslagstjenester

Det finnes en del oppslagstjenester som ikke er webbaserte. Disse inkluderer åpne/gratis og betalbare katalogtjenester av ulike typer. Disse inneholder informasjon om organisasjoner eller personer og omtales ofte som et "directory". Den mest benyttede standarden for denne type tjenester er LDAP (Lightweight Directory Access Protocol), se også[17].

Kataloger er et viktig element for PKI og digitale signaturer. Brukerens digitale sertifikat må for åpne PKIer gjøres tilgjengelig for alle brukere for å muliggjøre verifikasjon. Dette innebærer at en må kunne søke å finne sertifikater og annen relevant informasjon om alle i katalogen. Dette er normalt ikke problematisk i forhold til den som har et sertifikat som letes opp i katalogen fordi det sjelden er særlig følsom informasjon i sertifikatene, men informasjon som e-postadresse forekommer ganske ofte.

Katalogoppslag er potensielt vanskeligere for den som skal verifisere brukeren. Ved å gjøre oppslag mot katalogen vil en mer eller mindre tilkjennegi hvem en er (ved IP adresse) og hvem en kommuniserer med ovenfor utstederen av sertifikatet (og eier av katalogen). Så lenge brukeren eller brukerstedet stoler helt og fult på at informasjon vedrørende oppslaget ikke lagres og misbrukes går alt bra. Problemet oppstår i det øyeblikk for eksempel en tjenesteleverandør skal bruke en ID leverandør en av forretningsmessige grunner slett ikke kan eller vil stole på.

En annen tilnærming til dette med oppslag til PKI kataloger er at sertifikatene absolutt ikke er åpen informasjon, men noe en skal vite hvem bruker og ta betalt for det. For dette formål er OCSP standarden passende og men denne løsningen vil alle oppslag normalt autentiseres, loggføres og avregnes iht en avtal mellom ID leverandøren og bruker(stedet). I dette tilfellet blir det enda viktigere å ha tillit til at ID leverandøren ikke misbruker disse elektroniske sporene.

5.3.5 Video distribusjon - streaming over IP

Såkalt "Video streaming" brukes for å distribuere levende bilder over IP. Dette kan være TV-sendinger live/opptak eller video på forespørsel (Video On Demand) type tjenester. Som brukerutstyr brukes en hjemme-PC med multimediemuligheter for å vise bildene. Med bredbåndsaksess med kapasitet over ca 1 Mbit/sek er det mulig å overføre TV bilder av brukbar kvalitet. Avhengig av overføringskapasiteten vil selvsagt kvaliteten på bildene variere, men

[17] RFC 2251, ftp://ftp.rfc-editor.org/in-notes/rfc2251.txt

generelt kan en si at 1 Mbit/sek er noe lite mens 10 Mbit/sek er svært bra. Dette betyr at med dagens bredbåndstjenester vil flere og flere ta i bruk denne type tjenester, kanskje spesielt for Video-on-demand type tjenester som videoleie, opplæring, repriser og lignende.

I utgangspunktet skulle en kanskje tro at en slik løsning fungerer på noenlunde samme måte som tradisjonell kringkastet TV. Det er imidlertid ikke tilfelle med tanke på elektroniske spor da "streaming" teknisk sett er like sporbart som alle andre webbaserte tjenester; dvs. oppkobling, pålogging, programvalg osv. etterlater elektroniske spor i sentrale tjenester som kanskje også skal brukes for faktureringsformål.

To typer data blir sendt over Internett: oppkoblingsdata/trafikkdata for forbindelsen (såkalt "kontroll protokoll") og innholdsdata som er kodet lyd og bildedata. Tjenesteleverandørene sitter altså på mye "sensitiv" informasjon og det er også her vanlig for operatørene å innføre selvregulering med hvordan de skal håndtere personlig informasjon med en "Privacy Policy". Sammenlignet med mottak av TV-signaler fra bakkenettet og satellittsendinger uten returkanal er det altså en betydelig forskjell; tradisjonell kringkastning gjør det selvsagt ikke mulig for sentraliserte tjenester å vite noe om dine programvalg eller når du ser på TV.

5.3.6 Bredbånds telefoni / Voice over IP

IP-Telefoni eller Voice over IP (VoIP) brukes for å gjennomføre telefonsamtaler via Internett. Med bredbåndsaksess (se kap. 5.2.1) er det nok båndbredde for overføring av tale tilgjengelig. Som brukerutstyr brukes også her en hjemme-PC med multimediemuligheter, eller spesielt utstyr levert av tjenestetilbyderen. Det tradisjonelle telefonapparatet og telefonkabelen blir erstattet med PC med programvare og Internett-tilgang. Løsninger som finnes i Norge er bl.a. Skype, Telio, Telenor Bredbåndstelefoni, NextPhone, Tele2, og lokale tilbydere (ofte strømleverandører). IP telefoni kan også brukes internt hos telefonselskaper, eller telefonselskaper seg imellom selv om brukeren har vanlig telefonapparat eller mobiltelefon. I slike tilfeller brukes IP telefoni uten at brukeren er klar over dette.

Teknisk sett blir to typer data sendt over Internett: oppkoblingsdata/trafikkdata for forbindelsen (såkalt "kontroll protokoll") og innholdsdata som er kodet lyddata. Nyttedata blir oftest overført via RTP protokollen over UDP, men det finnes også andre løsninger. Som kontrollprotokoll brukes for eksempel SIP, H.323, SCCP, H.248 og andre. Fellesnevneren for disse løsningene er at de bruker IP protokollen, og dermed IP adresser for sende nyttetrafikk.

Siden trafikken går over det åpne internett må applikasjonen selv ivaretar nødvendige sikkerhetsmekanismer. Tilbydere som Skype krypterer trafikken fra ende til ende, og er dermed rimelig avlyttingssikre. Andre tilbydere kan ha andre regler og løsninger for kryptering. Skype bruker en peer-to-peer løsning, som gir andre sikkerhetskarakteristika enn løsninger med sentrale tjenere. For administrasjons- og betalingsformål finnes det databaser hos tilbyderne som inkluderer lagring av samtalenes administrative data som for fasttelefoni (samtalepartnere, lengde, tidspunkt, mm.). Dette blir også delvis utvekslet på internett og kan bare delvis beskyttes.

I den utstrekning det er forskjeller mellom hvordan personlig informasjon håndteres for VoIP kontra tasttelefoni er muligheten for avlytting og personvernslovgivningen to viktige momenter. Fasttelefoni går over et rimelig godt beskyttet telenett i Norge og innsyn er regulert

av norske lover for avlytting og personopplysningsloven. VoIP går over det åpne og globale Internett og er regulert av de lokale lover i det landet operatøren drifter sin tjeneste. I tillegg vil operatøren normalt ha en selvregulering gjennom sin "Privacy Policy". En vurdering av i hvilken grad det ene er bedre enn det andre vil kreve betydelige undersøkelser som ikke er mulig å inkludere her, men det er viktig å være klar over at det er forskjeller på sentrale områder i forhold til personvern.

5.3.7 Diverse

Øyeblikksmeldinger / MSN Messenger
MSN Messenger er en populær tjeneste, hvor du kan chatte, dele dokument, sende filer, ha videokonferanse, bruke voice-over-IP etc. Du må bruke et Microsoft Passport for å logge på MSN Messenger tjenesten. Når du har logget in kan du søke etter medlemmer i MSN nettverket. Du kan legge in personer i din kontaktliste. Personer på din kontaktliste kan du overvåke gjennom at du ser om de er logget på og om de er borte (ikke har brukt tastaturet på en viss tid).

En legger til medlemmer til sin kontaktliste gjennom å oppgi deres e-postadresse. Den du legger til må godkjenne at du legger vedkommende inn (standard) men han/hun kan endre policy til at alle kan legge seg inn. Du kan også se hvem som har deg på sin kontaktliste. At du som brukere kan gjøre dette innebærer trolig at MSN må føre et register over hvem som er på hvems kontaktliste.

Det er også teknisk mulig for MSN å logge hvem som kommuniserer med hvem (trafikkdata). Selve kommunikasjonen (innholdsdata) kan gå direkte mellom dem som kommuniserer eller innom en sentral server. Se også MSNs personvernspolicy på nettet [18].

P2P nettverk
"Peer-to-peer" (P2P) nettverk er en spesiell type applikasjoner som gjør at man ved hjelp av en sentral koordinerende tjeneste kan dele ressurser mellom mange medlemmer i et nettverk. Et eksempel er Gnutilla. Den sentrale tjenesten er ikke involvert i overføring av innholdsdata mellom deltagerne i nettverket og har bare en koordinerende funksjon. Fordi innholdsdata kommuniseres direkte mellom likeverdige parter ("peers") kalles dette peer-to-peer nettverk. Fordelen med dette er at man kan dele en rekke ressurser som CPU-kraft, lagringsplass, (mp3)filer og andre data direkte mellom medlemmene uten at en sentralisert tjeneste er involvert. Medlemmene i nettverket er normalt kontinuerlig "påkoblet" P2P nettverket.

Dette skaper på den en siden frihet og reduserer behov for sentrale (og kostbare) tjenester som kan være flaskehalser. På den annen side har det en rekke sikkerhetsimplikasjoner ettersom en risikerer å ha lite innsyn og kontroll med hva denne type applikasjon virkelig foretar seg med de maskinene de er installert på. Det er også risiko for at en uvitende kan bli mottager av sensitivt eller ulovelig innhold. Denne type applikasjoner er også svært anvendbare for å distribuere "spyware" og programvare som benyttes i forbindelse med kriminell aktivitet. Altså er det grunn til å være forsiktig med hva slags P2P nettverk en deltar i fordi det er knyttet betydelig risiko til hvilken kontroll en selv har med hvilken informasjon og elektroniske spor som sendes fra ens egen maskin med denne type applikasjoner.

[18] MSN personvernspolicy, http://privacy.msn.no

5.4 Telefoni og andre tjenester

5.4.1 Telefoni og taletjenester

Vanlig oppringt telefoni mellom to abonnenter er fortsatt en viktig tjeneste. I de senere år har det kommet en rekke såkalte "tilleggstjenester". Disse kan generere elektroniske spor avhengig av hvilken tjeneste en bruker. Under er noen eksempler.

	Abonnement	Lagring av trafikkdata	Lagring av innhold
Viderekobling	Fastpris	Nei	Nei
Telefonsvar	Fastpris	Nei	Svaret
Telefonsvarer	Fastpris	A-nr (antatt)	Beskjeder

Et svar lagret elektronisk på en elektronisk og sentralisert telefonsvarer kan være "vi er på ferie og kommer hjem til høsten". Her påpekes det bare at muligheten for misbruk er tilstede.

5.4.2 Lokasjonsbaserte tjenester

"Buddy tjenester"

Denne type tjenester er basert på mobil telefoni og går ut på at det er mulig å registrere andre brukere ("buddies") som en gruppe nummer som kan spørre etter din lokasjon og så få vite hvor mobiltelefonen din befinner seg geografisk. Denne type tjenester er så langt basert på at registrering, spørring og svar skjer ved SMS meldinger. Hvis en spør etter en buddy vil en i praksis få vite hvilken celle eller lokasjonsområde i mobilnettet en telefon befinner seg i. Hver celle er gitt et stedsnavn som sier noe om det geografiske og avstanden mellom den som spør og svarer kan angis. Et tenkt svar kan være "Bjarne er på Aker Brygge ca 2 km øst for deg". En slik tjeneste forutsetter at celle informasjon om alle brukere med tjenesten på samles inn og det oppstår elektroniske spor som er ganske følsomme. I en slik sammenheng er det viktig at de slettes så snart de ikke har noen verdi for tjenesten. Hvis ikke er det betydelig risiko knyttet til utro tjenere hos tjenesteleverandøren.

Dirigering av taxi

Basert på tilsvarende løsning kan drosjesentral bruke lokasjonsinformasjon til å finne en ledig bil som er nærheten av en som ringer fra en mobiltelefon. Igjen blir det formidlet elektroniske spor til andre om din lokasjon, men i dette tilfellet er det enda mindre under brukerens kontroll hva som skjer videre med informasjonen. Det er uklart om slike tjenester er i bruk i Norge per i dag.

5.4.3 Minibanker

Bruk at minibank fører til elektroniske spor vedrørende hvilket bakkort som ble brukt, hvilken konto, beløp og tjeneste som ble benyttet. Disse sporene antas det at blir lagret primært sentralt, men i en periode vil en del lagres også i minibanken. Det antas også at slike spor er godt beskyttet med både fysiske og logiske sikkerhetsmekanismer.

5.4.4 Digital TV (DVB over satellitt eller kabel)

Vanlig bruk av et kringkastet TV-signal vil normalt ikke etterlate spor med mindre en tar opp TV programmene på eget opptaksutstyr som for eksempel video eller DVD opptager. Interaktiv TV som bruker en returkanal til tjenester som krever toveis kommunikasjon vil kunne etterlate elektronisk spor. Dette inkluderer;

- bestilling av programmer (Pay-Per-View)

- interaktive tjenester som spill etc.

I disse tilfellene kommuniserer brukerens utstyr med en sentralisert tjeneste som teknisk sett kan lagre all dialog med brukeren. Normalt vil en slik tjeneste lagre informasjon tilsvarende som for betalte web applikasjoner.

5.5 Digitale identiteter

PKI, Digital Id og Digitale signaturer

En digital identitet kan etableres på mange måter, ref kap. 4.1. En Public Key Infrastructure (PKI) er en teknologi som gjør det mulig for to parter å kommunisere sikkert uten å kjenne hverandre eller ha utvekslet informasjon seg imellom på forhånd. Dette er spesielt attraktivt når en skal tilby tjenester til store kundegrupper via Internett. Forutsetningen er at begge parter har kommunisert med utstederen av den elektroniske identiteten og stoler på denne.

Innehaveren av en identitet har en privat (hemmelig) digital kryptografisk nøkkel(verdi) som brukes for å "signere" data. Den som skal verifisere at data faktisk kommer fra innehaveren henter en tilsvarende (men ikke identisk) nøkkel fra en offentlig katalog og bruker denne for å verifisere ektheten av signaturen. Noen viktige momenter med PKI er at:

- teknologien er *meget sikker* så lenge den private (hemmelige) nøkkelen beskyttes godt, for eksempel på et smartkort
- den som skal autentiseres eller signere behøver *ikke å dele sensitiv informasjon* med andre, eksempelvis tjenesteleverandøren eller mottager
- partene behøver ikke å kjenne til hverandre eller kommunisere på forhånd
- når identiteten er autentisert genereres det elektroniske spor
- når partene kommuniserer kan nøklene brukes til å sikre selve innholdet som utveksles mot innsyn fra tredje part
- en digital signatur kan på samme måte som håndskrevne *etterprøves* i lang tid, men det forutsetter at en tar vare på tilstrekkelig informasjon

Altså er PKI en teknologi som på flere områder skaper mindre "hemmelige" elektroniske spor enn brukernavn/passord og gir god sikkerhet mot innsyn fra andre. Dette kan vurderes som positivt for personvernet. PKI gir på den annen side ikke anonymitet, men det motsatte; god sporbarhet. Dette kan vurderes som negativ for personvernet, spesielt hvis Digitale Identiteter brukes i situasjoner der brukeren kan/bør være anonym.

Dette er en teknologi som, så lenge det ikke er alternativer, er en forutsetning for en rekke elektroniske tjenester i dag. Likevel har den ikke blitt like raskt utbredt som antatt, spesielt ikke i konsumentmarkedet. PKI er teknologi som kan støtte en "tjeneste" som omtales som en TTP (Tiltrodd Tredje Part). Den tiltrodde part støtter altså de to kommuniserende parter med sikkerhetsmekanismer som nevnt over. I og med at kostnadene med å utstede slike digitale identiteter er betydelige så er det en forutsetning av brukerne, for eksempel innbyggere på ene siden og kommunene på den andre, vil betale noe for tjenesten etter at den er etablert. Foreløpig har det i Norge (som et særtilfelle i Europa) ikke vært mulig å finne en løsning på dette som har gitt vanlige innbyggere en Digital Id. Få aktører investerer i en (TTP) tjeneste hvis de som drar nytte av den ikke kan/vil betale. Alternativet er å bruke PKI som en tjenestespesifikk sikkerhetsmekanisme, og det er i betydelig grad det som har skjedd så langt i Norge. Viktige utstedere av Digitale IDer per i dag er ZebSign og BankID/BBS.

Federated Idenity
Dette kan kanskje oversettes til Delegert Identitet. Motivasjonen med teknologien er at en ønsker å redusere antall påloggingen en bruker gjør. Det finnes da en sentralisert tjeneste som brukeren autentiserer seg mot og det etableres et midlertidig elektronisk "bevis" for autentiseringen som gis til den (web)tjenesten brukeren skal benytte. Dette beviset kan så delegeres videre til en annen (web)tjeneste som gjenbruker autentiseringen uten at brukeren er direkte involvert i denne prosessen. Fordelen er at brukeren bare må "logge på" en gang, ulempen at brukeren ikke nødvendigvis har full kontroll med hva som utveksles av informasjon mellom de samarbeidende tjenestene. Microsoft Passport og standarder fra Liberty Aliance representerer teknologi som støtter denne type funksjoner.

5.6 Elektroniske blanketter

Adobe har lansert en ny teknologi for elektroniske blanketter som kan leveres elektronisk eller skrives ut og leveres på papir[19]. Denne type av blanketter kan f. eks. anvendes for forselvangivelsen, søknader etc.

Når man fyller i en slik blanketten skapes en strekkode lengst nede på blanketten. Denne strekkoden koder den informasjon som har blitt fylt in på blanketten samt potentielt informasjon om hvem har lest blanketten, hvem har fylt i den, når ble den i fylt etc. Når blanketten er utfylt sender brukeren den elektronisk eller skriver ut den på papir og legger den i postkassen. Før blanketten leveres kan den signeres på tradisjonell måte eller elektronisk ved digital signatur. Når papirblanketten ankommer mottageren skannes blanketten slik at mottager har de utfylte dataene og sporene som blanketten og strekkoden gir på et elektronisk format.

5.7 Autentisering

Normalt vil alle metoder for Autentisering av brukere innebære at det systemet som verifiserer identiteten lagrer mer eller mindre hemmelig informasjon som den deler med brukeren. Dette gjelder alle typer referanseverdier som passord, serienummer på id-kort, etc. Selv om en autentiseringstjeneste ikke nødvendigvis må lagre en kopi av hemmelige data i klartekst så vil normalt all autentisering loggføres og føre til elektroniske spor som i de fleste tilfeller er personlige. Siden vi autentiserer oss mot veldig mange ulike typer systemer er dette en rik kilde til elektroniske spor og det er viktig å ha tillit til at de systemene som behandler identitetsinformasjon.

Som nevnt tidligere er det tre overordnede faktorer som kan benyttes for autentisering. Når en type autentisering kombineres med en annen faktor omtales dette ofte som "to-faktor" autentisering. Det kan selvsagt også utvides til tre-faktor. Se også kap. 4.1.

Autentisering ved noe en vet
Dette er den vanligste typen av autentisering, fordi den gir en rimelig grad av sikkerhet ift. kostnadene knyttet til registrering og bruk. Det kreves ikke spesiell maskinvare, noe som holder kostnadene nede. Ulempen er at det ikke er umulig, og noen ganger ganske lett, å gjette den informasjonen (passord, PIN etc.) som brukes. Enten informasjonen eller en avledet referanse eller hemmeligheten må den lagres hos den som verifiserer identiteten.

[19] Face value: The alchemist of paper, The Economist, 14. april 2005.

Autentisering ved noe en har
Denne typen autentisering gir sikkerhet ved at en bruker er i besittelse av en fysisk gjenstand. Sikkerheten ligger i at gjenstanden ikke stjeles, mistes eller dupliseres uten at brukeren kan gi beskjed om å stenge for bruk av gjenstanden. Det finnes ulike former for utstyr; passordgeneratorer for engangspassord, adgangskort, smartkort, osv. Denne typen autentisering er normalt mer kostbar fordi det er en form for fysisk utstyr og eventuelt en fysisk avleser involvert.

Autentisering ved noe en er - biometrisk autentisering
Biometrisk autentisering baserer sikkerheten på at når en først har innsamlet en referanseverdi fra en person så er den meget vanskelig å endre på i ettertid. Biometriske metoder er delt i to faser; registrering og bruk. Registrering involverer "fangst" av biometriske referanseverdier og lagring av disse enten lokalt hos brukeren eller sentralt i en database. Denne informasjonen er spesielt viktig som et elektronisk spor da den per definisjon er personlig og det er viktig at de systemene som bearbeider og lagrer disse referanseverdien ikke bryter med personvernlovgivningen. Ved selve autentiseringen "avleses" biometrien på nytt for så å sammenlignes med referanseverdien. Hvis det er en tilstrekkelig god match vil autentiseringen godkjennes. Her ligger en av kjernetemaene ift biometri; under autentiseringen vil det systemet som verifiserer personen nødvendigvis måtte ha en kopi av referansen. Denne kan komme til verifikatoren på ulike måter, for eksempel fra et smartkort (i et pass), men det er hvordan verifikator i ettertid lagrer referansen som er det springende punktet. Er det slik at den slettes etter verifiseringen er det rimeligvis best, gjør den ikke det må en stole at verifikator ikke misbruker referansen. Denne problemstillingen kommer raskt opp når ulike land skal starte med verifisering av biometriske pass og det er svært ulike nasjonale regler og praksis knyttet til behandling av personlig informasjon.

Det er en god del biometriske teknikker hvor det nå finnes praktiske løsinger som tas i bruk. De mest vanlige er: fingeravtrykk, iris skanning, ansiktsgjenkjenning, retina mønster, stemme, "skrivstil" – måten en skriver på og håndgeometri. På grunn av at det er en viss sannsynlighet for en av disse ikke virker (forkjølet, sår på finger og lignende) blir det sett på som naturlig å utvikle systemer som håndterer flere biometrier i samme løsning.

5.8 Adgangs og tilgangs kontroll

Adgang til bygg og lokaler
Det utøves stadig mer og kontroll med adgang til bygninger og lokaler av sikkerhetsmessige grunner. Privat eiendom beskyttes på den måten mot innbrudd, tyveri og opphold av uønskede personer. De fleste slike systemer er en kombinasjon av et IT system og at den fysiske sikring med åpning og lukking av dører kontrolleres sentralt og er avhengig av person, tid og sted. Autentisering av brukere skjer normalt ved bruk av et adgangskort og evt. sammen med en PINkode for to-faktor autentisering. Adgangskontrollen skjer iht. oppsatte regler om soner, segmenter og personer. I utgangspunktet vi denne type systemer kunne lagre all informasjon om når for eksempel ansatte kommer og går samt hvor i lokalene de har vært. Normalt vil det være en godt beskrevet og etterlevd Policy for hva som logges og hvor lenge.

Logisk tilgangkontroll – aksesskontroll
Dette er i datasystemer all den aksesskontroll som systemet utfører på ulike nivåer. Det er prinsipielt basert på hvem som er autentisert, hvilke rettigheter denne har og hva slags objekt,

delsystem, fil eller lignende som en forsøker å få aksess til. Svært mange av disse begivenhetene vil logges og etterlate elektroniske spor. I næringslivet er det i praksis obligatorisk å logge mye data fordi arbeidsgiver er forpliktet til å kunne finne ut av hvem det var som var som forårsaket hva hvis noe går (riktig) galt.

DRM (Digital Rights Management) teknologi brukes for å kontrollere hvordan brukere kan benytte seg av digitalt innhold som er underlagt opphavsrettigheter. Det fungerer ofte slik at brukeren har en spesiell applikasjon (f. eks. Windows Media Player) eller et utstyr (f. eks. Apple I-pod). Når denne mottar en beskyttet fil, for eksempel en musikkfil, vil applikasjonen håndheve reglene for bruk og kopiering som gjelder for denne ved hjelp av kryptografiske teknikker. I teorien kan alt som brukeren utfører i applikasjonen logges og sendes over til en sentral server.

Elektroniske billetter
Elektroniske billetter er per i dag noe utbredt, men for eksempel de store kollektivselskapene har enda ikke satt slike systemer i drift. Dette er under arbeid og Oslo Sporveier forventes å innføre elektroniske billetter om ikke altfor lenge.

5.9 Sporingsteknologi

RFID (Radio-Frequency IDentification) brikker består av en liten "integrated circuit" koblet til en liten antenne. En RFID brikke svarer på forespørsler fra en leser gjennom å sende ut et unikt serienummer. De fleste RFID brikker er passive. Det betyr at de ikke trenger noe batteri. De får den energi de trenger fra selve forespørsel signalet. For at RFID brikken skal svare på en forespørsel må leseren vare tilstrekklig nære, typisk som mest noen meter. RFID brikker er allerede brukt i mange sammenhenger, så som erstatter før nøkler, for å detektere tyveri i butikker, før å spore pakker under transport og før lagerhåndtering. RFID brikker blir stadig billigere[20] og det blir mulig å produsere mindre å mindre[21] brikker.

Man kan se på RFID som en utvikling av de strekkoder som finnes på alle produkter vi kjøper. De som er forskjellen er at RFID brikker kan leses av på avstand og at hver RFID bikke har en unik id og dermed har også hver enkelte produkt en unik id.

Hvis alle produkter vi kjøper er utstyrt med en RFID brikke som ikke lett kan tas bort medfører det vi kan spores via de produkter vi bærer med oss (f. eks. klær) og at informasjon om disse produkter kan leses når vi beveger oss i samfunnet. F. eks. så skulle man kunne registrere hva folk har i vesker/ryggsekker/håndvesker.

RFID tilbyr store effektivitetsgevinster for bedrifter ved at det underletter transport og lagerhåndtering. Men det eksisterer også anvendelser som kan forenkle ting for folk flest. Eksempler på anvendelser som er presenteret inkluderer: mikrobølgeovner som kan tillage mat automatisk gjennom å lese av RFID brikken på emballasjen og garderober som kan presenter sitt innhold på en display. Men de personvernsproblem RFID medfører er fremst relatert til bruken etter at produktene forlater butikkene. Derfor har det blitt utviklet flere løsninger på

[20] S.E Sarma, Towards the five-cent tag, Report MIT-AUTOID-WH-006, MIT AutoID Center, 2001.

[21] K. Takaragi, M. Usami, R. Imura, R. Itsuki, og T. Satoh, An ultra small individual recognition security chip, IEE Micro, 21(6):43-49, 2001.

hvordan RFID brikker skal kunne deaktiveres av konsumenten selv eller når de kjøps i butikken.

GPS (Global Positioning System) er en teknologi som gjør det mulig å finne geografisk posisjon for en mottager. Systemet er basert på mer enn 24 satellitter som sender ut signaler som mottageren lytter til og basert på disse kan finne sin egen posisjon, høyde over havet og tid. Tradisjonell bruk har vært navigasjon for båt, fly og bil og teknologien ble opprinnelig utviklet av US DoD for militære formål, men er siden 1995 kommersielt tilgjengelig. Så lenge mottageren er et passivt utstyr og ikke kommuniserer posisjonen til annet utstyr genereres *ikke* elektroniske spor. Det som derimot er tilfelle er at GPS mottagere blir mindre og mindre og brukes som en del av et større system der posisjon er en verdi som brukes sammen med andre elementer og lagres. Et eksempel på dette er systemer for kjøreanvisning og veivalg. Her brukes posisjon fra en GPS mottager sammen med elektroniske kart for å anvise kjørerute fra ett sted til et annet og systemet er hele tiden oppdatert på de nærmeste veikryss og lignende under veis. Slike systemer kan lett utvides til å måle hastighet og å lagre tid og sted. I den grad dette utstyret er personlig vil slike elektroniske spor også være personlige. Andre anvendelser av GPS kombinert med andre systemer er; tyverialarmer og trygghetsalarmer som rapporterer posisjon tilbake via mobil kommunikasjon (GSM), overvåkning av varetransport og muligens overvåkning av personer, fartsovertredelser etc.

5.10 Identifiseringsteknologi

Biometrisk identifisering
Biometrisk autentisering har to ulike anvendelser. Den ene er *verifisering* av en identitet; altså en en-til-en autentisering hvor brukeren selv hevder å ha en bestemt identitet. Den andre anvendelsen er *identifisering* hvor man ønsker å finne identiteten til en person blant mange. Verifisering er det som benyttes ved autentisering mot systemer der brukeren allerede er registrert. Her har brukeren en viss tillit til systemet eller pålegg om å gi fra seg sine referanseverdier, se kap. 5.7.

Identifisering er det som benyttes for å plukke ut en person blant mange uten at systemet får oppgitt den identitet brukeren hevder å ha. Dette vil en del tilfeller kunne gjøres selv uten at personen nødvendigvis er klar over prosessen.

5.11 Innsamlingsteknologi

Det eksisterer en rekke teknologier for å samle in elektroniske spor i den elektroniske verden og for å etablere elektronisk dokumentasjon av hendeler i den fysiske verden. Ved bruk av alle former for innsamlingsteknologi er det stor risiko at det samles inn mer informasjon enn det en i utgangspunktet var ute etter, såkalt overskuddsinformasjon.

Web bugs også ibland kalt web beacon er et lite bilde, ofte transparent, som er umulig for øynet å se. Denne type bilde plasseres oftest i html e-poster. Når brukeren leser e-posten leses html koden som forteller e-post leseren at den må laste ned bilder fra en server på Internett. Serveren registrerer så IP adressen til brukeren og potentielt annen informasjon som f. eks. tidspunkt. Nå kan den som sendte ut "web buggen" koble brukerens e-post adresse til brukerens IP adresse.

Web bugs kan også plasseres på websider for å samle in informasjon om websider som en bruker besøker. Om man tenker seg at alle websider på Internett inneholdt samme web bug ville en sentralt kunne registrere hvilke sider hver enkelt bruker besøkte.

De annonser som plasseres på websider på Internett lastes ofte ned fra en bedrift som hjelper andre bedrifter med å håndtere deres Internett annonsering. Eksempler på slike bedrifter er Google AdSense og Doubleclick. Disse har muligheten å føre register over folks surfevaner på samme måte som man kan gjøre med web bugs. Det som skiller Internett annonser fra web bugs i denne sammenheng er at web bugs er usynlige bilder medens reklame selvfølgelig må synes.

For å håndtere problemet med dynamiske IP adresser blir ofte cookies brukt sammen med web bugs.

Spionprogrammer (spyware) er programmer som spionerer på brukeren ved å sende informasjon om brukerens handlinger til en sentral server. Spionprogrammer inngår ofte som en del i gratisprogrammer som kan lastes ned fra Internett. Formålet med disse spionprogrammene er ofte å skape brukerprofiler. Disse brukerprofilene brukes deretter til å skreddersy reklame i det nedlastede programmet eller på nettsider som brukeren besøker. F. eks. kan et program for å lytte på CD plater og mp3-filer rapportere tilbake til bedriften som har laget programmet hvilke sanger brukeren lytter på.

Key loggers er et eksempel på et spionprogram. En key logger er et program og/eller et utstyr som logger alle "tastetrykk" på en maskin. Tastetrykkene sendes enten til en sentral server eller lagres lokalt på utstyret. Key loggers brukes ofte for å fange opp brukeres passord og brukernavn. Når man bruker offentlige datamaskiner skal man være spesielt observant i forhold til key loggers.

En **Trojaner** er et program som forsøker å åpne en "bakdør" i datamaskinen der det er installert. Hvis en trojaner har blitt installert kan alle som har kjennskap til den fjernstyre maskinen. Hackere installerer ofte en trojaner etter at de brutt inn i en maskin slik at de enkelt kan vende tilbake til maskinen senere og bruke den for å nå sitt egentlige mål.

Søkmotorer på Internett kan brukes for å søke etter personopplysninger på Internett. Det går ofte an å finne informasjon som e-post adresser, telefonnummer, forskjellige lister over ansatte og medlemmer etc. Det anbefales å teste hva du kan finne om deg selv på Internett. F. eks. "spammers" bruker ofte automatiske verktøy for å søke på Internett etter e-post adresser (dette kalles ofte "screen scraping").

Datakommunikasjon kan enkelt fanges opp av "**pakkesniffere**" som man kan laste ned gratis på Internett. Usikrede trådløse nettverk er spesielt enkle å avlytte ettersom man ikke trenger i ha fysisk tilgang til noen nettverkskabel. Telekommunikasjon kan også fanges opp med diverse avlyttingsteknologi.

Det eksisterer diverse **dataetterforskningsutstyr** og mye er tilgjenglig gratis på Internett. Dette brukes til å lese ut informasjon fra PCer og servere og spesielt hele innholdet på harddisker (som ikke er skrevet over). Det eksisterer også spesialutstyr og programvare for lese ut informasjon fra mobiltelefoner og PDAer.

Videoovervåkning er en velkjent teknologi for å fange hendelser i den fysiske verden. De kameraer som brukes er ofte digitale, hvilket gjør det enkelt å lagre, analysere og distribuere det innspilte materialet. Se for øvrig kap. 5.12.

Teknologi for **lokasjonssporing** av ting eller mennesker som for eksempel GPS og RFID er en annen type teknologi som kan brukes med det formål å overvåke personer ved at det "plantes" på den en vil overvåke.

Hjemmelarm med abonnement hos vaktsentral (f. eks. Hafslund og Securitas). Informasjon om hjemmet i form av aktiverte sensorer, tidspunkt og lignende prosesseres og lagres lokalt. Hele eller deler av denne informasjonen kan rapporteres til alarmsentralen.

5.12 Videoovervåkning

Digitale videokamra med TV-monitorer og lagrings utstyr har blitt billigere og det er enkelt å installere. Utstyret blir benyttet lovlig eller ulovlig, over alt i samfunnet og spesielt innen det offentlige og næringslivet. Privat er videoovervåking lite utbredt, men vaktselskapene leverer enklere systemer i forbindelse med innbruddsikring. Overvåking og kommunikasjon med besøkende ved inngangsdører forekommer også. Det er innehaveren som setter opp videoovervåkingen som er ansvarlig for dette.

Videoovervåking er ofte uten lyd, men i noen sammenheng kan lyd kobles til, hvilket medfører en annen bruk (avlytting) i forhold til lovverket. Videoovervåking oppfattes av nordmenn flest som positivt. Et effektivt preventivt middel til å forebygge kriminelle handlinger og som dokumentasjon på hendelser i ettertid. Det er viktig å presisere at videoovervåking inngår i begge kategoriene av elektroniske spor; spor vi bevisst legger igjen eller er oppmerksomme på blir registrert eller elektroniske spor vi ikke er oppmerksomme på blir registrert.

Alt et videokamera registrerer og lagrer, og som kan settes i tilknytning til en identifiserbar person, er et elektronisk spor. Videoen registrerer automatisk tidspunktet, og den geografiske lokasjonen er definert. Det er regler for lagring av videoovervåking og bildebruk i personopplysningsforskriftens § 8. Se [22]

Ytterligere informasjon om dette tema finnes blant annet på
http://www.personvern.uio.no/pvpn/eksempler/index.html

5.12.1 Videoovervåkning i næringslivet

Næringslivet har for lenge siden tatt i bruk videoovervåking, men det er først i den senere tid, når prisene har gått ned og kvaliteten på det digitale, i forhold til analogt utstyr, er vesentlig forbedret at videoinstallasjoner tas i utstrakt bruk.

Til å begynne med var videokamra forbeholdt adgangskontroll tilkoblet bemannede kontrollrom med intern talekommunikasjon til personene som ankom. Dette ble normalt ikke lagret. I dag brukes ofte videokameraer i adgangskontroll sammen med annet utstyr for identifikasjon og fysisk åpning av dører, porter og bommer. Overvåkingen lagres og ved bruk av sporingsmekanismer basert på de ulike registreringsfunksjonene, kan hendelser enkelt

[22] Personopplysningsforskriften, http://www.lovdata.no/for/sf/mo/xo-20001215-1265.html

dokumenteres i ettertid. Eksempelvis hvem som ankom på et bestemt tidspunkt og hvem (en eller flere) som passerte inn.

I selvbetjeningsbutikker blir videoovervåking stadig mer vanlig i selve lokalet og ved kasseapparatene. Videokameraene ved kassaapparatene kobles ofte sammen med betalingsfunksjonen og butikkens salgsregistreringsfunksjon. Det oppstår elektronisk spor som inneholder identifisering om den ansatte i kassen, kunden, varekjøpet og i tillegg eventuelt elektronisk betaling. Systemet settes opp for å kontrollere at den registrerte varen er i overensstemmelse med den fysiske varen. Av andre områder næringslivet ofte benytter videoovervåking er produksjonslokaler, lagerområder og parkeringsplasser.

5.12.2 Videoovervåkning i offentlig sektor

Det offentlige rom er ofte debattert i forbindelse med bruk av videoovervåking. Tryggheten for allmennheten i forhold til personlig integritet kan være et dilemma.

Samferdselssektoren

Det skilles mellom videoovervåkingen som (1) foretas i forbindelse med trafikkovervåkingen, (2) det som foretas ved bomstasjoner og (3) automatisk trafikkontroll (ATK).

Det finnes mange videoovervåkingspunkter langs de mest trafikkerte veiene ved større byer. Videoovervåking langs norske veier er først og fremst en trafikal overvåking med hensyn til trafikkavvikling. Bildene er slik at ikke personer eller kjennemerkene kan gjenkjennes. Det blir heller ikke lagret noe fra denne videoovervåkingen. Slik overvåking skjer av alle tunneler og vegstrekninger med stor trafikk, som E6, E18 og Ring 3.

Videoovervåkingen som foretas på bomstasjoner registrerer bare kjennemerkene.

Ved automatisk trafikkontroll (ATK), som sjekker overtredelse av fart eller kjøring mot rødt lys, tas det bilder som gjenkjenner både personer og bilens registreringsnummer.

Teknologien til videokamerasystemene har imidlertid også potensial til å kunne brukes til automatisk fartskontroll. Overtredelser registreres og lagres, som ved fartsradarer og bilde. Identifisering av kjøretøy og personer er nødvendig for oppfølging av overtredelser. Det som gir elektroniske spor er kjøretøyets registreringsnummer og muligheten for personidentifisering. Dagens ATK teknologi kan også utvides til å måle fart over en strekning mellom to automater.

Offentlige steder

Det er satt opp videoovervåking flere steder i det offentlige rom. Dette er ofte begrunnet med den preventive virkningen overvåkingen medfører. En spesiell funksjon har videoovervåkingen ved plasser som vurderes spesielt utsatt for terrorhandlinger. Innen denne kategorien er flyplasser, større transportterminaler og spesielle offentlige bygninger. Det er utviklet funksjoner som analyserer video- registreringen i sanntid for å kunne identifisere mulige trusler som folkeansamlinger, mistenkelige personer og bomber. Situasjonene kan gi automatisk alarm. Spørsmålet er i hvilken grad videoovervåking av offentlig rom krenker den enkelte persons integritet ved eventuell registrering og lagring. Det forskes på mekanismer for å "anonymisere" videoene, bla annet ved hjelp av videoanalyse for ansikt gjenkjenning (posisjon).

6 Lagringssteder

Elektroniske spor lagres på forskjellige steder. En viktig skillelinje er hvem som har kontroll over lagringsstedet og dermed har mulighet å beskytte det. Det er grovt sett tre alternativer som er relevante. Elektroniske spor kan lagres i databaser kontrollert av de virksomheter som har samlet in de elektroniske sporene, de kan lagres i den enkeltes private utstyr eller de kan lagres i utstyr og databaser som eies av den enkeltes arbeidsgiver.

Tjenester kan ofte konstrueres slik at informasjon lagres sentralt og/eller lokalt. For eksempel kan man ha en lokal kalender på mobiltelefonen og/eller man kan ha en kalender som lagres sentralt på en server som man kan få tilgang til via internett og GPRS. Når informasjon lagres sentral er det nødvendig at man har tillit til at tjenestetilbyderen beskytter og ikke misbruker informasjonen.

Generelt er det også slik at kostnaden for lagring per lagret bit faller etter hvert som kapasiteten til lagringsmediene øker. Dette har ført til at det snart er billigere å lagre data permanent enn å slette dem – ikke fordi det er gratis, men fordi en kan lages nye tjenester basert på lagring av ekstreme mengder data. Altså risikerer vi at en del elektroniske spor blir tilnærmet ”evigvarende” med de konsekvenser det har.

6.1 Virksomhetsdatabaser

De elektroniske spor som samles inn av bedrifter, foreninger, og det offentlige lagres i forskjellige databaser. Disse er som regel ikke offentlig tilgjenglige, men den enkelte har ifølge personopplysningsloven rett til innsyn i slike register. Problemet er nok ofte at den enkelte ikke har oversikt over hvilke virksomheter som har opplysninger lagret om en selv.

Eksempler på slike databaser inkluderer: kundedatabaser, bankenes databaser med betalings- og kontoinformasjon, e-post tjenere, teleoperatørers databaser over telefonsamtaler og forskjellige register det offentlige har over norske borgere.

6.2 Offentlig tilgjenglige databaser

Andre databaser er åpent tilgjenglige for allmennheten. Databaser kan også være tilgjenglige og søkbar via Internett som for eksempel skattelistene. Offentlige databaser vil være tilgjengelige i henhold til offentlighetslovens § 2, annet ledd. Enhver kan gjøre seg kjent med innholdet i en bestemt sak. I henhold til denne lovbestemmelsen utleveres det blant annet opplysninger fra Det sentrale motorvognregister. Alle kan ringe til Statens vegvesen, blant annet til en trafikkstasjon, og spørre hvem som eier en bestemt bil. Forutsetningen er at det oppgis hele kjennemerket (jfr. Offentlighetslovens krav om identifisering av en bestemt sak). Ved en slik forespørsel oppgis eierens navn og adresse og eventuelt tekniske opplysninger, dersom det er av interesse.

Andre eksempel er diverse (private) lister som er publisert på Internett, som resultatlister og lister over ansatte, medlemmer og studenter. Bekjente og andre kan også ha lagt ut informasjon om enkelte på sine hjemmesider. F. eks. private fotoalbum på nettet eller de kan ha koblet opp webkameraer. Noen av disse webtjenestene krever autentisering og autorisasjon for tilgang, men i mange tilfeller brukes brukernavn og passord som er lette å gjette.

Man kan tenke seg et scenario der noen med onde hensikter publiserer personlig informasjon på Internett. Selv om informasjonen oppdages og man lykkes med å få den slettet fra websiden er det ikke sikkert at informasjonen er borte fra Internett ettersom de forskjellige søkemotorene på Internett kontinuerlig tar kopier av websider. Informasjonen kan da fortsatt være tilgjenglig for alle som bruker de rette søkekriteriene.

Nyhetsgrupper kan innholde mye informasjon om enkelt mennesker. Det er viktig å være klar over at innlegg i nyhetsgrupper vil finnes tilgjenglige over svært lang tid. Nyhetsgrupper kan leses med hjelp av spesielle leser og på Internett.

6.3 Personlig utstyr - PC

PCer innholder ofte mye elektroniske spor ettersom de brukes til mange forskjellige anvendelser som f. eks. å lese og skrive e-post, surfe websider, spill, skrive dokumenter og betale regninger.

Disse elektroniske sporene kan komme i feil hender ved at PCen blir stjålet. Risikoen for dette er spesielt høy for bærbare maskiner som man ofte har med seg når man reiser. En annen måte å få tilgang til disse elektroniske sporene hvis maskinen er koblet til Internett er å gjøre datainnbrudd i maskinen.

Det er spesielt viktig å tenke på hva man gjør når man bruker offentlige datamaskiner, f. eks. på bibliotek eller Internettkafeer. Her kan hvem som helst tilgang til de elektroniske spor du etterlater deg.

På en PC finnes ofte en mengde filer laget av brukeren og de programmer brukeren benytter. Det finnes ofte også en rekke logger som er skapt av operativsystemet og de programmene som er brukt. Eksempler på slike filer og logger inkluderer:

- Logger over hvilke dokumenter brukeren nylig har åpnet
- Adressebok
- Digitale fotografier
- Øyenblikksmeldinger
- Chat-logger
- E-post
- Bokmerker
- Besøkte websider
- Cookies
- Passord og brukernavn (krypterte og ikke krypterte)
- Klient sertifikat

6.4 Mobiltelefoner/PDA

En PDA (Personal Digital Assistent) er en liten bærbar datamaskin. I de senere år har ofte PDAer blitt utstyrt med mobiltelefonfunksjonalitet og motsatt. Flere og flere mobiler har nå PC liknende funksjonalitet (f. eks. mulighet å lese dokumenter, webbrowser etc.), altså kan de samme elektroniske spor som man finner på PCer ofte bli funnet på mobiltelefoner. På en rekke nyere mobiltelefoner har man også mulighet å bruke høykapasitets minnebrikker for å lagre

informasjon utover den begrensede lagringskapasitet som finnes på SIM-kortet og i eventuelt innbygget minne.

Mobiltelefoner er enkle å miste pga at de alltid er med og at de ofte er små.

Eksempel på informasjon som man kan finne på en mobiltelefon:

- Anropliste - innkommende og utgående samtaler, hvem, når, og hvor lenge
- Adressebok – ofte mer innholdsrik enn adresseboken på PCen.
- SMS/MMS - innhold, mottagere, avsender og tid
- Dagbok/kalender – møter, timeboking hos legen

Flere og flere mobiltelefoner har også Bluetooth funksjonalitet (Blåtann). Hvis Blåtann er konfigurert feilaktig er det ofte mulig for andre å laste ned innholdet fra mobiltelefonen gjennom å initiere en Blåtann oppkopling. Se for øvrig kap. 7.2.

6.5 Annet utstyr

Spesielt utstyr med innbygget persistent minne, slik som harddisker, innholder ofte elektroniske spor uten at det er åpenbart for brukere av utstyret. Faksmaskiner, kopimaskiner, og skrivere (ofte kombinert i en maskin) er eksempler på utstyr som kan ha innbygget harddisk. På denne harddisk kan man finne dokument som blitt fakset, kopiert eller skrevet ut.

Harddisker blir både mindre og billigere og dermed finner man dem i stadig flere typer utstyr, som f.eks. mp3-spillere og videokamera.

Annet utstyr som kan innholde elektroniske spor:

- GPS utstyr
- Ferdskrivere
- Kartdata/kjøreanvisninger/navigasjonsutstyr
- Telefonsvarere - kan også være virtuelle, dvs. meldinger lagres sentralt hos teleoperatøren
- Minnebrikker - kan f. eks. lagre personlige bilder.
- Lagringsmedia – CD og DVD

6.6 Trusler mot lagringssteder

Det eksisterer mange typer trusler mot IKT systemer og Senter for Informasjons Sikkerhet (SIS) publiserer hver måned en status rapport; "IKT Trusselbilde for Norge", se forøvrig [23]. Her nevnes 17 ulike trusler mot IKT systemer i april 2005 og det vurderes slik at minst halvparten av disse er primært knyttet til misbruk av elektroniske spor. I tillegg til aktive trusler beskrevet av SIS er det også et betydelig problem at det oppstår mange elektroniske kopier av dokumenter og lignende og det behandles kort herunder.

[23] http://www.norsis.no/details.php?type=trusselbilde

6.6.1 Mangelfull filsletting

Det er viktig å være klar over at når en bruker sletter en fil så blir vanligvis ikke innholdet i filen slettet. Det som skjer er at operativsystemet markerer den plassen på disken som filen benytter som ledig. Filen blir ikke overskrevet før nye data blir skrevet over på det samme stedet som den gamle filen var. Det betyr at om man avleser disken direkte uten å gå via operativ systemet så kan man fortsatt lese filens innhold. For å slette filen en gang for alle må man skive over hele den fysiske lagringsplassen på disken som filen opptok.

Harddisker i mobilt utstyr og tradisjonelle harddisker i PCer og tjenere blir før eller senere kassert fordi utstyret går i stykker eller harddiskene blir umoderne. Dette gjelder også taper for backup lagring og andre magnetiske lagringsmedia. Hvis ikke disse diskene og tapene destrueres eller overskrives skikkelig kan man normalt gjenfinne elektroniske spor på dem. Kostnaden ved å lete er heller ikke veldig stor hvis en vet hva en leter etter.

6.6.2 Swap-space

Et annet moment å tenke på er det som vanligvis kalles ”swap-space”. En datamaskin har to typer av hukommelse; harddisken og arbeidsminnet. Når en starter et program lastes det inn fra harddisken til arbeidsminnet. Arbeidsminnet er ikke persistent som harddisken er men det er mye raskere å lese og skrive til. Ulempen med arbeidsminnet er at det er dyrt og derfor er det begrenset hvor mye man kan ha i en vanlig PC. For å øke størrelsen på arbeidsminnet allokerer man ofte en del plass på harddisken. Denne plass kalles ”swap-space”. Det faktum at en del av arbeidsminnet lagres på harddisken betyr at denne del av arbeidsminnet er persistent, dvs den går å lese også ner strømmen har slåtts av. Det betyr at om man leser denne del av disken kan man potentielt finne elektroniske spor som bare var tiltenkt å være i arbeidsminnet.

6.6.3 Midlertidige filer - .tmp

Utover eventuelle kopier av filer på ”swap-space” kan det forekomme at filen eller deler av filen finnes lagret i temporære filer som programmet en bruker har lagret på eget initiativ.

F. eks. når brukeren skriver et dokument lagres det i arbeidsminnet. Når brukeren trykker på ”lagre” knappen lagres det på harddisken også. Brukeren åpner så noen andre programmer. Dette fører til at arbeidsminnet må fylles med disse programmene. Dokumentet som brukeren fortsatt har åpent flyttes derfor til ”swap-space” på harddisken. Nå bestemmer brukeren seg for å slette dokumentet. Ettersom dokumentet nå kan finnes i to ekstra kopier på harddisken (en på ”swap-space” og en .tmp fil) må brukeren skrive over begge disse kopiene hvis en virkelig ønsker å slette innholdet i den opprinnelige filen. Det antas at et fåtall brukere er inneforstått med disse momentene.

7 Scenarier

7.1 Innledning

Det følgende skisseres tre scenarier

1. Et scenario fra helsesektoren.
2. Et fra samferdselssektoren.
3. Et om mulige misbruk av elektroniske spor.

I det første beskrives dagligdagse situasjoner i løpet av en arbeidsdag i helsesektoren hvor ulike typer informasjons- og kommunikasjonsteknologi spiller en rolle i aktørenes daglige virke. Scenariet dekker deler av det daglige arbeidet til leger, sykepleiere og kontormedarbeidere.

Det andre scenariet beskriver en tenkt arbeidsreise, altså en sekvensiell beskrivelse av forflytning mellom forskjellige lokasjoner med ulike framkomstmidler, hvor IKT-teknologi brukes underveis og hvor ulike elektroniske spor legges igjen.

Det siste scenariet beskriver noen potensielle situasjoner hvor elektroniske spor og data bevisst misbrukes av tredjepart. Vi tar ikke stilling til sannsynligheten for at de beskrevne situasjoner inntreffer.

7.2 Scenario fra helsesektoren

I dette skisserte scenariet ser vi på de elektroniske spor som kan legges igjen av en medarbeider i helsesektoren. Vi prøver å være såpass generelle at det kan gjelde lege, så vel som sykepleier, hjelpepleier eller merkantilt personale (sekretærfunksjoner). Videre skisserer vi et scenario som kan gjelde et sykehus, så vel som et legekontor/en legevakt.

7.2.1 Reise til og fra arbeid

Elektroniske spor som legges igjen på vei til og fra arbeid dekkes av scenariet som omhandler samferdsel.

7.2.2 Bevegelse inne på sykehusområdet

Ved ankomst til sykehuset (sannsynligvis ikke legekontoret) kan det være videoovervåkning av inngangspartiet og muligens på utvalgte andre lokasjoner, men sannsynligvis ikke noen omfattende videoovervåkning. Elektroniske spor kan også legges igjen i forbindelse med parkering på sykehusområdet.

Sykehus er tradisjonelt et åpent miljø med få adgangsbegrensninger, men dersom vedkommende helsepersonell f.eks. arbeider med spesialutstyr eller på spesialavdelinger så vil man typisk måtte benytte nøkkelkort for å komme inn på slike steder. Enkelte rom hvor kun personale befinner seg vil sannsynligvis være låst, i hvert fall på større sykehus.

Mulige elektroniske spor som legges igjen vil være:

- Man blir fanget opp av videokameraer.
- Adgangskort blir registrert, dersom kortets kode må tastes inn.

7.2.3 Sykehusets PC-nettverk

Helsepersonell jobber i ulike team på ulike avdelinger og hver enkelt medarbeider har typisk ansvaret for et visst antall pasienter, enten man er lege, sykepleier, hjelpepleier eller merkantilt personale.

Avhengig av arbeidets art kreves det ulik tilgang til forskjellig type informasjon, og denne informasjonen er lagret enten på papir eller digitalt i sykehusets systemer. I det siste tilfellet kreves det innlogging på sykehusets PC-nettverk, ved hjelp av passord og brukernavn. Da kan det til enhver tid spores hvem som er logget på systemet. Dersom internett og e-post er tilgjengelig for medarbeideren vil også dette kunne spores. Vanlig e-post skal ikke inneholde pasientinformasjon.

Sykehuset eller legekontoret har ulike IKT-systemer som etter hvert blir tettere og tettere integrert via nettverk. Elektronisk pasientjournalsystem vil typisk være et av de mest sentrale systemene her. Typiske elektroniske pasientjournalsystemer vil for norske sykehus være DIPS, Infomedix og DocuLive. De meste brukte pasientjournalsystemene på legekontorene er Profdoc WinMed, Profdoc Vision, SystemX og Infodoc. For å komme inn på disse systemene må man også logge seg inn med brukernavn og passord.

Ulike prøvesvar blir typisk sendt mellom laboratorier og sykehus og legekontorene, eller internt mellom ulike avdelinger på sykehuset. Dette kan være prøver innen klinisk kjemi, mikrobiologi, patologi, røntgen, EKG, samt epikriser med mer. Per i dag skjer dette som en kombinasjon av digitalt overførte data og data som blir sendt i brev, faks eller internpost. Utviklingen går i retning av at stadig mer blir digitalisert og de ulike systemene blir koblet tettere sammen i nettverk.

Mulige elektroniske spor som legges igjen vil være:

- Registrering av når en bruker logger seg inn/ut av nettverket.
- Registrering av mulig internett bruk, dvs. hvilke websider som leses.
- Registrering av eventuell e-post korrespondanse.
- Registrering av innlogging på andre typer systemer, f.eks. pasientjournalsystem eller ulike spesialist-/laboratoriesystemer.

7.2.4 Elektronisk pasientjournalsystem

Tilgang til ulike deler av sykehusets eller legekontorets (elektroniske) pasientjournalsystem er definert ut ifra hvilken rolle man har. En lege vil typisk ha flere rettigheter enn andre typer medarbeidere som bruker systemet.

Hovedregelen for å gi en helsemedarbeider tilgang til informasjon i en pasients (elektroniske) journal, er at denne informasjonen er nødvendig som beslutningsgrunnlag for å gjennomføre et tiltak i forhold til pasienten.

Mange tiltak som gjennomføres på sykehus vil være komplekse og involvere mange (typer) medarbeidere som bidrar ved gjennomføring av en større eller mindre del av tiltaket. Disse vil

kunne ha forskjellige behov for helseopplysninger i forbindelse med gjennomføringen av tiltaket.

Alle skal med andre ord ikke kunne ha tilgang til all informasjon i en pasients elektroniske journal, og pasienten kan også reservere seg i forhold til hvem som skal ha tilgang til hva. Et elektronisk pasientjournalsystem, eller andre typer systemer som behandler pasientdata, vil typisk være i stand til å registrere:

- Hvem som er logget på systemet og når de er logget på.
- Hva disse personene leser og registrerer (endrer) i systemet.
- Samt ulike former for sporbarhet, for eksempel mellom hva en medarbeider leser eller endrer i systemet og besluttede tiltak .

7.2.5 Oppsummering

Medarbeidere i helsesektoren legger igjen ulike elektroniske spor i sitt daglige virke.

Flere av de elektroniske sporene er de samme som finnes ellers i samfunnet, f.eks. elektroniske spor knyttet til Internett og e-post bruk, eller spor knyttet til innlogging på interne nettverk.

Imidlertid vil leger, sykepleiere osv. måtte forholde seg til mer detaljert registrering av sin aktivitet i IKT systemene som inneholder sensitive pasientdata.

7.3 Scenario fra samferdsel

I dette skisserte scenariet ser vi på de elektroniske spor som legges igjen ved en tenkt reise til utlandet, f.eks. London. Vi tenker oss at vedkommende i de ulike situasjonene bruker elektroniske betalingsløsninger framfor kontanter. Elementer i dette scenariet er typiske i forhold til hvilke spor hver og en av oss legger igjen i hverdagslivet.

7.3.1 I bil

Vi tenker oss først at vedkommende kjører til jobben/kontoret og parkerer der. Kanskje legges det igjen elektroniske spor knyttet til selve parkeringen og kanskje informasjon knyttet til betaling for parkeringen også. På vei til arbeidssted vil vedkommende kunne ha lagt igjen spor (kjennemerke) ved passering av bomring og kanskje har vedkommende kjørt for fort og blitt registrert i en fotoboks også, stakkars.

7.3.2 Mobiltelefonbruk

Bruker vedkommende i tillegg mobiltelefon vil denne kunne spores lokasjonsmessig, med informasjon om hvem du ringer til, hvilket SIM kort du bruker og hvilken enhet du har. Mobiltelefonen vil benyttes i de fleste situasjoner i det etterfølgende, bortsett fra ombord på flyet.

7.3.3 I taxi

Etter en stund på arbeidsstedet bestilles det kanskje en taxi til jernbanestasjonen, Oslo S, og informasjon om reisens lokasjoner, tidspunkt og varighet registreres, i tillegg til informasjon om ditt kredittkort og hvor mye det har blitt belastet. (Kanskje også videoovervåkning i taxi?).

7.3.4 På jernbanestasjonen

På Oslo S blir du fanget opp av videokameraer mens du beveger deg inne på jernbaneområdet, kanskje mens du står i billettskranken og kjøper billett. Du betaler for en elektronisk billett, denne gangen bruker du bankkort (Bank-Axept fra BBS). Denne benytter du under togreisen og må dra kortet da du forlater stasjonsområdet på Oslo Lufthavn.

7.3.5 På flyplassen

På flyplassen vil du kunne bli fanget opp av videokameraer, og du vil også her kunne sjekke inn elektronisk og papirløst. Du benytter bankkortet ditt til å ta ut reisevaluta, i dette tenkte tilfellet britiske pund. Du sjekker inn og går deretter til tax-free utsalget hvor du kjøper sprit og sigaretter og betaler på nytt med kort. Du er kanskje uoppmerksom og går med Bluetooth påslått uten at du bruker den (mer om dette senere) og du tar fram din bærbare pc og kobler deg opp på flyplassen trådløse nett (også mer om dette senere). Her logger du deg inn, benytter på nytt kredittkort og bestemmer deg for å spille on-line poker. Du taper 100$ før det blinker boarding på lystavlen.

7.3.6 Ved passkontrollen

Du skal til Storbritannia hvor det kreves passkontroll ved avreise. Dersom reisen foregår etter 1.oktober og du nylig har skiftet pass, vil biometriske data om deg bli sjekket. Disse dataene ligger sannsynligvis lagret i passet ditt, og ikke sentralt registrert. Før du går ombord sjekkes din papirløse billett ved gaten.

7.3.7 På bestemmelsesstedet i utlandet

Vel framme i London må du også vise pass i London. Her kan du som reisende ikke være sikker på om de biometriske dataene slettes i utlandet eller om de blir liggende igjen utenfor den reisendes kontroll. Hadde reisen gått til Amerika eller et annet fjernt land utenfor EØS ville usikkerheten sannsynligvis være enda større.

Når du har ankommet flyplassen i London slår du på mobiltelefonen hvorpå "home-location" registeret oppdateres med nytt nett og lokasjonsområde. Dine mobilsamtaler går nå via en utenlandsk operatør.

Du tar taxi til sentrum og hotellet du skal bo på. På nytt betaler du med kredittkort, både i taxi og på hotell. Kanskje du har et bonuskort på hotellet (hotellkjeden) du benytter. Dette må også registreres.

Du bruker kanskje også hotellets nettilkobling slik at du kan surfe på internett eller logge deg inn hos arbeidsgiver og kanskje jobbe litt før møtene begynner.

7.3.8 Oppsummering

Dette scenariet eksemplifiserer at det ligger elektroniske spor på av ulik type på mange ulike steder etter deg i løpet av en dag med reising.

Når det gjelder spor lagt igjen mens du kjører bil er disse av følgende typer:

- Automatisk trafikkontroll, som registrerer kjennemerke og ansikt.
- Bompassering, som registrerer kjennemerke

For mobilsamtaler registreres:

- SIM-kort og enhet
- Hvilket nummer det ringes fra og til
- Samtalens varighet

Taxituren registrerer:

- Lokasjoner, inklusive reisens start og avslutning
- Reisens varighet og pris
- Kanskje også video fra kupeen

Ellers er mye av de elektroniske sporene knyttet til betaling med kort, enten kredittkort eller Bank-Axept. Her registreres:

- Tid for transaksjon
- Ditt kortnummer
- Hvor stor sum som belastes
- Hvor lenge kortet er gyldig
- Sted (terminal) for transaksjon

Er det Bank-Axept som brukes sjekkes det i tillegg:

- Om det er nok penger på konto.

Denne informasjonen er tilgjengelig både der hvor du bruker kortet samt banken du har konto hos eller kredittkortselskapet du er kunde hos.

Når det gjelder biometrisk informasjon i pass så er det mer uavklart. Dette kan lagres i passet/kortet, eller disse dataene kan ligge lagrest sentralt. Den største usikkerheten knytter seg til hvor mye informasjon som blir lagret ved utenlandsk grensepassering.

7.4 Misbruk av elektroniske spor

Det følgende beskriver noen tenkte situasjoner hvor tredjepart bevisst prøver å tilegne seg elektroniske spor og data, for så å misbruke disse. Vi tar ikke stilling til sannsynligheten for at slike situasjoner inntreffer.

7.4.1 Misbruk av trådløse nett

I dette avsnittet kan vi beskrive et tenkt "worstcase scenario" i et åpent trådløst nett, for eksempel i en park, på et sykehus, på en flyplass eller andre steder i det offentlige rom. Her vil du som bruker skaffe deg tidsbegrenset brukeraksess til det åpne trådløse nettet. Du betaler sannsynligvis for og får tildelt brukernavn og passord. Det du nå ikke vet er at en "skurk" sitter i buskene (eller på sykehuset eller flyplassen) i nærheten av deg. Hans signaler er sterkere enn det egentlige trådløse nettet og han imiterer innloggingswebsiden for aksess til det trådløse nettverket. Du blir derved for eksempel lurt til å gi fra deg brukernavn og passord eller trafikken blir omdirigert til andre websider hvor du kan bli lurt til å gi fra deg ulike typer personlig informasjon. Som de fleste skjønner vil imitering av nettbanksider kunne få store konsekvenser, spesielt hvis brukeren ikke oppdager imitasjonen. Dette kalles wireless "phising" eller "WiPhishing".

Svakheten her er autentiseringsprosedyren. På et sykehus eller et legekontor, hvor trådløse nett benyttes, vil konsekvensen i verste fall kunne være at f.eks. pasientdata kommer på avveie dersom autentiseringsprosedyren i et sykehus' trådløse nett inneholder tilsvarende svakheter. Leger, sykepleiere og andre vil bli lurt til å tro at de logger seg inn i sykehusets system, mens noen i nærområdene faktisk imiterer dette. Men dagens praksis med mye håndskrevne notater

har også sine svakheter. Det er bare å komme seg inn på et kontor hvor lapper og skjemaer ligger lett tilgjengelige på skrivebordet.

7.4.2 Misbruk av mobiltelefon og Bluetooth (Blåtann)

Det finnes sikkerhetshull i mobiltelefoner med Bluetooth, og det finnes programmer som utnytter disse sikkerhetshullene for å trenge inn i og kopiere data fra adressebøker i Bluetooth-mobiler. Med et slikt program installert på en bærbar PC, kan "skurken" i mange tilfeller komme seg forbi sperrene i telefonen som skal sikre at data bare byttes mellom telefoner når eierne har godkjent dette.

Dette er spesielt relevant på steder hvor mange mennesker (med Bluetooth telefoner) oppholder seg, for eksempel flyplasser, jernbanestasjoner, kafeer, buss, tog, sykehus og lignende steder. Det er derfor et godt tiltak å slå av Bluetooth funksjonaliteten når den ikke brukes, eventuelt å aktivere "skjult" modus for enheten.

7.4.3 Mobiltelefon og overvåkning av venner

Flere (norske) mobiloperatører har markedsført og (noen har) igangsatt tjenester hvor det er mulig for deg å få se hvor vennene befinner seg geografisk. Dette er også omtalt i kap 5.4.2. Denne typen tjenester har vært omtalt i media fordi abonnenter ikke har vært klar over at de har blitt registrert og i tillegg ikke har vært bevisst på konsekvensen i forhold til personvernet.

En kan tenke seg situasjoner hvor "tyven" er registrert som din venn i tjenesten og kan overvåke dine bevegelser slik at han kan være sikker på at du ikke er hjemme når han gjør innbrudd i hjemmet ditt.

8 Teknologiske løsninger for anonymitet

Anonymitet betyr at en person ikke kan identifiseres. Et spesialtilfelle av anonymitet er pseudonymitet, som betyr at en person over tid opptrer under ett og samme pseudonym, men at dette ikke kan knyttes til personens egentlige identitet. For elektroniske spor innebærer altså dette at det er mulig å avgjøre at sporene er etterlatt av samme person, men ikke hvem denne personen er.

Teknologiske løsninger for anonymitet kan sies å ha forskjellige grader av styrke, avhengig av hvor mye som skal til for å identifisere en person. I noen løsninger er anonymiteten så sterk at det ikke er praktisk gjørbart å identifisere personen, i andre løsninger kreves det at mange av de involverte partene i løsningen er korrupte og samarbeider om å identifisere personen, og i noen løsninger er det tilstrekkelig at bare én part er korrupt.

Vi beskriver her løsninger som har anvendelse generelt, i tillegg til en del løsninger som er mer Internett-orienterte. Ettersom denne rapporten omhandler elektroniske spor begrenser vi oss tilsvarende til elektroniske løsninger for anonymitet.

8.1 Policy-basert anonymitet

Anonymitet kan bevares på to prinsipielt forskjellige måter. Én mulighet er at teknologien i seg selv har iboende begrensninger som hindrer identifikasjon. En annen mulighet er at teknologien ikke har slike begrensninger, men at anonymiteten implementeres ved en anonymitetsbevarende policy for bruk av teknologien. Sistnevnte kan vi kalle policy-basert anonymitet, og denne formen for anonymitet er vesentlig svakere og mer illusorisk enn førstnevnte. Policyen kan endres raskt og usynlig av én tjenestetilbyder slik at anonymiteten ikke bevares, og det er full adgang til å implementere en policy som gjør det mulig å identifisere en person i ettertid.

Ett eksempel på policy-basert anonymitet er anonyme videresendere (anonymous remailers), dvs. e-posttjenester som videresender e-post med identifiserende informasjon fjernet. Et annet eksempel er tjenester som tilbyr web-surfing gjennom en anonymiserende proxy (f.eks. www.anonymizer.com). Brukeren setter opp sin nettleser til å kommunisere gjennom proxyen, som fjerner all informasjon som kan identifisere brukeren. I begge disse tilfellene kan brukeren identifiseres hvis den som administrerer tjenesten er korrupt.

I det følgende vil vi kun beskrive teknologi som har iboende egenskaper som gir anonymitet, slik at det er praktisk ugjørbart å identifisere en person selv om én tjenestetilbyder skulle være korrupt.

8.2 Anonym betaling

Det eksisterer teknologi som muliggjør totalt anonyme elektroniske betalinger. Eksempler er digitale kontanter og forhåndsbetalte småpengekort.

8.2.1 Digitale kontanter

Denne teknologien er basert på et prinsipp kalt "blinde digitale signaturer". En blind digital signatur virker nøyaktig som en vanlig digital signatur, med den forskjell at den som signerer ikke kan se hva det er han signerer. Dette kan utnyttes til å lage digitale kontanter ved at selve signaturen tilordnes en pengeverdi, slik at det som enn er signert med denne signaturen har den tilordnede pengeverdien. En bruker kan dermed få banken til å blindsignere en melding med en gitt valør samtidig som kontoen debiteres med det samme beløpet. På et senere tidspunkt kan meldingen brukes som kontant betaling. Betalingsmottakeren kan deretter levere meldingen til banken og få oppgjøret. Dette systemet forutsetter et kontrollsystem for å hindre at samme melding blir brukt som betaling flere ganger, men dette er fullt mulig å integrere uten å bryte anonymiteten.

Digitale kontanter som bruker dette prinsippet gir full anonymitet selv om pengeutsteder og betalingsmottaker samarbeider om å prøve å identifisere betaleren. Det er mulig å implementere digitale kontanter både til bruk på Internett og i betalingsterminaler.

8.2.2 Forhåndsbetalte småpengekort

Forhåndsbetalte småpengekort er kort eller lignende som kjøpes for et kontant beløp, og som deretter kan brukes til betaling i spesielle terminaler. Disse kortene er usporbare så lenge de er betalt med kontanter. Følgende er eksempler:

- **Telekort**: Man kjøper et kort kontant og kan bruke dette til å ringe fra telefonkiosker.

- **Anonyme klippekort til bomstasjoner**: Noen bompengeanlegg tilbyr en kontant betalt bombrikke som kan brukes til et pålydende antall passeringer gjennom disse bomstasjonene.

- **Anonyme elektroniske kollektivkort**: Noen kollektivselskaper tilbyr kontant betalte elektroniske klippekort.

8.3 Anonym telefoni

Mobiltelefoner med uregistrerte kontantkort gjør det mulig å ringe pseudonymt. Det vil fremgå at samtalene kommer fra samme nummer, men det er ikke mulig å knytte dette telefonnummeret til en bestemt person. Denne type kontantkort var tidligere tilgjengelig i Norge, men selges nå ikke lenger. Ellers er det mulig å ringe helt anonymt fra telefonkiosker som tar kontanter eller telekort.

8.4 Anonym passering av bomstasjon

Noen typer av bompengeanlegg tilbyr forhåndsbetalte anonyme klippekort.

8.5 Anonym kommunikasjon over Internett med kjent mottaker

8.5.1 Mix-nett – usporbar anonym elektronisk post

Mix-nett gjør det mulig å sende elektroniske meldinger med anonym avsender. Prinsippet er at avsenderen sender meldingen til en spesiell tjeneste kalt en "mix" som videresender meldingen til adressaten i en annen konvolutt. Meldingene som sendes både til og fra mixen er kryptografisk beskyttet mot manipulasjon og innsyn. For å vanskeliggjøre korrelasjon ved trafikkanalyse kan meldingene fra mixen ha fått endret sin størrelse og være stokket om. Istedenfor bare én mix brukes kaskader (kjeder) av flere mixer, og det kan eksistere et helt nettverk av mixer, altså et mix-nett. For å identifisere avsenderen av en melding er det dermed nødvendig å kompromittere samtlige mixer i kaskaden.

Denne grunnleggende modellen kan også utvides på flere måter. Det er lett å legge til mulighet for mottageren å svare på en melding uten å vite den første avsenderens identitet. Det er også mulig å opprette lister over digitale pseudonymer for en gitt organisasjon, slik at et individ kan kommunisere med denne organisasjon under et fast pseudonym. Dette kan gjøres på en slik måte at et individ ikke kan opptre under andre pseudonymer overfor samme organisasjon, men at organisasjonen heller ikke kan finne ut individets identitet.

8.5.2 Onion routing

Prinsippet for mix-nett kan også anvendes på nettverksnivå (OSI lag 3), og kalles da "onion routing". Onion routing kan gjøres helt uavhengig av applikasjonene og gir anonymitet begge veier.

8.5.3 Web-mixer

Prinsippet for mix-nett kan også anvendes på web-kommunikasjon, og kalles da web-mixer.

8.5.4 Crowds

En hop ("crowd") tillater anonym web-lesing ved å la brukeren "forsvinne i den store hopen". En hop et laget som et nettverk av maskiner der hver maskin enten kan være avsenderen av en forespørsel eller den kan være en mellommaskin som bare viderebringer en forespørsel fra en

annen maskin. Når en maskin kobler seg opp mot en web-tjener opprettes en tilfeldig rute gjennom et antall deltagende maskiner i hopen. Alle forespørsler etter dette blir sendt gjennom den samme ruten. Dette resulterer i to viktige egenskaper: For det første ser web-tjeneren bare en forespørsel som kommer fra en tilfeldig maskin i hopen. For det andre vet ikke en maskin som viderebringer en forespørsel om den ble levert direkte fra avsenderen eller fra en maskin som bare viderebrakte den. Med andre ord kan avsenderen ikke identifiseres bare på basis av trafikkinformasjon.

8.6 Anonym kringkastning av data over Internett

Et kringkastningsnett er et nettverk som formidler data fra hver avsender til samtlige deltagere i nettet.

Et DC-nett er en type nettverk som gir usporbar anonymitet for alle avsendere og mottakere i nettet. I prinsippet virker nettet som et kringkastningsnett der alle kan sende og lytte på meldinger uten at avsenderen av en melding kan identifiseres.

XOR-trær er et eksempel på en annen type anonyme kringkastningsnett. Egenskapene ligner DC-nett, men den tekniske virkemåten er forskjellig.

9 Utviklingstendenser og trender

Elektroniske spor legges i stort omfang igjen på et stort antall steder. Formålet med denne delen av dokumentet er å vise utviklingstrekk. Hvordan har mengden, karakteristika og utbredelsen av elektroniske spor forandret seg i nær fortid? Hva er utviklingstendenser i dag og hvordan kan vi forvente denne utviklingen vil fortsette i de neste årene? Ulemper og fordeler med ulike utviklinger er ikke vurdert i særlig grad. Vi vil beskrive antatte utviklingstrekk for IKT baserte systemer og utviklingen innen elektroniske spor.

9.1 Kvantitativ utvikling

En kan vente at mengden av elektroniske spor som legges igjen i samfunnet vil øke markant de nærmeste årene. Situasjoner som før ikke etterlot noen spor når de ikke understøttes av teknologi etterlater nå elektroniske spor. Dette er en utvikling som kommer å fortsette når flere og flere situasjoner i samfunnet blir mer og mer brassert på teknologi. For eksempel;

- Bruk av kontanter er anonymt etterlater seg ikke spor, mens bruk av kredittkort etterlater elektroniske spor.
- Bruk av vanlige nøkler etterlater ikke spor, mens bruk av adgangskort etterlater elektroniske spor.

60% av norske husholdninger hadde tilgang til Internett i 2004. Halvparten av disse hadde bredbåndstilknytning [24]. Tendensen er at antall personer med Internettilgang i hjemmet fortsatt er økende. Med bredbånd lettes tilgangen til Internett sammenliknet med tregere tilkobling. Bredbåndbrukere er oftere på nettet enn de uten. Det er derfor antatt at en økning av antall

[24] SSB, *IKT i husholdningene*, 2004 http://www.ssb.no/emner/10/03/ikthus/ (2004)

bredbåndsbrukere vil øke antall transaksjoner på Internett. Det er fortsatt en tung satsing på bredbåndutbygging og vi kan forvente at andelen av husstander med brede linjer vil øke i årene som kommer. Det siste er et utalt mål fra norske myndigheter [25]. Siden antall elektroniske spor øker med stigende bruk av elektroniske tjenester vil altså mengden elektroniske spor fortsatt øke betydelig, spesielt i tilknytning til bruk av Internett.

9.2 Konvergens av tjenester

Det er tendens til at elektroniske tjenester samles på en leverandør, jf. Min side [26], der det offentlige Norge skal tilby sine tjenester under én portal. Dette fører til oppsamling av elektroniske spor og mulighet for å binde sammen spor som er fra samme person. Samtidig vil innlogging på en slik tjeneste medføre at identitet og IP adresse kan kobles. Det fører til at senere bruk er løst koblet til denne identiteten så lenge IP adressen er det samme. Stadig billigere lagringskapasitet gir større lagringsplass som gjør at en større mengde elektroniske spor også kan lagres. Økt prosesseringskapasitet gjør at flere og mer sammensatte elektroniske spor kan behandles. Eksempler er automatisk bilnummerskiltgjenkjenning fra videobasert trafikkovervåkning.

Samling av tjenester er ikke designet for å generere flere spor men fører til dette ved at personinformasjon vil legges igjen oftere og på stadig nye tjenester.

Det forbindes med plunder å stadig logge seg inn på nettjenester. Derfor gjøres innlogging først når man trenger det. I nettbutikker trenger man foreksempel ikke logge seg inn før man skal betale. Med nettbutikken som en av et knippe tjenester i en portal vil engangsautentisering senke terskelen for autentisering og man risikerer å være autentisert ved utføringer av tjenester som egentlig ikke krever det.

9.3 Distribuert intelligens i nettet

Med fremveksten av bredbånd i private hjem har rutere etc. kommet inn i hjemmene til sluttbrukerne. Kabelmodemer har fått mer og mer intelligens innbygget og det er mulig for nettleverandøren å kontakte modemet i forbindelse med f.eks. feilsøking. Det samme gjelder koblingsbokser for kabel TV og telefoni. Det er uklart hvilken og hvor mye informasjon som lagres i disse ruterne, modemene eller koblingsbokser men man må forvente at potensialet for å logge informasjon vil øke med tiden. Om brannmurer legges i disse aksesspunktene vil det være ønskelig å legge inn en loggingsfunksjonalitet med de konsekvenser det vil ha med hensyn på distribuering av spor. Dekodere for kabel TV kan også tenkes å få funksjonalitet som gjør det i teorien mulig for utenforstående å finne ut hvilke programmer en husholdning ser. Mange moderne TV-er eller dekodere husker allerede sist sette programvalg.

9.4 Teknologikonvergens

Med stadig mer funksjonalitet bygget inn i mobiltelefoner og PC-er, som for eksempel GPS posisjonering, vil potensialet for mer informasjonsrike spor øke. I nye biler blir det stadig mer utbredt med GPS navigasjonssystemer. Koblet opp mot lokasjonsbaserte tjenester vil dette føre til en spredning av lokasjonskoblede elektroniske spor. Lokasjonsbaserte tjenester har ikke tatt av ennå men dette avhenger av teknologier som antagelig vil komme.

---

[25] Samferdselsdepartementet, *Bredbånd til hele landet – forslag til nasjonal satsing*, Rapport, http://odin.dep.no/sd/norsk/publ/rapporter/028021-220002/index-dok000-b-n-a.html, (2000)

[26] Moderniseringsdepartementet, *Versjon én av "Min Side" kommer allerede i juni 2005*, pressemelding, http://odin.dep.no/mod/norsk/aktuelt/pressesenter/pressem/050001-070033/dok-bn.html (2005)

9.5 Vekst i elektroniske betalingsmåter

Nordmenn ligger i verdenstoppen når det gjelder betaling med kort. I motsetning til kontant betaling legges det igjen elektroniske spor når man betaler en vare med et bankkort. Derfor vil en videre overgang fra kontant betaling til betaling med bankkort medføre en økning av etterlatte elektroniske spor. Det er også en økende tendens til at små kjøp (under 200,- kr) gjøres ved hjelp av bankkort i tillegg til ordinær betaling av varer i butikker. Eksempelvis betaling av parkeringsavgift i automater. Man ser også en generell økning av handel over Internett og knyttet til mobil telefoni.

Ved reising med kollektivtransportmidler vil det i nær fremtid bli mer og mer bruk av elektroniske billetter.

Ser man lengre frem i tid kan det hende at bruk av tradisjonelle bankkort ved betaling vil kunne overtas av anonyme digitale penger. Det kan tenkes at mengden identifiserbare digitale spor kan reduseres noe som følge av anonym elektronisk betaling. En slik reduksjon er ikke helt usannsynlig hvis anonym betaling kombineres med DRM teknologi som tillater anonyme kjøp. Da kan en tjeneste som selger digitale varer (lyd, bilde, programmer etc.) beskytte sine produkter mot misbruk og få betalt med elektroniske kontanter - samtidig som brukerne kan være anonyme eller pseudonyme overfor tjenestetilbyderen.

9.6 Trådløse teknologier

Ved bruk av trådløse teknologier vil potensialet for legal og illegal sporinnsamling øke. Vi kan forvente en ganske kraftig vekst i bruk av trådløs teknologi for datakommunikasjon i nærmeste framtid. Denne veksten vil komme i næringslivet, konsumentsegmentet og i helsevesenet. Når 3G mobiltelefoni kommer for fullt vil veksten i bruk av trådløs teknologi øke enda mer. Noen år frem kommer vi også til å få UWB som arvtager til blåtann. Personlige lokale nettverk med båndbredde i underkant av en halv Gbit/sek. Denne teknologien tenkes brukt i hjemmeunderholdning som digital-TV og trådløs overføring av musikk.

9.7 Fysiske sporinnsamlingsteknologier

Med fysiske sporinnsamlingsteknologier menes teknologier som samler inn spor direkte fra den virkelige verden. Eksempler på dette er videoovervåkning og irisskanning.

9.7.1 GPS sporing og sorte bokser

Drosjer og tungtransport blir allerede i dag sporet mer eller mindre kontinuerlig ved hjelp av GPS. Ved hjelp av trådløs overføring av data kan sentraler følge med hvor de forskjellige enhetene er. I tillegg lagres kjøredata som posisjon og fart i sorte bokser. I fremtiden kan det også bli pålagt å ha sorte bokser i privatbiler. Sporene som legges igjen vil være i bilen og derfor under bileiers kontroll så lenge han fortsatt er eier av bilen. Så snart han selger bilen vil han miste kontrollen hvis boksen følger bil og ikke eier.

9.7.2 Sporing av varer / post

Sporingsteknologier som RFID muliggjør sporing av for eksempel matvarer fra produksjonsledd via foredlingsledd helt til konsumenten kjøper varen. Ved sporing av varer spores ikke bare varen men også den som transporterer eller behandler varen. Ettersom denne type teknologi har et betydelig element av risikoreduksjon i seg bør en forvente ad bruken øker betraktelig over de nærmeste år.

9.7.3 Videoovervåking

Flere vil installere overvåkningsutstyr i butikker og bedrifter etter hvert som prisen på slikt utstyr ventes å falle i årene som kommer. Det er tenkelig at det med ny teknologi blir mulig å identifisere personer automatisk fra videomateriale. I avsnittet om biometri under beskrives blant annet tenkte metoder for å gjøre slik identifikasjon.

Det utplasseres digitale kameraer i automatiske trafikkontrollbokser langs veiene i Norge[27]. Flere biler vil derfor fotograferes. TØI tenker seg at man i fremtiden også ønsker å måle bilers gjennomsnittshastighet over større avstander. Dette krever at passerende biler blir automatisk identifisert og informasjon om passeringen lagres. Teknologi for automatisk lesing av bilnumre finnes. For hver passering må denne informasjonen sendes til en sentral enhet for å regne ut snitthastigheten. Bilder av alle kontrollerte biler må også lagres for å sikre bevis. Videre kan man tenke at den samme teknologien kan brukes ved innganger til parkeringshus. Sporene som genereres vil kunne være bl.a. bilnummer, hastighet og bilde av bilfører og bil.

9.7.4 Biometri

Hvert menneske har et unikt fingeravtrykk. Dette kan brukes til å identifisere mennesker. Annen biometrisk informasjon, som foreksempel irismønster, kan også brukes til dette formålet. I tillegg til å kunne identifisere et menneske kan også mange biometriske egenskaper fortelle noe om selve personen og ikke bare identifisere vedkommende. Mens det er lite man kan lese ut fra et fingeravtrykk, så forteller et DNA spor svært mye om personen det kommer fra. Biometri er nevnt tidligere, men dette er primært en teknologi for fremtiden. De ulike typer biometri som er i praktisk bruk eller undersøkes er stort sett de følgende:

- Ansiktsgjenkjenning består av to deler: Deteksjon av ansikter i et bilde og kobling av dette til en person. Den første delen er enklest av disse to og det finnes allerede teknologier som gjør dette med høy presisjon. Denne teknologien ligger litt frem i fremtiden men vil komme.
- Geometriske mål; vekt, høyde, etc er ikke egnet alene til å identifisere personer i en stor befolkningsgruppe men i mindre avgrensede grupper eller sammenstilt med andre identifiserende metoder kan slik informasjon være med på å identifisere personer.
- Fingeravtrykk / håndgeometri. Bruk av fingeravtrykk har inntil nylig vært forebehold påtalemakten. Med ny teknologi er det åpnet for at flere kan bruke fingeravtrykk for identifisering ve foreksempel adgangskontroll til bygninger eller utstyr.
- Iris-/ retinaidentifikasjon. I de Olympiske Leker i Nagano Japan benyttet man Iris identifikasjon av skiskytingsutøvere før de fikk adgang til våpnene. Teknologien er allerede tilstede men på grunn av problemer med blant annet brukervennlighet kan man ikke forvente at den kommer til å komme i utstrakt bruk i årene som kommer.
- DNA spor. Denne teknologien brukes allerede ved etterforskning av forbrytelser og i forskning. Resultatene fra DNA-tester lagres elektronisk. Stadig flere tar i bruk DNA-tester, det være seg organisasjoner som banker og private. Billigere og mer effektive analysemetoder kan åpne opp for innsamling og analyse av DNA spor av flere aktører enn bare påtalemakten. Man kan for under 1000 kr kjøpe DNA-tester på Internett til personlig bruk.
  På Island har man opprettet et register som inneholder alle gener til Islands befolkning. Et medisinsk firma kjøpt rettighetene til å koble DNA data fra dette registeret til

[27] Ravlum, I-A., *Makt, beslutning og integritet - IKT og personvern i transport*, http://www.toi.no/attach/a516676r712780/703_2004.pdf, (2004)

sentrale helseregistre.
Med såkalte DNA-mikromatriser kan man analysere DNA materiale med en meget stor nøyaktighet. Denne teknologien er foreløpig kostbar og krever høy ekspertise for å betjene. Men med tiden kan man forvente at tilgjengeligheten til slik teknologi vil øke.

- Sensorer for innsamling av foreksempel DNA spor og fingeravtrykk inngår i samlebegrepet biosensorer. Det er kun fantasien som legger grenser for hvilke sensorer man kan få i fremtiden. Teknologi for elektronisk måling blodsukker er allerede i bruk av pasienter med sukkersyke. Det gjøres feltforsøk i prosjektet Wireless Health and Care (WsHC) [28] der data fra blodsukkermålinger sendes via mobiltelefon til lege. Målet med WsHC er å få opp et spekter av elektroniske trådløse tjenester på norske sykehus. Teknologi for elektronisk måling av blodtrykk har allerede vært tilgjengelig i flere tiår. Det nye nå er at dataene skal kunne lagres og hentes opp trådløst av autorisert personale.
- De fleste av oss kan høre hvem som kommer gående hvis det dreier seg om en person som en kjenner godt. På avstand kan man også ofte se hvem som kommer bare ved å se på ganglaget. Selv om at det er tenkelig at man kan utvikle teknologi som kan identifisere personer på ganglaget virker det som at det kan ta lang tid før man kan komme dit.
- Hvordan man bruker et tastatur til en datamaskin varierer fra person til person. Det er mulig å skille forskjellige brukere av en datamaskin fra hverandre ved å analysere hvordan man bruker tastaturet på en datamaskin. En slik analyse kan brukes for å detektere uautorisert bruk av datamaskiner.
- Stemmeidentifikasjon. De fleste kjenner igjen stemmen til familie, venner og kolleger og kan avgjøre hvem de snakker med uten å vedkommende har sagt hvem han/hun er. Elektronisk stemmegjenkjenning er under stadig utvikling. Teknologi kan for eksempel brukes til å effektivisere serviceavdelingen til et firma ved at man vet hvem som ringer ved å sammenlikne med tidligere telefonsamtaler og annen samtale informasjon. Resultatet er at man kan registrere navn på innringer uten at vedkommende trenger å presentere seg.
- Håndskrift / signatur gjenkjenning.

9.7.5 Oppsummering

Det er ikke lett å spå om fremtiden men om utviklingen fortsetter som den har gjort opp til i dag er det likevel mulig å kjøre kvalifiserte gjetninger om hvilke utviklingstrekk man kan vente seg. Det vil være en øking av steder / situasjoner der elektroniske spor vil samles, flere typer elektroniske spor vil bli generert og sporene vil være i økende grad være direkte koblet til identiteten til sporkilden.

[28] *Wireless health and care*, prosjekt, http://www.wshc.no/index.php