Elektroniske spor og personvern

Rapport 1 – 2005

Elektroniske spor og personvern

ISBN 82-92447-05-9

Utgitt: Oslo, mars 2005
Omslag: Enzo Finger Design AS
Trykk: ILAS Grafisk

Elektronisk publisert på: www.teknologiradet.no

Innholdsfortegnelse **side**

Forord

I gamle dager var det allment kjent at damene på "sentralen" kunne lytte på private telefonsamtaler. Det var ikke tillatt, men like fullt skjedde det. Dagens "sentralborddamer" er store databaser og datamaskiner med enorm prosesseringskapasitet. De inneholder mengder av informasjon om hvilke nettsteder som besøkes, når og hvor lenge, hvilke søkeord som er brukt i søkemotorer og hva kunder har kjøpt på internett.

I motsetning til før i tiden er mange ikke klar over at det er noen som kan "spionere" på dem. Sporene de legger igjen er skjulte, det samme er prosesseringen, og prosessen er automatisert slik at en enorm mengde personprofiler kan håndteres til enhver tid.

I denne rapporten fra Teknologirådets prosjekt *IKT og personvern* viser vi hvordan dagens og morgendagens teknologi endrer betingelsene for personvernet. I tillegg beskrives også annen utvikling i samfunnet som er viktig for personvernet.

Teknologirådet jobber prosjektbasert. Det vil si at vi involverer nye ressurspersoner for hvert nytt tema vi tar opp. Bak denne rapporten står en ekspertgruppe med kompetanse på en rekke fagområder, blant annet jus, personvern, antropologi/arbeidslivsstudier og elektronikk. I tillegg har andre viktige aktører og eksperter blitt involvert gjennom en åpen høring. Ekspertgruppen har hatt følgende medlemmer:

Ann-Kristin Olsen – Fylkesmann i Vest-Agder
Tian Sørhaug – Senter for Teknologi, Innovasjon og Kultur (TIK)
Einar J. Aas – NTNU
Ben Johnsen – Universitetet i Tromsø
Lee A. Bygrave – Universitetet i Oslo
Andreas Wiese – Dagbladet
Einar Snekkenes – Høgskolen i Gjøvik
Inger Marie Sunde – Politiets Datakrimsenter, Økokrim

Arbeidet har vært ledet av Teknologirådets prosjektleder Erlend Jakobsen. Fra 01.01.05 har Christine Hafskjold hatt ansvaret for prosjektet.

Resultatene av Teknologirådets arbeid skal formidles til Stortinget, øvrige myndigheter og samfunnet generelt. Vi tror denne rapporten har verdifulle innsikter for alle disse målgruppene

Tore Tennøe
Sekretariatsleder, Teknologirådet

Sammendrag

De senere årene har det vært en enorm utvikling innen IKT og relaterte områder som e-handel, digitalisering av offentlig sektor og oppfølging av trusler mot samfunnssikkerheten. Teknologier som internett og mobiltelefoni har en enorm utbredelse, og vi ser at teknologier som RFID og biometri er i ferd med å gjøre sitt inntog også i konsumentmarkedet. Dette er teknologier som etterlater en stor mengde spor etter brukeren.

Også tidligere tiders teknologier, som gammeldagse sentralbord, muliggjorde overvåkning av enkeltpersoner. Det som er fundamentalt nytt med dagens situasjon er at sporene er digitale, de etterlates ofte uten av vi er klar over det, og de kan lagres og bearbeides på en helt annen måte enn tidligere. Dette åpner for økt overvåkning både fra myndighetene og kommersielle aktører.

Personvern – fundamental rett som stadig veies mot andre hensyn

Personvernbegrepet forbindes primært med beskyttelse av individets integritet. Autonomi (suverenitet) og privatliv er også grunnleggende verdier som forutsetter et personvern. Ivaretakelse av personvernet handler om å sikre den enkeltes frihet til selv å velge hvordan hun vil leve sitt liv og i hovedsak selv å kunne definere grensene for hva som tilhører det private. Personvernet stiller også krav til kvaliteten på de opplysninger om enkeltpersoner som legges til grunn for beslutningsprosesser, og til at sterke parter ikke må misbruke sin kunnskap om den enkelte til å øve utilbørlig press.

Personvernet er en fundamental menneskerett som i stor grad er anerkjent på tvers av kulturer og regioner. Det som gjør beskyttelsen av personvernet så vanskelig er at det ikke kan gjelde absolutt, men alltid må veies mot andre hensyn, som for eksempel åpenhet, effektivitet eller sikkerhet.

Holdninger hos folk flest

Teknologirådets fokusgruppeundersøkelse fra våren 2004 viser at folk flest i praksis ikke er så flinke til å beskytte eget personvern. Undersøkelsen viser at kunnskapsnivået om elektroniske spor blant vanlige brukere er lav. De fleste mener at personvern er en viktig sak, men oppgir gjerne personopplysninger mot å få gratis tjenester som ringetoner og spill, og er lite villige til å bruke tid på å sette seg inn i hva de kan gjøre for å beskytte personvernet bedre. Personvernet prioriteres i praksis lavere enn effektive tjenester og hensynet til kriminalitetsbekjempelse. Samtidig har de fleste stor tillit til at myndighetene og store private selskaper sørger for å ivareta brukernes personvern slik at de ikke selv trenger å bekymre seg.

Et viktig aspekt er den reelle muligheten til å si nei til overvåkning. Vil det være sosialt akseptert å nekte å la seg overvåke av ektefelle eller arbeidsgiver, for eksempel gjennom en posisjoneringstjeneste? Gjennom økt fokus på samfunnssikkerhet, og stadig mer begrensninger på anonyme tjenester, risikerer vi at det å ville ivareta personvernet sitt blir betraktet som noe mistenkelig.

Elektronisk ID og biometri skaper nye utfordringer

For å kunne holde individer ansvarlige for sine handlinger må det være mulig å identifisere dem. For å ivareta den enkeltes personvern og personlige sikkerhet er det derimot nødvendig å forhindre unødig identifikasjon. Nøkkelen til hvilke konsekvenser elektroniske spor har for personvernet, ligger i hvilken grad av personidentifikasjon som er knyttet til sporene. Full anonymitet er et ytterpunkt på en skala hvor full verifisert identifikasjon utgjør det andre ytterpunktet. Alt mellom disse ytterpunktene kalles pseudonymitet og innebærer at brukeren opptrer under pseudonym, gjerne i form av en digital identitet.

Mens anonymitet fortsatt har sin berettigelse på mange områder og full identifikasjon er nødvendig i enkelte sammenhenger, er det i informasjonssamfunnet som oftest mest hensiktsmessig at elektroniske spor er beskyttet under en form for pseudonymitet. Da kan de ikke så enkelt knyttes til en person og faren for misbruk er dermed langt mindre. Samtidig vil det da være mulig for politiet, fortrinnsvis etter en rettskjennelse, å identifisere brukeren hvis hun har gjort noe hun må stilles til ansvar for.

Autentisering innebærer å verifisere at en bruker er den hun gir seg ut for å være. Det er bekymringsverdig at mye personlig informasjon etterspørres i autentiseringsprosesser, enda det sjelden er nødvendig. I forhold til personvern er det viktig at autentiseringsgraden er tilpasset formålet. For eksempel: Dersom en blir bedt om å bevise at en er gammel nok til å kjøpe et produkt eller en tjeneste i den virkelige verden, vil man vise legitimasjon i form av bankkort, pass eller førerkort. Selv om en da viser frem mer informasjon enn strengt tatt nødvendig, er det usannsynlig at kontrolløren vil huske informasjonen. Når man gir fra seg overflødig informasjon i den digitale verden, lagres dette, og det kan senere brukes til andre formål.

For å verifisere en brukers identitet baserer man seg på noe hun *vet* (eks. passord eller PIN-kode), noe hun *har* (eks. legitimasjon eller smartkort) eller noe hun *er* (biometri). Biometri er et teknologiområde knyttet til identifikasjon av individer ved avlesning av kroppens unike biologiske kjennetegn. Typiske eksempler er gjenkjenning av fingeravtrykk eller iris. Biometriske løsninger er generelt bedre egnet til autentisering enn til identifikasjon. Det anbefales at biometriske data lagres lokalt, ettersom dette gir bedre sikkerhet mot misbruk. Dette er spesielt viktig fordi biometrisk informasjon ikke kan endres når den er blitt kompromittert, slik for eksempel et passord eller en PIN-kode kan.

Når vi får identifiseringsløsninger som er lette å bruke, som elektronisk ID og biometri, kan det bli fristende å bruke denne identifiseringen i flere sammenhenger, også der sterk identifisering ikke er nødvendig.

Elektroniske spor

Elektroniske spor kan være alt fra digitale ”fotavtrykk” som forteller hvem som har vært et sted til en gitt tid, til detaljerte personopplysninger man legger fra seg på et nettsted. Transaksjoner med betalingskort og i nettbanken, passeringer i bomring med Autopass-brikke og bruk av adgangskort på jobben er klassiske eksempler på elektroniske spor. I rapporten ser vi nærmere på en del utbredte teknologier hvor det settes til dels store mengder elektroniske spor

Kommunikasjonsdata – innholdsrike elektroniske spor
Kommunikasjonsdata fra elektronisk kommunikasjon omfatter tre typer av informasjon: *Trafikkdata* forteller hvem som har kommunisert med hvem og på hvilke tidspunkt, *lokasjonsdata* er informasjon om hvor partene befant seg geografisk under kommunikasjonen og *innholdsdata* er det som ble kommunisert. Slike spor etterlates ikke bare ved bruk av telefonitjenester, men også ved bruk av andre elektroniske kommunikasjonstjenester som e-post, chat og internett. Nettopp bruk av tjenester som e-post og internett etterlater spesielt mange og innholdsrike elektroniske spor. En ukryptert e-post kan sammenlignes med et postkort, og kan leses av administratorer og driftspersonell med tilgang til de serverne e-posten er innom. E-post kan også relativt lett fanges opp og leses av utenforstående.

Ved bruk av tjenester på nettet vil PC-ens IP-adresse, sammen med informasjonskapsler (cookies) som lagres på brukerens egen PC, bidra til å identifisere brukeren overfor nettsteder og tjenesteleverandører. Dette innebærer at man ikke er fullstendig anonym på internett, samtidig som det gjør det mulig for nettsteder å etablere personprofiler med data som samles inn over tid.

Lokasjonsteknologi avslører brukerens posisjon
Teknologi som enten kan posisjonsbestemme brukere nøyaktig eller som kan beregne en omtrentlig geografisk plassering kalles lokasjonsteknologier. I mobilnettverk kan brukeren posisjoneres med noen hundre meters nøyaktighet. Langt større nøyaktighet i utendørs posisjoner oppnås ved bruk av et satellittnettverk som GPS.

Tjenester som tilbys på bakgrunn av hvor brukeren befinner seg (lokasjon) er det vi kaller lokasjonsbaserte tjenester. Typiske bruksområder i dag er navigasjonssystemer, trafikktjenester, informasjonstjenester, flåtestyring og nødassistanse. I et økende antall sammenhenger kan brukere etterlate seg elektroniske spor med nøyaktig posisjonsinformasjon.

RFID er små brikker som identifiserer de gjenstander de er festet til gjennom utsendelse av radiobølger. Slike brukes i dag til å effektivisere vareflyt og lagerhåndtering innen vareproduksjon og i transportsektoren. Merking av sluttprodukter i varehandelen er et område hvor det forventes store utfordringer knyttet til personvernet. I den grad disse brikkene forblir funksjonelle også etter at kunden forlater butikken, oppstår en fare for at informasjonen på RFID-brikken kan misbrukes til andre formål. Ved bruk av unike ID-numre for hver brikke kan det bli for lett å knytte en RFID-utstyrt vare til kjøperens identitet, og slik spore kjøperen.

Sikkerhet på hjemme-PC – også et spørsmål om personvern
En utfordring som er knyttet spesielt til private PC-er er mangelfull sikring mot eksterne trusler som kan kompromittere brukernes personvern. Både tekniske tiltak og hensiktsmessig brukeratferd er nødvendig for å beskytte seg mot de tallrike trusler internettet kan by på. Virus og ormer er den form for trussel som er best kjent blant folk flest. E-postbaserte svindelforsøk (*phishing*) og spionprogrammer (*spyware*) er derimot de truslene som nå øker mest i omfang, og disse har gjerne et større potensiale til grove overtramp mot brukerens personvern enn et virus. Uønsket e-postreklame (*spam*) oppfattes av mange som et personvernbrudd og er problematisk også fordi slik post brukes som middel til phishing og til spredning av ondsinnet programvare.

Sikkerhetsproblemer på folks hjemme-PC blir enda mer akutte i en situasjon hvor så mange går til anskaffelse av bredbåndstilknytning til internett. Med bredbånd er forbindelsen til nettet stort sett alltid oppe, noe som åpner muligheten for hackere til å bryte seg inn på dårlig sikrede PC-er. Hackere kan skaffe seg tilgang til sensitive data på offerets PC, men de kan også bruke den til å gjennomføre andre kriminelle handlinger. Aller mest utsatt er de som i tillegg til bredbånd installerer et trådløst nettverk i hjemmet uten å sikre dette tilstrekkelig mot avlytting og tjuvlån. Ulempen med trådløse nettverk er at signalene rekker langt utenfor husets vegger og at usikrede signaler relativt enkelt kan fanges opp og utnyttes av folk på utsiden.

Samfunnssikkerhet og overvåkning – vanskelig balansegang

Billige og tilgjengelige kommunikasjonsmidler har bidratt til økt aksjonsradius for enkelt-individet og økt potensiale for mindre grupper til å påføre samfunnet stor skade. Etter terrorangrepene i USA i 2001 og i Spania i 2004 er folk mer opptatt enn tidligere av at myndighetene treffer de tiltak som er nødvendige innenfor rimelighetens grenser for å forhindre terrorangrep.

Det er et faktum at også kriminelle gjør bruk av elektroniske kommunikasjonsmidler og etterlater seg elektroniske spor som kan utnyttes til å etterforske kriminelle handlinger og til å avverge alvorlig kriminalitet. Politimetodeutvalget foreslo i 2004 å gi politiet utvidet adgang til å bruke IKT-relaterte metoder som teknisk sporing (peiling av bevegelser), kommunikasjonskontroll (avlytting) og dataavlesning. Utvalget foreslår også lagringsplikt for trafikk- og lokasjonsdata fra elektronisk kommunikasjon. Dette er et mindre invaderende tiltak enn de andre, men om det skulle bli vedtatt vil det på den annen side omfatte absolutt alle IKT-brukere og således representere en betydelig økning av overvåkningsnivået i samfunnet.

Utenlandske etterretningsorganisasjoner driver en omfattende avlytting og datainnsamling fra elektronisk kommunikasjon i mange land. Den såkalte UKUSA-alliansen driver systemet Echelon som antas å være det mest omfattende og ambisiøse av slike etterretnings-systemer. Problemet med dette systemet er at det opererer utenfor den normale juridiske og politiske kontroll, og at det kan medføre ubegrunnede mistanker mot vanlige mennesker.

Teknologistøttet personvern – for vanskelig for folk flest

Det er knyttet betydelig håp til at personvernteknologier etter hvert vil kunne motvirke tendensen til at ny IKT i så stor grad bidrar til å svekke det faktiske personvernet. Allerede finnes teknologier som kan brukes til å redusere mengden av identifiserbare elektroniske spor, sikre kommunikasjon og informasjon ved hjelp av kryptering og sikre informasjons-systemer og PC-er mot innbrudd og uautorisert tilgang. Teknologier som bidrar direkte til å sikre personvernhensyn kalles gjerne personvernøkende teknologier, mens personvern-vennlige teknologier lar brukeren selv bestemme hvor streng beskyttelse av egne person-opplysninger hun ønsker.

Viktige personvernøkende teknologiområder er anonymiseringsteknologi, krypterings-teknologi og teknologier innen informasjonssikkerhet. Personvernvennlige teknologier omfatter blant annet innbygging av personvernregler i informasjonssystemer samt systemer for teknologistøttet identitetshåndtering. Rene personvernteknologier har så langt ikke hatt særlig suksess i markedet. En av hovedgrunnene til dette kan være at vanlige

brukere er lite bevisste på behovet for slike teknologier, og lite villige til at bruke ressurser for å beskytte sine personopplysninger bedre.

Anbefalinger

Vi har sett at personvernet er under press som følge av en rivende teknologiutvikling som medfører stadig økende sporbarhet. I tillegg er det lav bevissthet omkring personvern hos folk flest, og teknologier for å beskytte personvernet er lite tilgjengelige.

For at personvernet skal overleve den kontinuerlige strømmen av nye informasjons- og kommunikasjonsteknologier må myndigheter og beslutningstakere vite hvordan man kan vurdere konsekvensene av nye teknologier. Disse utfordringene løses ikke først og fremst gjennom lovreguleringer, men gjennom fokus på hvilke valg som kan gjøres når teknologiene skal implementeres i systemer og tas i bruk. Når nye teknologier lover fordeler som automatisering, økt effektivitet eller enkelhet for brukerne, må disse hensynene veies mot hensynet til den enkeltes personvern. Følgende overordnede prinsipper for ivaretakelse av personvern bør følges:

1. Brukere av IKT-tjenester må identifiseres på et nivå som er tilpasset tjenestens behov. Er det ikke strengt nødvendig å vite hvem brukeren er, bør man heller ikke autentisere på individnivå, men la brukerne opptre anonymt eller under pseudonym.

2. Innsamlede data og elektroniske spor må sikres mot unødig innsyn eller spredning. Kun den som har et tjenestlig behov for å bruke slike data bør få tilgang til dem.

3. Man må være restriktiv i forhold til å tillate at innsamlede data blir brukt til andre formål enn de ble samlet inn for.

Av konkrete tiltaksområder for å sikre et fortsatt sterkt personvern peker Teknologirådet på følgende:

Identifikasjon og autentisering må gjøres på riktig nivå
Ved innføring av sterke metoder for autentisering som for eksempel digitale signaturer eller biometri, må bruken av personopplysninger minimeres. Autentisering på individnivå bør unngås såfremt dette ikke er strengt nødvendig. Pseudonyme løsninger med bruk av virtuelle identiteter bør stimuleres som alternativ til full anonymitet og full identifikasjon.

Anonyme tjenester må fortsatt tilbys i sammenhenger hvor det ikke er nødvendig å kunne holde brukerne ansvarlig. For eksempel må det fortsatt være mulig å betale med anonyme penger på nettet, lese nettaviser og ytre seg offentlig uten å vise digital legitimasjon.

Det må være reell gjennomsiktighet i systemer som lagrer personopplysninger
I en situasjon hvor et økende antall aktører lagrer stadig mer elektronisk informasjon om hver enkelt borger blir det vanskeligere å sikre informasjon mot spredning. Dette øker viktigheten av at borgerne kan kontrollere hvilke opplysninger som er lagret om dem og hvordan både statlige og private datainnsamlere håndterer innsamlede personopplysninger.

Man må gjøre grundige vurderinger før tiltak som reduserer personvernet innføres
Privatsfærens kår blir trangere ettersom elektroniske hjelpemidler blir vanlige på stadig flere livsområder. Siden reduksjoner i privatsfæren sjelden lar seg reversere, bør myndighetene vurdere nøye om gevinsten står i forhold til kostnaden i form av redusert personvern.

Det må utvises forsiktighet ved innføring av nye teknologier som kan identifisere brukere. Konsekvenser for personvernet må utredes ved innføring av nye teknologier av denne type.

Det må tas hensyn til personvern ved implementering av nye IKT-systemer
Ved innføring av ny teknologi eller nye IKT-baserte metoder som håndterer nærgående eller sensitive personopplysninger må det stilles krav om at systemer må implementeres på måter som ivaretar sentrale personvernhensyn.

Internkontrollsystemer må dokumentere hvordan personvernkrav ivaretas
Mye tyder på at mange aktører som behandler personopplysninger ikke godt nok overholder kravene i personopplysningsloven med forskrift. Kravet om et system for internkontroll som dokumenterer hvordan lovens krav oppfylles, bør følges sterkere opp.

Personvern og informasjonsetikk bør inn som tema i skolen
Ungdom har svake kunnskaper om og er lite bevisste på problemstillinger knyttet til personopplysninger og personvern. Det er behov for å få personvern og informasjonsetikk inn som et tema i grunnskolen.

Bevisstheten og kunnskapsnivået om elektroniske spor og personvern bør styrkes
Folk må hjelpes til selv å kunne ta ansvar for sitt personvern på de områder hvor dette er nødvendig. Som et bidrag til dette har Teknologirådet utarbeidet 12 råd til nettbrukere. Disse rådene kan finnes i Vedlegg 1 i denne rapporten.

Kapittel 1 Innledning

1.1 Introduksjon

Nye informasjons- og kommunikasjonsteknologier (IKT) introduseres i høyt tempo. Mange av disse lager elektroniske spor som kan føres tilbake til oss som brukere og som således kan utnyttes til å overvåke vår atferd. Mange spør seg hva som egentlig skjer med personvernet oppi alt dette. Tre typer av responser er vanlige på dette spørsmålet:[1]

- *"Ikke egentlig noe nytt"*
  Dette synet sier at alle samfunn må ha metoder for å behandle og beskytte informasjon om personer og for å beskytte sosiale grenser. Alle endringer som ny teknologi bringer utgjør kun gradsforskjeller og representerer ikke egentlig noe substansielt nytt.
- *"Personvernet er dødt"*
  Dette synet er basert på en oppfatning av at vi lever i en tid med revolusjonære endringer med hensyn til overskridelser av personlige og sosiale grenser. Det hevdes at situasjonen aldri har vært så ille og at personvernet rett og slett har avgått ved døden. Scott McNealy i Sun Microsystems er for eksempel kjent for å ha uttalt følgende: *"You have zero privacy anyway. Get over it!"*[2]
- *"Balansen vil bli gjenopprettet"*
  Mens dette synet også mener at man er vitne til revolusjonære endringer, legges det her vekt på at teknologibruk reflekterer sosiale og kulturelle faktorer, og at beskyttelsen av personopplysninger må forventes å bli styrket gjennom mot-teknologier, endrede vaner, politiske vedtak eller juridiske grep ettersom nye trusler dukker opp.

Slike bredpenslede utsagn er derimot ikke spesielt hjelpsomme for den som ønsker å forstå hva som faktisk skjer. Elementer av sannhet finnes i alle de tre forenklede forklaringene. For å få bedre innsikt i hvordan dagens og morgendagens IKT påvirker personvernet er det derimot nødvendig å dykke ned i materien og betrakte den underliggende kompleksiteten som de forenklede utsagnene skjuler.

Teknologirådets utgangspunkt er at privatsfæren lever, men at den utsettes for store belastninger fra ny teknologi som gjør våre liv mye mer sporbare. I denne rapporten søker vi å beskrive hvordan ulike teknologier kan virke inn på personvernet og hvordan omkring-liggende faktorer som for eksempel utviklingstrekk i samfunnet for øvrig, samt holdninger hos brukere og partsinteresser, også påvirker personvernets stilling.

Det er ingen tvil om at de fleste mennesker setter beskyttelsen av sin privatsfære svært høyt. Personvernspørsmål ser nå også ut til å være gjenstand for en noe økende interesse. Danske forskere har spådd at vi vil se en motreaksjon mot stadig økende informasjonsstress og elektronisk overvåkning hos en betydelig gruppe av brukere. De kaller fenomenet OFF og

---

[1] Marx (2002)
[2] Wired, 26.01.1999: *Sun on Privacy: 'Get Over It'*
http://www.wired.com/news/politics/0,1283,17538,00.html

hevder at et betydelig antall brukere i større grad vil unngå IKT-verktøy som for eksempel PC og mobiltelefon for å unnslippe deres negative bivirkninger.

Forskningsrådet har som en del av sine framsynsaktiviteter også vurdert den framtidige bruken av IKT. De ser blant annet for seg et mulig scenario for 2015 hvor brukerne er blitt mer skeptiske til bruk av IKT og krever *teknofrie soner* hvor man kan oppholde seg uten å bli stresset av teknologien og dens sporingsegenskaper.[3]

1.2 Grunner til å beskytte det private

Men hva så om privatsfærens kår skulle bli noe trangere? Kan det være så farlig? Mange hevder at de ikke har noe å skjule, og at det derfor ikke gjør noe om noen samler inn og registrerer informasjon om deres personlige forhold. Den som har rent mel i posen har etter sigende ingenting å frykte. Så enkelt er det derimot ikke. For hvem skal bestemme hvilket mel som er rent nok? Ulike sosiale grupper og miljøer har ulike standarder for hva som er sosialt akseptert, og hva som burde henges ut til spott og spe. Det er ikke enkelt å leve slik at man aldri påkaller seg noen annens misbilligelse, latterliggjøring eller forfølgelse. Melet i din pose kan være så rent det bare vil – du har uansett et behov for å beskytte deg mot trangsynte og intolerante mennesker i dine omgivelser, mot å bli bedømt eller kategorisert på basis av ufullstendig informasjon tatt ut av sin kontekst og mot kriminelle som ønsker å stjele din identitet. Personvernet finnes ikke av hensyn til folk med urent mel i posen, men for at normalt lovlydige mennesker skal kunne leve som frie og suverene individer.

Mennesker er forskjellige, og behovet for å verne om det private oppleves ulikt. Men selv om ikke alle ville oppleve en innskrenket privatsfære like problematisk, er det et faktum at personvernet beskytter hensyn som er av grunnleggende betydning for alle. Følgende fire hensyn kan betraktes som de mest sentrale grunnene til å sikre et robust personvern og til å beskytte den enkeltes private sfære:

Hensynet til menneskeverdet og individets integritet
Dette hensynet innebærer blant annet at mennesker må beskyttes mot ulike typer av krenkelser som kan skade individets psykiske integritet eller omdømme. En rekke forhold kan oppleves av mennesker som en krenkelse av deres identitet. Eksempler kan være påførelse av skamfølelse, uthengning, latterliggjøring, stigmatisering eller andre negative reaksjoner på egenskaper, holdninger, ytringer eller atferd som andre velger ikke å akseptere.

Hensynet til menneskelig autonomi
Reell selvbestemmelse forutsetter en beskyttet sfære hvor man kan ta beslutninger uten at noen kikker en i kortene. Dette hensynet innebærer beskyttelse fra uforholdsmessig innsyn og overvåkning. Mennesker som føler at de er under observasjon eller en form for overvåkning vil normalt tilpasse sin atferd til det de tror forventes av dem. Personvernet blir slik en forutsetning for et fritt samfunn hvor individet er suverent og selv kan velge hvilket liv hun vil leve.

Behovet for å få være i fred
En klassisk og enkel definisjon av privacy-begrepet sier at det omhandler retten til å kunne få være i fred ("right to be let alone"). Folk har generelt vanskelig for å slappe av og kunne

[3] http://www.forskningsradet.no/CSStorage/Vedlegg/Tre%20IKT-scenarier.pdf

”være seg selv” når de kan observeres av andre. De aller fleste har et sterkt behov for å kunne trekke seg tilbake til en beskyttet sfære hvor de kan stresse ned, la masken falle og bare være sitt private ”jeg” – alene eller sammen med sine nærmeste.

Behovet for etablering av nære sosiale relasjoner
Utvikling av intimitet forutsetter en mulighet til selektiv åpenhet, det vil si en viss eksklusivitet i deling av erfaringer og hemmeligheter med et annet menneske. Da må informasjon om mennesker være beskyttet slik at ikke alt er kjent for alle. Privatsfærens verdier som empati, tilgivelse, lekenhet og kjærlighet trenger dessuten beskyttelse fra offentlighetens harde søkelys og andre menneskers fordømmende blikk.

Personvern innebærer at det finnes grenser og regler for behandling av personopplysninger og en grunnleggende beskyttelse av den enkeltes privatliv. Basale hensyn til individets integritet og selvbestemmelse er avhengige av et robust personvern, på samme måten som muligheten til å kunne få være i fred og til å kunne etablere nære relasjoner til andre. Grunnene til å forsvare vernet av personopplysninger og den private sfære er med andre ord sterke, selv om sammenhengene ikke er åpenbare for alle.

Introduksjonen av elektronisk databehandling medførte i sin tid nye utfordringer knyttet til beskyttelse av personopplysninger. De senere års utvikling av nye digitale informasjons- og kommunikasjonsteknologier (IKT) gjør at personvernet nå står overfor større utfordringer enn noensinne. Det er derfor god grunn til å spørre om de grunnleggende hensyn vi her har nevnt, kan stå i fare for å svekkes som en følge av begeistringen for ny teknologi.

Kapittel 2 Utviklingstrekk

Moderne informasjons- og kommunikasjonsteknologi (IKT) er blitt stadig viktigere i dagens samfunn, og dette har aktualisert behovet for å se på hvordan IKT har påvirket personvernet. Forutsetningene og virkemidlene for sikring av samfunnet og bekjempelse av kriminalitet har også sett en markant utvikling de senere år. På det kommersielle området har bruk av ny teknologi og framveksten av elektronisk handel medført en betydelig økning i etterspørselen etter informasjon om kundene og påfølgende behandling av personopplysninger. Og sist men ikke minst, har teknologien for mange bidratt både til å svekke skillet mellom arbeid og fritid, og til å gjennomhulle og svekke beskyttelsen av den private sfære.

2.1 Teknologiutvikling

Utviklingen innen informasjons- og kommunikasjonsteknologier (IKT) har lenge gått raskt, og spesielt i de senere årene har det skjedd mye som er svært merkbart for vanlige brukere. Teknologier som mobiltelefoni og internett var for bare 10-12 år siden forbeholdt en relativt liten andel av befolkningen, men er i dag å betrakte som allemannseie. 81% av befolkningen hadde i 2004 tilgang til internett og 91% hadde brukte mobiltelefon (TNS Gallup, 2005). Den hurtige utviklingen av nye teknologier faller altså sammen med en sterk økning i utbredelsen og bruken av slike teknologier. Det som er felles for nye informasjons- og kommunikasjonsteknologier er at de er digitale og i mange tilfeller lagrer elektroniske spor som vitner om den faktiske bruken av teknologiene. Følgende aspekter er fremtredende i denne teknologiutviklingen og har betydelig innvirkning på personvernet:

Økning i spormengden
Samfunnet har i de senere år sett en sterk økning i bruken av ulike typer elektroniske hjelpemidler. Stadig flere livsområder støttes nå av elektronikk som gir nye muligheter for brukerne. Detaljhandel, økonomiske transaksjoner, bevegelser i trafikken og interaksjon med det offentlige er eksempler på områder hvor det settes mange elektroniske spor. Dessuten foregår i dag nesten all kommunikasjon som ikke skjer ansikt til ansikt, ved hjelp av sporsettende elektronisk kommunikasjon. Dette gjelder for eksempel både fasttelefoni, mobiltelefoni, e-post og internett. Resultatet av alt dette er en dramatisk økning i mengden av elektroniske spor som mennesker etterlater seg i hverdagen. Dette er en utvikling som vil fortsette i årene som kommer og som forventes ytterligere intensivert ved introduksjonen av teknologier for *intelligente omgivelser* (se kapittel 6.8).

Mer innholdsrike spor
Samtidig som spormengden øker blir også de sporene som settes mer innholdsrike og potensielt avslørende. Dette er en følge av at sporene blir mer finmaskede og nærmere knyttet til konkret menneskelig aktivitet. Eksempler på de mer nærgående sporene er geografisk posisjon og bevegelse knyttet til bruk av mobiltelefon, hvilke websider man besøker på internett, hvilke søkeord man har brukt på søkemotorer som Google, og all skriftlig kommunikasjon som man sender ubeskyttet over internett. Etter hvert vil vi også få se mer av elektroniske spor som inneholder genetisk informasjon. DNA-sniffere forventes å bli en realitet innen få år og vil kunne fange opp og lagre elektroniske spor med informasjon om menneskers arvestoff.

Sårbare systemer
Ettersom stadig flere bedrifter, organisasjoner og offentlige etater har databaser hvor de lagrer konfidensielle opplysninger om enkeltpersoner, er faren for at det kan forekomme uautorisert innsyn eller lekkasje av opplysninger mye større enn tidligere. Mangelfulle organisatoriske rutiner, interne utro tjenere, nysgjerrige og ubetenksomme ansatte eller sviktende teknisk sikring mot datainnbrudd er eksempler på årsaker til at slikt kan skje. Infrastrukturen på internett er også sårbar, og det er betydelig risiko for snoking og utilbørlig innsyn i informasjonssystemer. Ettersom en stadig større andel av vår totale kommunikasjon går via internett, øker også eksponeringen for sårbare loggfiler og informasjonssystemer.

2.2 Samfunnssikkerhet

Kriminalitetsbildet slik det framstår i dag. skiller seg dramatisk fra det bildet vi så for noen tiår siden.[4] Ikke bare er omfanget av kriminaliteten blitt større, men den har dessuten blitt grovere og mer alvorlig både i forhold til enkeltpersoner og mot samfunnet som sådan. Nye former for økonomisk kriminalitet samt organisert og internasjonal kriminalitet har vært en sentral tendens de senere år. Samtidig vokser også tradisjonell volds- og vinningskriminalitet.

Utbredelsen av internett har dessuten ført med seg en ny type av kriminalitet som utføres over datanettverk. Det vi kan kalle cyberkriminalitet eller datakriminalitet omfatter for eksempel slike ting som datainnbrudd (hacking) og tjenestenektangrep (DoS – denial of service). Etter hvert har e-post og andre nettbaserte tjenester blitt så utbredt at de ofte brukes i planlegging, koordinering eller gjennomføring av tradisjonelle former for kriminalitet. I etterforskning av kriminalitet i dag må politiet derfor rette søkelyset mot datanettverk og nettverk for mobiltelefoni i nesten alle typer saker.

Det er likevel en helt annen type kriminalitet som i løpet av de siste årene har drevet personvernet i elektronisk kommunikasjon på defensiven. Verden hadde sett mye terrorisme også tidligere, men det var terrorangrepene i USA den 11.september 2001 som for alvor brakte terrorfaren inn i bevisstheten til folk i store deler av verden. Det voldsomme inntrykket fra den dagen sitter fortsatt dypt i mennesker, spesielt i USA, men også i Europa og Norge. Terrorbombene i Madrid den 11.mars 2004 brakte terrorfaren enda nærmere inn på livet for Europa, og utløste på nytt sterke følelsesmessige reaksjoner hos innbyggere i mange land. Disse store terroraksjonene har begge utløst forsterket aktivitet for sikring av samfunnet mot nye tilsvarende aksjoner, og de tiltak som er foreslått eller allerede implementert i USA, EU og andre land er i betydelig grad rettet mot elektronisk kommunikasjon. Heller ikke Norge er noe unntak i så henseende.

Også om vi ser bort fra disse store terroraksjonene, er det trekk ved samfunnsutviklingen som øker behovet for robuste sikkerhetstiltak og nye metoder i kriminalitetsbekjempelse. Dagens moderne samfunn har gitt enkeltindivider en betydelig utvidet aksjonsradius. Mennesker kan lettere og raskere forflytte seg mellom land ettersom spesielt flytrafikk er blitt billigere og mer tilgjengelig. Man kan også mye lettere og raskere enn tidligere kommunisere med folk over hele verden ved hjelp av e-post, internett, mobiltelefoni og andre former for elektronisk kommunikasjon. En konsekvens av dette er et utvidet mulighetsrom for alvorlig, internasjonal kriminalitet og terrorisme.

---

[4] Politiregisterutvalget (2003)

I den elektroniske verden kan hackere og organiserte kriminelle påføre andre stor skade, for eksempel gjennom et tjenestenektangrep som gjør angrepsmålets nettsider utilgjengelige for kundene. Det fryktes også at terrorister etter hvert skal kunne lamme elementer av samfunnets infrastruktur gjennom angrep på systemer som støtter for eksempel elektrisitetsforsyningen i et område. Når IT-systemer i dag er en sentral del av de fleste virksomheter og samfunnsfunksjoner, er det et faktum at samfunnet er mer sårbart for angrep mot slike systemer.

Utviklingen i trusselbildet mot samfunnet gjør det nødvendig å vurdere nye politimetoder som i større grad kan utnytte informasjons- og kommunikasjonsteknologi på måter som er egnet til å beskytte innbyggernes trygghet. Noen av de tiltak som vurderes i en slik sammenheng kan ha betydelig negative konsekvenser for den enkeltes personvern.

2.3 Utvikling i næringslivet

Utviklingen innen handel og forretningsdrift har i løpet av få år i betydelig grad endret situasjonen for personvernet. Dette området er nå blitt den sentrale driver for innsamling og utnyttelse av informasjon om enkeltpersoner. Strekkoder på butikkvarer har sammen med utbredelsen av kort for elektronisk betaling åpnet muligheten for å finne ut hvem som kjøper hva. Inntil nylig har likevel de fleste handelsbedrifter i Norge vært relativt lite interessert i å utnytte slik informasjon. Den situasjonen er nå i ferd med å endre seg.

De senere år har som nevnt internett og elektronisk handel gjort det mye enklere både å samle inn og å utnytte informasjon om konsumentene. Mulighetene til å etterspore den enkeltes forbruk er blitt mye større, og dessuten kan man nå i større grad kartlegge den enkeltes preferanser og forbruksvaner. De nye nettbaserte tjenestene har samtidig åpnet nye muligheter for å utnytte opplysninger om den enkelte kunde til å skreddersy produkter eller reklame til den enkeltes behov. Næringslivet satser i økende grad på sterkere kundeorientering og informasjonssystemer for håndtering av kundeinformasjon (Customer Relationship Management).

Resultatet av dette har vært økende aktivitet fra en rekke kommersielle aktører for å samle inn data til omfattende personprofiler med informasjon om hver enkelt kunde. Slike personprofiler har lagt grunnlaget for en ny liten industri hvor selskaper kjøper og selger informasjon om mulige kunder. Mest utbredt er dette i USA, men vi ser fenomenet også i Norge, for eksempel gjennom Postens tjenester ”Meg og mitt” og ”Finn dine kunder”.

De økte mulighetene til å samle inn og utnytte kundeopplysninger faller sammen med en voldsom økning i bruken av de teknologiene som gjør dette mulig. Ved handel i butikk har elektronisk betaling nå langt på vei tatt over for kontanter. Og selv om mange brukere fortsatt er skeptiske, ser man en sterk økning i bruken av elektronisk handel. Folk handler stadig flere ting selv på nettet og legger igjen store mengder personlig informasjon i prosessen. For å sikre brukernes tillit til internett-baserte tjenester og elektronisk handel, vil det være avgjørende at brukernes personvern og sikkerhet blir ivaretatt.

2.4 Forholdet mellom privat og offentlig sfære

Vi ser også et utviklingstrekk hvor skillet mellom den private og den offentlige sfære blir svakere og mer uklart. Det private beveger seg inn i offentligheten og offentligheten sniker seg inn i det private. Enkelte har hevdet at dagens offentlighet er preget av en form for

”intimitetsterror”, og i en situasjon hvor så mange eksponerer sine privatliv i offentlige medier, blir det stadig mer uklart hvor grensene omkring det private går.[5]

Dette er problematisk fordi en beskyttet privatsfære er en forutsetning for individets autonomi og den arena som tillater dyrkelse av familiens verdier. Mens offentligheten er preget av verdier som rettferdighet, lovlydighet og likhet er det private preget av verdier som empati, tilgivelse og kjærlighet. Offentlighetens søkelys har en tendens til å undertrykke slike mellommenneskelige uttrykk. Også derfor er det problematisk at man i situasjoner som tidligere var privat og uovervåket, nå i mange tilfeller må være forberedt på at ens aktiviteter kan bli registrert og slik bli synlig for andre.

Kommunikasjon over internett hjemme utfordrer privatsfæreforståelsen ved at brukeren oppfatter å være i privatsfæren, samtidig som hun likevel langt på vei opptrer i offentlighet. Denne type grenseoverskridelser mellom sfærene gjør det vanskelig for brukerne å vite helt hvordan de skal forholde seg. Dette gjelder også i høy grad på arbeidsplassen.

Skillet mellom jobb og fritid er også blitt svekket, og dette bidrar til å forsterke uklarheten omkring grensene for den private sfære. Omfanget av retten til en privat sfære på jobben er uavklart på mange arbeidsplasser. Arbeidstakere presenteres ofte ikke for klare regler for hva de kan og ikke kan gjøre. For eksempel er det mange steder uklart i hvilken grad den enkelte kan sende og motta privat e-post på jobben. Med hjemmekontor blir også jobben ofte med hjem og inn i privatsfæren.

[5] Pauer-Studer (2003)

Kapittel 3 Personvern

Personvern er et sammensatt og komplekst begrep som de fleste ser ut til å ha en noe uklar forståelse av.[6] Vi skal i dette kapitlet se litt nærmere på hva som egentlig ligger i begrepet, og vi skal se at personvernet ofte må veies mot andre viktige hensyn som for eksempel åpenhet, offentlighet og samfunnssikkerhet.

3.1 Personvernbegrepet

Personvern er en fundamental menneskerett som i større eller mindre grad er anerkjent over store deler av verden, på tvers av kulturer og regioner. Det vi i Norge kaller personvern omfatter to ulike begreper i engelsk som kanskje noe bedre illustrerer hva det dreier seg om. *Privacy* er knyttet til vern av grunnleggende verdier som integritet, autonomi og privatliv, mens *data protection* har å gjøre med vern av personopplysninger. Sammenhengen mellom begrepene er nær, og man kan observere dem brukt om hverandre.

En måte å se dette på er at sikring av *privacy* er målet for personvernet, mens *data protection* i informasjonsalderen er et nødvendig middel for å nå dette målet. Da kan vi altså betrakte personvern som vern av personopplysninger av hensyn til beskyttelse av individets integritet, autonomi og privatliv.

I dagligtalen er det vanlig å bruke personvernbegrepet mer eller mindre synonymt med integritetsbeskyttelse. Men begrepet er videre enn som så, og personvernet skal sikre flere hensyn enn vern av individers integritet. Vi skal kort oppsummere en anerkjent modell for personvern som illustrerer de ulike komponentene som kan sies å inngå i begrepet. Modellen skiller mellom tre ulike verdimessige perspektiver på personvern, samt fem juridisk-faglige personverninteresser.[7]

De tre verdimessige perspektivene er:

Integritetsperspektiv
Dette perspektivet tar utgangspunkt i mennesker som frie og ukrenkelige individer som har behov for beskyttelse av en privat sfære de oppfatter som sensitiv eller personlig. Her er det hensiktsmessig å skille mellom fem ulike aspekter av integritet.

- *Territorial integritet* har å gjøre med beskyttelse av individers geografiske territorium, typisk det private hjem hvor mennesker forventer å kunne nyte privatlivets fred. Forventningen om å kunne være i fred innenfor "husets fire vegger" er sterk. På engelsk snakker man om "sanctity of the home" – hjemmet som noe hellig.
- *Kroppslig integritet* gjelder kravet på beskyttelse av kroppen vår mot krenkelser. Det er ikke vanlig å betrakte voldsutøvelse som et personvernproblem, så her menes beskyttelse mot ikke-voldelige krenkelser som for eksempel undersøkelse av kroppens hulrom eller biometrisk prøvetaking av kroppslige egenskaper som for eksempel kan gi informasjon om medisinsk eller genetisk status.

[6] Teknologirådet (2004)
[7] Beskrivelsen er basert på Schartum & Bygrave (2004) samt Wiik Johansen m.fl (2001)

- *Psykisk integritet* omfatter beskyttelse mot et bredt spekter av krenkelser som kan ramme et menneskes selvbilde, ære og omdømme eller på annen måte påføre alvorlig psykisk belastning. Inngripen i retten til uforstyrret refleksjon, som for eksempel gjennom lesning av annen persons dagbok, kan også sies å være en integritetskrenkelse.
- *Kommunikasjonsintegritet* gjelder respekten for andres rett til å kommunisere uforstyrret. Åpning av andres brev, lesing av andres e-post og avlytting av andres telefonsamtaler er eksempler på tiltak som kan sies å være brudd på den aktuelle personens kommunikasjonsintegritet.
- *Informasjonsintegritet* sikrer individets integritet gjennom informasjonsmessig selvbestemmelse. Dette innebærer at en person i stor grad selv kan bestemme hvilken informasjon om en selv som skal tilflyte andre. Har noen behov for å holde noe hemmelig, så bør dette behovet respekteres.

Beslutningsperspektiv
Dette perspektivet på personvern dreier seg om hvordan opplysninger om enkeltpersoner brukes i beslutningsprosesser. Primært gjelder dette i saker hvor det tas en beslutning som angår en enkeltperson, og hvor det følgelig ofte er viktig for vedkommende at beslutningen tas på et forsvarlig grunnlag. Det innebærer at beslutningstakeren må ha relevante, korrekte og fullstendige opplysninger om personen. Hvis den som skal fatte en beslutning derimot har mangelfulle opplysninger, må det vises varsomhet med å fatte beslutninger på dette grunnlag.

Dette perspektivet retter med andre ord oppmerksomheten mot kvaliteten på personopplysninger og kvaliteten i behandlingen av disse. Et problem man vil være opptatt av i denne sammenheng er om saker behandles på basis av tilgjengelige data, uten at den behandlende kan vite om de er korrekte og fullstendige.

Maktperspektiv
Dette perspektivet dreier seg om den makt som ligger i det å besitte personopplysninger om andre mennesker, spesielt i forholdet mellom asymmetriske parter som for eksempel et enkeltindivid overfor det offentlige, en arbeidstaker overfor sin arbeidsgiver eller en konsument overfor kommersielle selskaper. Det er nært beslektet med beslutningsperspektivet, men omfatter også saker som ikke gjelder konkrete beslutninger. Makt kan utøves uten at det treffes beslutninger, nemlig gjennom det som kan kalles forventningsmakt, dvs. en disiplinerende virkning som følger av at en person forventer at konkrete sanksjoner vil følge av bestemte handlinger.

Dette perspektivet er også egnet til å se på politiske vurderinger av mulige tiltak som vil medføre innsamling av data som kan utøve direkte eller indirekte makt over borgerne. For eksempel kan det være slik at iverksettelse av en rekke kontrolltiltak som hver for seg oppfattes som legitime og akseptable, i sum kan framstå som overdrevne og uakseptable. Dette er det som ofte kalles ”de gode hensikters tyranni”.

Vi kan peke på følgende 5 juridisk-faglige personverninteresser:

- *Bestemmelse over tilgangen til informasjon om egen person*
  Denne interessen beskriver det mange først og fremst forbinder med personvern, nemlig muligheten til å holde ting hemmelig og begrense tilgangen til opplysninger

av personlig eller privat karakter. Denne interessen har primært å gjøre med sikring av konfidensialitet og beskyttelse av privatlivet.

- *Innsyn og kunnskap*
  Interessen for innsyn i og kunnskap om forhold av betydning for behandlingen av opplysninger om en selv er helt grunnleggende for personvernet, fordi det er en forutsetning for at individet skal kunne ivareta sine andre personverninteresser. Innsynsretten er viktig for å kunne kontrollere hvilke data om en selv som ligger til grunn for en behandling, og slik korrigere eller komplettere opplysningene, evt kreve foreldede opplysninger slettet.
- *Opplysnings- og behandlingskvalitet*
  Denne interessen gjelder behandling av saker hvor beslutninger tas på bakgrunn av personopplysninger, og stiller krav til kvaliteten både på opplysningene og på behandlingsprosessen. Kvalitet på opplysninger innebærer at de må være relevante, presise, fullstendige og korrekte. Kvalitet på behandling gjelder primært rutiner for registrering og prosessering i informasjonssystemer, og stiller krav om at systemet må være håndterlig, robust, tilgjengelig, pålitelig og forståelig.
- *Forholdsmessig kontroll og overvåkning*
  Denne interessen har å gjøre med sikring av borgerne mot uforholdsmessig kontroll fra myndighetenes side. Også demokratiske samfunn har behov for å kontrollere at individer ikke opptrer i strid med samfunnets interesser, men det er viktig å sikre at kontroll- og overvåkningsnivået ikke blir så høyt at man fjerner behovet for et tillitsforhold mellom myndighetene og den enkelte. Denne interessen er viktig for å sikre individets autonomi og frihet.
- *Brukervennlig behandling*
  Denne interessen beskriver behovet for at forvaltningen og andre som behandler personopplysninger skal møte brukeren med et menneskelig ansikt. Bakgrunnen for dette er at den enkelte skal kunne forstå og påvirke måten opplysninger om henne behandles på, for å kunne bidra til et best mulig beslutningsgrunnlag og korrekt saksbehandling.

3.2 Traktater og lover som beskytter personvernet

Før vi beskriver nærmere hvilke kjerneprinsipper som ligger til grunn for personvernlovgivningen, skal vi kort nevne hvor personvernet har sine røtter, og liste opp utvalgte sentrale internasjonale og nasjonale instrumenter som bidrar i beskyttelsen av personvernet. Regelsett for vern av personopplysninger både i Norge og internasjonalt springer ut av grunnleggende internasjonale traktater om menneskerettigheter. Av særlig viktighet er artikkel 8 i Den europeiske menneskerettighetskonvensjon (EMK), som fastslår at enhver har rett til respekt for sitt privat- og familieliv, sitt hjem og sin korrespondanse.

Når det gjelder den konkrete utformingen av nasjonale regelsett er det derimot ulike instrumenter utarbeidet av EU, Europarådet og OECD som har størst betydning[8].

[8] Schartum og Bygrave (2004)

Internasjonale instrumenter:

- Verdenserklæringen om menneskerettigheter (1948)
- Den europeiske menneskerettighetskonvensjon (1950)
- FN-konvensjonen om sivile og politiske rettigheter (1966)
- OECDs retningslinjer for beskyttelse og utveksling av personopplysninger (1980)
- Europarådets personvernkonvensjon (1981)
- EUs personverndirektiv, 95/46/EC (1995)
- EUs direktiv om personvern ved elektronisk kommunikasjon, 2002/58/EC (2002)

Nasjonale instrumenter:

- Personopplysningsloven (2000)
- Sektorlover (Helseregisterloven, 2001; Lov om elektronisk kommunikasjon, 2003)

Personopplysningsloven er den sentrale personvernloven i Norge. Den bygger i hovedsak på EUs personverndirektiv og gir generelle bestemmelser for behandling av personopplysninger, dvs. opplysninger som direkte eller indirekte kan knyttes til en person generelt, og gjelder således på tvers av sektorer. Likevel er det enkelte viktige særlover som regulerer utvalgte personvernrelaterte hensyn innenfor gitte områder. Herunder kommer lover knyttet til helseregistre og elektronisk kommunikasjon.

I tillegg utfylles bestemmelsene i personopplysningsloven av bestemmelser i en rekke andre lover. Eksempler på dette er Folkeregisterloven samt taushetspliktreglene i forvaltningsloven, legeloven og sosialtjenesteloven.[9] For en omfattende oversikt over personvernrelaterte lovbestemmelser, se nettstedet *Personvern på nettet*[10].

3.3 Kjerneprinsipper i personvernlovgivningen

Et sett av kjerneprinsipper kommer til anvendelse i personvernlovgivning verden over. De fleste av disse prinsippene er felles for OECDs retningslinjer og EU sitt personverndirektiv, og er også sentrale i forhold til Personopplysningsloven. Framstillingen av disse kjerneprinsipper er basert på Bygrave (2002):

Rimelig og lovmessig behandling
Innsamling og behandling av personopplysninger må skje i overensstemmelse med lovverket, og på en måte som er rimelig i forhold til den registrerte. Med rimelig menes at behandlingen ikke må medføre urimelig belastning for den enkeltes privatsfære, autonomi eller integritet, at man må balansere hensynene til de ulike involverte partene, og at registrering av opplysninger må være proporsjonal med formålet. Dette prinsippet innebærer også et krav om at behandlingen av personopplysninger skal være transparent for den registrerte.

[9] Wiik Johansen m.fl. (2001)
[10] http://www.personvern.uio.no/pvpn/index.html

Minimalitet
Mengden av personopplysninger som samles inn må være begrenset til det som er nødvendig i forhold til det formål som ligger til grunn for innsamlingen og den videre behandling av disse opplysningene. En følge av dette prinsippet er at innsamlede data som ikke lenger er nødvendige for det angitte formål må slettes eller anonymiseres.

Formålsbestemthet
Personopplysninger må samles inn kun for bestemte formål. Disse formålene må være lovlige eller legitime. Dessuten må formålene for den videre behandling av opplysningene ikke være uforenlige med de formål opplysningene opprinnelig ble samlet inn for.

Kvalitet på opplysninger
Personopplysninger må være relevante, korrekte og fullstendige i forhold til det formål de skal behandles for. Dette innebærer at opplysninger som ligger til grunn for behandling skal være oppdaterte og nøyaktige, og ikke inneholde irrelevant informasjon. Dette prinsippet skal sikre at behandling ikke skjer på et ufullstendig eller feilaktig grunnlag.

Deltakelse og kontroll
Personer bør informeres om hvilken informasjon om dem som innehas av andre. De må også gis innsyn i disse opplysningene og få mulighet til å korrigere opplysninger som er feilaktige eller misvisende. Dette prinsippet bidrar slik også til å sikre transparens i forhold til den registrerte samt til bedre kvalitet på opplysninger.

Begrenset behandling og formidling
Personopplysninger skal ikke bringes videre til tredjepart eller behandles for andre formål enn de som de ble samlet inn for uten tillatelse fra den registrerte. Unntak fra dette prinsippet kan gjøres i de tilfeller hvor slik videre behandling av opplysninger er hjemlet i annen lov eller den registrerte samtykker til behandlingen.

Informasjonssikkerhet
Dette prinsippet innebærer at de som oppbevarer personopplysninger må treffe de nødvendige tiltak for å sikre opplysningene mot uautorisert tilgang, endring, ødeleggelse og spredning. Opplysningene må også beskyttes mot ødeleggelse som følge av uhell.

Sensitivitet
Dette prinsippet sikrer at kategorier av opplysninger som oppfattes som spesielt sensitive for de registrerte skal kontrolleres strengere enn andre typer opplysninger. Personopplysningsloven nevner følgende kategorier av opplysninger som sensitive: rase eller etnisk opphav, politiske oppfatninger, religiøs eller filosofisk overbevisning, medlemskap i fagforeninger, helse og seksualliv. Kriminalitetsregistre gis også spesielt vern i denne sammenheng. Dette prinsippet kan oppfattes å bryte med den relativt gjengse oppfatning i personverndiskurser, om at i hvilken grad opplysninger oppfattes som sensitive av den enkelte i hovedsak er situasjonsavhengig. Likefullt er det en lang tradisjon i europeisk lovgivning at de nevnte kategorier av data gis spesielt vern.

3.4 Avveininger mot andre hensyn

Diskusjoner om grensene for personvernet handler nødvendigvis også om andre hensyn enn bare personvernet. Det ligger i personvernets natur at det er et hensyn som ikke kan gjelde absolutt og som ikke kan maksimeres, men som må veies mot og delvis vike for andre hensyn. Dette fordi det i mange sammenhenger er helt nødvendig å kunne benytte person-

opplysninger for å sikre effektive og brukervennlige tjenester, og fordi samfunnet i mange tilfeller faktisk må kunne vite noe om den enkelte. Følgende er viktige eksempler på hensyn som personvernet må veies mot:

Åpenhet
Personvernet vektlegger konfidensialitet om personopplysninger som den enkelte oppfatter som privat. Av og til kan dette være i konflikt med legitime krav til åpenhet. Hvis noen for eksempel mishandler sin ektefelle eller barn, er det utvilsomt ønskelig at slikt kommer for dagen selv om overgriperen måtte ønske å holde det skjult. I et åpent og demokratisk samfunn må man også ha en viss transparens i forhold til hvordan beslutninger tas. Korrupsjon er en type problem som kun kan bekjempes gjennom krav til åpenhet og innsyn. Personvernet må altså ikke maksimeres slik at det beskytter ulovlige handlinger. Derimot spiller det en viktig rolle for å beskytte mot påtvunget åpenhet om atferd som i enkelte miljøer kan oppfattes som kontroversielle eller stigmatiserende. Eksempler kan være homofil praksis eller deltakelse hos Anonyme Alkoholikere.

Effektivitet og brukervennlighet
I mange tilfeller vil hensyn til personvernhensyn kunne medføre ekstra innsats eller tidsbruk fordi det gjerne krever noe mer omstendelige arbeidsprosesser. Det perfekte personvern ville kreve mer ressursbruk enn noen er villig til å yte. Man må i praksis finne en balanse mellom et tilstrekkelig personvern på den ene siden, og akseptabel effektivitet og brukervennlighet på den andre. Vanlige brukere er gjerne mer opptatt av effektive tjenester enn av å beskytte sine personopplysninger ved bruk av IKT. Også kommersielle aktører ønsker effektive systemer som brukerne lett kan ta i bruk og som koster minst mulig å implementere. Personvern kan derimot være dyrt, og det er grenser for hva folk er villige til å betale for å beskytte sitt personvern bedre.

Samfunnssikkerhet og kriminalitetsbekjempelse
Etterforskning av kriminelle handlinger og overvåkningstiltak for å avverge alvorlig kriminalitet vil ofte innebære behandling av personopplysninger som kan oppfattes som å medføre en belastning for personvernet. Likevel er det åpenbart at politiet må kunne bruke informasjon om personer i sin etterforskning. Det som er en evig utfordring er å finne grensene for hvilken informasjon de skal kunne samle inn, og under hvilke forutsetninger. Mer om avveiningen mellom disse hensynene i Kapittel 7, Samfunnssikkerhet og overvåkning.

Kapittel 4 Holdninger til personvern

Hovedfokus for denne rapporten er naturlig nok teknologiens innvirkning på personvernets kår. Vi skal likevel se litt på hvilke aktører som har spesiell interesse av hvordan personvernet veies mot andre hensyn, og hvordan disses holdninger legger viktige premisser for personvernets posisjon i samfunnet. For politikere som skal finne balanserte standpunkter er det er viktig å være klar over hvilke partsinteresser som spiller inn når det kommer til spørsmål omkring vern og utnyttelse av elektroniske spor.

4.1 Aktører som utnytter elektroniske spor

Mange ulike typer av aktører er enten helt avhengige av, eller har interesse av å utnytte elektroniske spor i sin virksomhet. Som nevnt omfattes et økende antall samfunnsområder av elektroniske innretninger som lagrer spor av brukernes handlinger. Slike spor kan ha betydelig verdi for mange aktører, og det er derfor også stor etterspørsel etter dem. Det er en klar tendens til at økningen i mengden av loggførte spor og lagret elektronisk informasjon om enkeltpersoner skaper et ønske om å utnytte denne informasjonen til nye formål. Det er i dag en av de viktigste utfordringene for personvernet at ulike aktører ønsker å kunne nyttiggjøre seg elektroniske spor til egne formål, selv om disse er helt andre enn de som lå til grunn for at dataene ble lagret.

Følgende er de viktigste aktørene på etterspørselssiden av elektroniske spor:

Offentlige myndigheter
Myndighetene ønsker informasjon om borgerne for å kunne tilby effektive offentlige tjenester, og samtidig hindre misbruk av fellesskapets midler. Politi og rettsvesen har behov for elektroniske spor som hjelp til å etterforske og pådømme kriminelle forhold, samt for å sikre liv og opprettholde lov og orden i samfunnet. Helsevesenet på sin side har behov for å lagre og utnytte data om pasientene i den hensikt å kunne gi effektiv medisinsk behandling.

Arbeidsgivere
Arbeidsgivere er avhengige av å ha en viss kontroll med sine ansatte for å sikre kvaliteten på arbeidet som utføres, og for å forhindre uønskede handlinger fra egne ansattes side. Utro tjenere kan påføre et selskap stor skade, og mange selskaper implementerer ulike tiltak for kontroll eller overvåkning for å sikre seg mot forhold som svinn, erstatningsansvar eller tap av omdømme. Videoovervåkning og ulike former for overvåkning av elektronisk kommunikasjon er tiltak mange arbeidsgivere enten bruker eller ønsker å kunne bruke.

Kommersielle interesser
Ettersom elektronisk handel har vokst fram, har kommersielle aktører tatt rollen som de mest aggressive brukerne av elektroniske spor som kan knyttes til brukere. En egen industri er oppstått knyttet til salg og utveksling av personopplysninger fra elektroniske spor. En rekke aktører samler inn data om brukerne for å bygge personprofiler. Slike profiler kan ha betydelig økonomisk verdi og selges til ulike andre kommersielle aktører.

Privatpersoner
Privatpersoner kan også ha interesse av å skaffe seg tilgang til elektroniske spor. Det kan dreie seg om alt fra en som av nysgjerrighet ønsker å avlytte naboens internettrafikk til en

forsmådd, sjalu type som ønsker å spore opp og forfølge sin eks-partner. I hovedsak vil private datasnoker være sportshackere som foretar datainnbrudd hos selskaper eller andre privatpersoner bare fordi de synes det er spennende, uten å gjøre skade.

Kriminelle
Både organiserte kriminelle grupper og enkeltstående kriminelle står bak en kraftig økning av lovbrudd som identitetstyveri, datainnbrudd og tjenestenektangrep. Identitetstyveri vokser raskt internasjonalt, og gjøres lettere ved at identifiserende opplysninger kan finnes i elektroniske spor som fanges opp. Spor fra usikrede PC-er eller usikrede trådløse nettverk lar kriminelle misbruke uskyldige personers datautstyr til kriminell aktivitet, som for eksempel datainnbrudd eller nedlasting av barnepornografi.

4.2 Aktører som beskytter personvernet

En rekke aktører er aktive for å tale personvernets sak i Norge og internasjonalt. Vi skal her kort nevne noen sentrale aktører, både slike som aktivt jobber for å sikre personvern-interesser, samt mer nøytrale aktører som bidrar til å øke kunnskapen om personvernet og dets grunnlag.

- *Datatilsynet*
  Datatilsynet[11] står i en særstilling i beskyttelsen av personvernet i Norge. De har tilsynsansvaret for personopplysningsloven, og således det formelle ansvaret for at loven overholdes i etater, bedrifter og organisasjoner. De utøver også en rolle som en aktiv forsvarer av personvernets stilling i samfunnet, og driver informasjons- og opplysningsvirksomhet omkring personopplysningsloven og personvern generelt.

- *Personvernnemnda*
  Personvernnemnda[12] er klageorgan for vedtak fattet av Datatilsynet.

- *Akademiske miljøer*
  De fremste miljøene som forsker og underviser innen IKT-relatert personvern finnes ved Institutt for Rettsinformatikk (IRI)[13] og Avdeling for Forvaltningsinformatikk (AFIN)[14] ved Universitetet i Oslo. Sterke miljøer knyttet til informasjonssikkerhet finnes blant annet ved NTNU[15] i Trondheim og Høgskolen i Gjøvik[16], mens fremtredende miljøer på området kryptografi finnes ved Universitetene i Tromsø[17] og Bergen[18].

- *Forsvarsadvokater*
  Siden vi i Norge ikke har tradisjon for sterke interesseorganisasjoner for sivile rettigheter som personvern, har enkelte forsvarsadvokater tatt rollen som personvernets forsvarere i offentlig debatt, spesielt i forhold til spørsmål rundt bruk av

[11] http://www.datatilsynet.no/
[12] http://www.personvernnemnda.no/
[13] http://www.jus.uio.no/iri/
[14] http://www.afin.uio.no/
[15] http://www.ntnu.no/
[16] http://www.nislab.no/
[17] http://uit.no/matstat/kryptografi/
[18] http://www.selmer.uib.no/

etterforskningsmetoder. Leder av Advokatforeningens lovutvalg for strafferett og straffeprosess, Harald Stabell, er fremtredende blant disse.

- *Borgerrettighetsorganisasjoner*
  Elektronisk Forpost Norge[19] er en rettighetsorganisasjon som jobber for borgerrettigheter i IT-samfunnet, og således det nærmeste vi kommer en interesseorganisasjon for elektronisk personvern i Norge. Internasjonalt finnes en rekke rettighetsorganisasjoner som jobber for å sikre retten til vern av integritet og privatliv. Følgende er sentrale eksempler på slike organisasjoner: Privacy International (UK)[20], Statewatch (UK)[21], Electronic Privacy Information Center (USA)[22], American Civil Liberties Union (USA)[23] og Center for Democracy and Technology (USA)[24]. Tyske delstater har aktive personverninstanser som sammen driver nettstedet *Virtual Privacy Office* [25].

- *Datatilsynsorganer i EU*
  EU har en rekke enheter som er involvert i beskyttelsen av personvernet[26]. Mest fremtredende er den såkalte *Artikkel 29-gruppen* som ble opprettet ved artikkel 29 i EUs personverndirektiv (95/46/EC), og som fungerer som et uavhengig rådgivende organ for personvern i EU. Gruppen består av representanter fra datatilsynsorganene i EU-landene. Datatilsynet i Norge deltar som observatør.

4.3 Borgernes holdninger til personvern

Som del av prosjektet IKT og personvern gjennomførte Teknologirådet høsten 2003 en lekfolksundersøkelse for å få et inntrykk av vanlige brukeres holdninger til personvern og bruk av IKT-tjenester som internett og mobiltelefoni. Undersøkelsen ble basert på samtaler med 48 personer fordelt på seks fokusgrupper, hvorav fire med ungdom i alderen 17 -19 år og to med voksne mellom 30 og 40 år. Resultatene fra undersøkelsen ble publisert i februar 2004 i en separat rapport fra Teknologirådet kalt *Holdninger til personvern*. I det følgende gis korte oppsummeringer av sentrale innsikter fra undersøkelsen.

Lavt kunnskapsnivå
Kjennskapen til elektroniske spor blant respondentene var generelt relativt lav. Voksne viste seg å ha noe bedre kjennskap enn ungdom til at elektronisk kommunikasjon etterlater spor. Kunnskapen om tradisjonelle elektroniske spor fra bruk av ting som betalingskort og telefon var bedre enn kunnskapen om spor fra bruk av internett. Innsikten omkring hva personvern innebærer og hvilken lovbeskyttelse vi har for personvernet i Norge var også relativt svak. Mange visste at det finnes en spesiell personvernlov, men oppfatningene av dens innhold var vage. Igjen var de voksne noe bedre orienterte enn de unge.

[19] http://www.efn.no/
[20] http://www.privacyinternational.org/
[21] http://www.statewatch.org/
[22] http://www.epic.org/
[23] http://www.aclu.org/privacy/
[24] http://www.cdt.org/
[25] http://www.datenschutz.de/privo/
[26] http://europa.eu.int/comm/internal_market/privacy/index_en.htm

Ubekymret ungdom
Ungdommene framsto som ganske så ubekymret i forhold til sitt eget personvern ved elektronisk kommunikasjon. Den gjennomgående holdningen var at hvis man ikke har noe å skjule, så har man vel ingenting å være redd for. Det de kunne være litt redde for var å bli stilt i forlegenhet av festbilder som venner og medelever legger ut på internett. De voksne var ikke bekymret for festbilder, men ellers mer oppmerksomme på potensielle farer, og således også noe mer urolige for hvordan lagringen av ulike elektroniske spor kan påvirke deres eget personvern.

Effektivitet viktigere enn personvern
Respondentene var generelt lite villige til å bruke tid eller krefter på å beskytte sitt personvern online. Selv om personvern oppfattes som viktig, er brukerne mer opptatt av at tjenester må være brukervennlige og tidseffektive. Hvis det å beskytte sine person-opplysninger skulle kreve nevneverdig innsats eller tid, var det svært få som ville være villige til å forsake effektiviteten for å få tilbake noe så abstrakt som bedre personvern. Kryptering av all e-post for å sikre innholdet mot uautorisert innsyn ble for eksempel sett på som ønskelig av mange, men ingen kunne tenke seg å yte den innsatsen som i dag faktisk må til for å realisere det.

Personvernet i prinsippet viktig, men kan selges billig
Alle deltakerne i våre fokusgrupper svarte på direkte spørsmål at de ser på personvern som en viktig sak. Når hensyn til personvern skal veies mot andre hensyn virker det likevel ikke som det er så viktig for dem. De fleste sa de var villige til å gi fra seg personopplysninger mot å få noe gratis. Og det skal ikke mye til – om man får være med i trekningen av noe eller får sende noen gratis SMS-er, kan personopplysninger sitte løst.

Kriminalitetsbekjempelse går foran personvern
De fleste hevdet at hensynet til kriminalitetsbekjempelse er viktigere enn hensynet til personvern. Enkelte kunne tolkes i retning av å mene at kriminalitetsbekjempelse er en svært viktig sak, mens personvern til sammenligning er en slags luksus man kan bevilge seg så lenge det ikke koster noe. Enkelte andre var mer bevisste på at også personvernet beskytter grunnleggende samfunnsinteresser og således må tas i betraktning i forhold til politiets arbeid. Det var enighet om at politiet ikke kan ha ubegrensede fullmakter, men stort sett mente de fleste at personvernet hvis nødvendig må vike for kriminalitetsbekjempelse.

Sporreduserende tiltak er lite kjent
Mens kjennskapen til elektroniske spor var relativt lav, var kunnskapen om hvordan mengden av slike spor kan reduseres eller gjøres mer anonyme enda lavere. Kun noen få kjente til hvordan det er mulig å redusere mengden av elektroniske spor som andre kan se. Stikkord her var sletting av informasjon som cookies, lokale internettlogger og midlertidige filer i nettleseren, samt bruk av anonymiseringstjenester og kryptering. Kun noen få hadde benyttet seg av slike tiltak.

Stor tillit til myndigheter og store selskaper
Brukerne i vår undersøkelse viste svært stor tillit til at myndigheter og større private selskaper (som for eksempel Telenor) ivaretar brukernes personvern. Dette kan muligens forklare noe av paradokset som ligger i at folk mener personvern er viktig, samtidig som de ikke selv er villig til å gjøre noe for det. Hvis de mener at myndigheter og selskaper må ta ansvaret for aktivt å sikre den enkeltes personvern, er det lettere å forstå hvorfor de tar så

lett på sin egen rolle i dette. Flere uttalte likevel at på internett må hver enkelt selvfølgelig ta ansvaret for hvilke opplysninger man oppgir om seg selv.

Menn opptrer mer anonymt på nettet
Mennene i undersøkelsen var mer tilbøyelige enn kvinnene til å beskytte personvernet sitt på internett ved å oppgi fiktive personopplysninger. Ettersom mange nettsteder uten spesiell grunn ber brukere oppgi informasjon om seg selv, er dette et viktig tiltak for å beskytte eget personvern. Kvinnene vi snakket med oppfattet det i større grad enn mennene som problematisk å ikke oppgi korrekte identifiserende opplysninger. Mens mange av mennene oppgav at de ofte opptrer som Donald Duck eller lignende på nettet, kunne kvinnene kanskje strekke seg til å bruke mellomnavn istedenfor etternavn. Dette kan gjøre deres personvern mer sårbart, ettersom faren øker for at deres personopplysninger kan havne i gale hender.

Et lite mindretall er svært bevisste på å beskytte sitt personvern
Mens det alt overveiende flertall av de vi snakket med var lite bevisste omkring personvern og elektroniske spor, var det enkelte av de voksne som derimot var svært bevisste på dette. Disse var også villige til å bruke både tid og krefter hvis det kan forbedre personvernet deres. Derimot uttalte disse at det er svært vanskelig å vite i hvilke tilfeller man etterlater seg spor, og hva det i hvert tilfelle er mulig å gjøre for å sikre seg bedre. Blant disse etterlyses muligheter for å finne ut hvem som lagrer informasjon om oss og for lettere å kunne få innsyn hos disse.

4.4 Holdninger hos våre nordiske naboer

EU-kommisjonen presenterte i februar 2004 en større undersøkelse[27] av holdninger til personvern og informasjonssikkerhet hos innbyggerne i alle EU-landene. Her er det spesielt interessant å se på holdningene hos våre nordiske naboer, ettersom dette i mange tilfeller er en god pekepinn på tilsvarende her i Norge. EU-undersøkelsen viser at det er tildels store ulikheter i holdninger mellom de ulike landene i EU. De nordiske landene, spesielt Sverige og Finland, skiller seg ut på flere områder. Primært gjelder dette at borgerne har svært stor tillit til myndigheter og virksomheter som behandler personopplysninger og føler seg trygge på at de vil beskytte deres personopplysninger. Samtidig skiller de nordiske land seg negativt ut når det gjelder kjennskap til lovverket på personvernområdet.

Denne kombinasjonen av lavt kunnskapsnivå og høy tillit sammenfaller godt med funnene fra Teknologirådets egen undersøkelse her hjemme. Det skulle derfor være god grunn til å anta at EU-undersøkelsens resultater for vår nordiske naboer langt på vei vil være representative også for holdningene i Norge. I gjennomsnitt oppgir 60% av EU-borgerne å være mer eller mindre opptatt av spørsmål knyttet til personvern. 25% oppgav å være svært opptatt av personvern. Forøvrig viser EU-undersøkelsen at det er store ulikheter i svarene mellom landene. For eksempel er det bare 13% av danskene som sier de er svært opptatt av dette, mens hele 54% av svenskene sier det samme.

[27] http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf

Kapittel 5 Identitet, anonymitet og autentisering

Personvern i informasjonssamfunnet er nært knyttet til begrepet identitet. Mens begrepet *person* brukes om individer som rettslig og moralsk ansvarlig handlende mennesker, er identitetsbegrepet noe mer sammensatt. Identitet og person er delvis overlappende begreper som begge er viktige i diskusjoner omkring personvern. For å kunne holde individer ansvarlige for sine handlinger må man ved behov kunne identifisere den handlende, altså den ansvarlige personen. For å ivareta individers personvern og personlige sikkerhet er det derimot nødvendig å beskytte dem mot unødig identifikasjon av deres person. Balansegangen mellom disse ulike hensynene er et av de store dilemmaene i informasjons-samfunnet, og hvordan man avveier disse to hensynene har stor innvirkning på personvernet. Til en viss grad kan man i elektronisk kommunikasjon ivareta begge hensynene samtidig ved bruk av ulike former for digitale identiteter. [28]

5.1 Identitetsbegrepet

Menneskers kommunikasjon med andre og deltakelse på ulike arenaer i samfunnet baserer seg på en underforstått felles forståelse av hva identitet er. Ulike mekanismer for identifikasjon bidrar til å gjøre det mulig å stole på informasjon gitt av mennesker vi ikke kjenner personlig. Informasjonssamfunnet har ført med seg nye kommunikasjonsformer som utfordrer eksisterende modeller for identitet, og som krever nye mekanismer for identifisering.

Identifikasjon i tradisjonelle samfunn er i høy grad basert på direkte kontakt og en kontinuitet hvor identitet langt på vei defineres gjennom tilhørighet til et større felleskap og vedlikeholdes ved at man møtes fysisk med jevne mellomrom. Informasjonssamfunnet er derimot ikke en ansikt til ansikts-kultur, så fysisk nærvær er intet alternativ ved behov for identifikasjon. Historisk kontinuitet i relasjoner er også i mindre grad et trekk i den virtuelle verden. Så da må man i den nye elektroniske verden benytte andre mekanismer for å identifisere mennesker, og for å skape den tilliten som er forutsetningen for å kunne gjennomføre transaksjoner som involverer ukjente parter.

Det er vanlig å knytte følgende tre aspekter til begrepet identitet:

- *Permanens*
  Selv om sider ved identiteten er i utvikling, er den permanent på tross av alle forandringer den måtte gjennomgå gjennom levetiden.
- *Enhet*
  Selv om en identitet gjerne er mangesidig og variert, oppleves den som én enhet, hvor de ulike fasetter bidrar til å definere én enkelt, unik identitet
- *Fysisk realitet*
  Identitet er knyttet til fysiske karakteristika som er i endring, men likevel permanente. I den fysiske verden har vi én kropp for én identitet.

[28] Framstillingen bygger på: Institute for Prospective Technological Studies (2003)

Disse tre aspektene ved identiteter utfordres i den virtuelle verden på internett, hvor introduksjonen av virtuelle identiteter kan sies å fremme mer kortvarige og fragmenterte identiteter som ikke alltid er knyttet til noen fysisk realitet.

Vi vil her konsentrere oss om identitet som et begrep knyttet til interaksjon mellom mennesker og til individets rolle som samfunnsborger. I den forbindelse vil vi se på individuell identitet, og ikke gå inn på forhold knyttet til kollektive identiteter (gruppe-tilhørighet). Vi kan i denne sammenheng skille mellom to ulike sider av identitetsbegrepet: en prosedural eller formell og en sosialpsykologisk[29].

Prosedural identitet
Prosedural identitet er knyttet til formell identifikasjon av individer i forbindelse med interaksjon eller transaksjoner med andre. Fra et slikt ståsted er identitet en samling av formelle karakteristika som muliggjør identifikasjon og nødvendig autentisering (verifikasjon) i sosiale eller økonomiske forhold samt i forhold til myndighetene. Utvalget av karakteristika kan variere med behovet, men typiske eksempler vil være navn, fødselsdato, personnummer, høyde, øyenfarge, hudfarge, nasjonalitet, sivil status, antall barn, utdanningsbakgrunn, jobb og lignende.

Vår prosedurale identitet følger oss formelt fra fødsel til død, og presenterer oss overfor omverdenen som unike individer. Prosedural identitet er sterkt knyttet til individets fysiske karakteristika. Disse er som oftest representert ved et fotografi i pass eller annet ID-kort, men kan også representeres ved biometriske egenskaper som for eksempel håndskrevet signatur, fingeravtrykk, avbildning av øyets regnbuehinne (iris), håndgeometri, ansiktsgeometri, stemme eller arvestoff (DNA).

Sosialpsykologisk identitet
Fra et sosialpsykologisk (eller sosialfilosofisk) ståsted er identitetsbegrepet knyttet til individets forming av seg selv, dets selvforståelse og følelse av tilhørighet. Sosialpsykologisk identitet er altså en dynamisk konfigurasjon som er sterkt påvirket av historikken i et individs interaksjon med sine omgivelser, spesielt med andre individer. Sosialpsykologisk identitet er også nært knyttet til individets fysiske karakteristika (kroppen), samt til en rekke ikke-fysiske individuelle og relasjonsmessige aspekter mennesker assosierer med seg selv.

En dyp beskrivelse av et menneskes sosialpsykologiske identitet er en nær umulig oppgave, både fordi denne identiteten er i kontinuerlig utvikling og fordi innvirkningen fra tidligere interaksjon er kompleks og uoversiktlig. Det er innenfor dette området at psykoterapi og metoder for selvutvikling kommer til anvendelse. Til tross for, eller kanskje nettopp fordi menneskers forståelse av egen identitet ofte er problematisk, oppfatter de fleste mennesker i moderne samfunn utvikling og presentasjon av egen identitet som en svært viktig sak.

Et spesielt trekk ved den menneskelige identitet er at den er knyttet til en søke- eller bygge-prosess. Man kan oppfatte utviklingen av et menneskes identitet over tid som en kontinuerlig identitetsbygging gjennom interaksjon med andre. Mange, spesielt blant ungdom, oppfatter å være på leting etter sin identitet og er opptatt av å "finne seg selv". Søkeprosessen er forbundet med fasespesifikke krisetider som for eksempel puberteten. Den er også for mange karakterisert ved et behov for å eksperimentere med ulike roller og ulike typer sosiale nettverk. Informasjonssamfunnet byr folk nye muligheter til interaksjon

[29]Bogdanowicz og Beslay, IPTS (2001)

med nye felleskaper av mennesker over hele verden og eksperimentering med ulike roller gjennom bruk av det vi kan kalle virtuelle identiteter.

5.2 Digitale og virtuelle identiteter

Digital identitet er en elektronisk representasjon av identitet, altså en samling identifiserende personopplysninger i elektronisk form. All identifikasjon på nettet er basert på bruk av digitale identiteter. Dette begrepet er svært bredt og omfatter alt fra prosedural identitet i digital form (som kan identifisere en fysisk person) til virtuelle delidentiteter som har svært svak knytning til en fysisk person. Identifiserende opplysninger som er digitalt signerte er et eksempel på en digital identitet som kan brukes til formell identifikasjon av en fysisk person på nettet. I den andre enden av skalaen kan man ved hjelp av den strøm av elektroniske spor en person etterlater seg lage "kontekstuelle modeller" av individer gjennom innsamling, lagring og analyse av data om dem. Slike modeller vil utgjøre en form for kontekstuell identifikasjon, basert på hva man gjør[30].

Virtuelle identiteter (også kalt *nym*) er en form for digitale identiteter. Disse er elektroniske delidentiteter som uttrykker en større eller mindre del av et individs personlige opplysninger. Slike identiteter kan gjenspeile elementer av sosialpsykologiske identiteter og slik være uttrykk for personers ulike roller og ulike måter å presentere seg selv for omverdenen på. Det er med andre ord slik at en person gjerne vil operere under ulike virtuelle identiteter i ulike sammenhenger, akkurat som man i den fysiske verden opptrer i ulike roller på ulike arenaer. Samtidig brukes slike identiteter for å redusere knytningen mellom elektroniske spor og faktisk person for å minske faren for at noen kan aggregere en stor mengde personopplysninger i en personprofil. Slik er virtuelle identiteter et helt sentralt hjelpemiddel for å sikre personvernet i informasjonsalderen.

Virtuelle identiteter brukes også av hensyn til individuell sikkerhet. Ved å redusere informasjonsmengden som lett kan knyttes til ens egen person, kan man gjøre livet vanskeligere for kriminelle som vil kunne bruke eventuelle personopplysninger for ulike typer kriminelle formål. Eksempler på kriminelle handlinger som er lettere hvis man kan få tak i personlig informasjon om offeret og dets bevegelser er identitetstyveri, innbrudd i bolig og personforfølgelse.

Identifisering og personprofiler

Når vi snakker om identifisering, dreier det seg her om i hvilken grad handlinger som involverer lagring av elektroniske spor eller data kan knyttes til en person. Dette er en sentral problemstilling for personvernet, ettersom det nettopp er i knytningen til en person at mengden av elektroniske spor kan være problematisk. Hvis det var lett å samle alle de elektroniske spor som en person over tid etterlater seg i ulike sammenhenger i en helhetlig profil, så ville denne profilen fortelle svært mye om personen. Man ville i detalj kunne studere informasjon om personens bevegelser, kommunikasjon, økonomiske disposisjoner, interesser, preferanser, bekjentskapskrets, bosted, arbeidsgiver, familie og så videre. Det er ikke mange livsområder som i dag ikke er støttet av innretninger som lagrer elektroniske spor.

De fleste vil være enige i at etablering av slike personprofiler som langt på vei kan si "alt" om en person er et redselsbilde for et fritt samfunn. Men det er viktig å kunne skille mellom det

[30]Bogdanowicz og Beslay (2001)

som er tenkelig, og det som i praksis blir gjort eller kan gjøres. Det er flere grunner til at det ikke er lett å lage såpass nærgående profiler. For det første vil en stor del av de spor man setter ikke lett kunne knyttes til ens person. For det andre er det ikke slik at ulike aktører har anledning til å spleise sammen sine dataregistre med andre for å skape et mer helhetlig bilde av den enkelte, selv om dette skulle være mulig på bakgrunn av en felles identifikator (som for eksempel fødselsnummer, telefonnummer eller navn og adresse). Det er imidlertid all grunn til å være på vakt overfor en utvikling hvor både mulighetene til, og ønsket om å kunne sette sammen nærgående personprofiler øker.

5.3 Anonymitet og pseudonymitet

Det som er selve nøkkelen til hvordan elektroniske spor virker inn på personvernet, er hvilken grad av identifikasjon som er knyttet til sporene. Det avgjørende er om sporene kan knyttes til en faktisk person, og hvor lett dette eventuelt er. Hvis det er enkelt å knytte elektroniske spor eller data til et individ (for eksempel hvis telefonnummer eller fødselsnummer er knyttet til dataene), kan det være svært uheldig for den berørtes personvern. Dette fordi det i den elektroniske verden er vanskelig å ha kontroll med tilgang til og spredning av slike data. Hvis det derimot er vanskelig eller ressurskrevende å knytte et spor til en person, så er det langt mer betryggende for personvernet. Et eksempel på det siste er tilfeller hvor kun polititjenestemenn kan få tilgang til aktuelle loggfiler, og kun etter klarsignal fra en dommer. Det er til en viss grad også mulig å etterlate elektroniske spor som under normale omstendigheter ikke kan spores tilbake til den faktiske brukeren. Da er sporene anonyme, og som sådan uten potensial til å skade brukerens personvern.

Anonymitet i elektronisk kommunikasjon
Anledningen til å være anonym i elektronisk kommunikasjon er et omstridt spørsmål som er av stor betydning for personvernet. Anonymiteten som er så selvfølgelig for oss i mange dagligdagse situasjoner, er ikke like selvfølgelig når vi kommuniserer med elektroniske hjelpemidler. En av grunnene til dette har å gjøre med hvordan elektronisk kommunikasjon fungerer. For at telefonanrop, SMS-er, e-post og websider skal nå fram til mottakerens telefon eller PC, må nettoperatøren kjenne mottakerens elektroniske adresse, altså henholdsvis telefonnummer for telefonitjenester og IP-adresse for datakommunikasjon. Informasjon om senderens og mottakerens elektroniske adresser loggføres av operatører og tjenestetilbydere, slik at de kun trenger å knytte de aktuelle telefonnumre eller IP-adresser til en abonnent for å vite hvem som har vært involvert i et kommunikasjonsforløp.

Inntil nylig var det i Norge mulig å ringe anonymt ved bruk av uregistrerte kontantkort for mobiltelefon. Denne muligheten ble fjernet da forskriften til lov om elektronisk kommunikasjon (ekomforskriften) i 2004 påla alle operatører av telefonitjenester å føre kunderegister som unikt identifiserer hver enkelt kunde. Som regel vil det derfor nå være enkelt å finne ut hvem som skjuler seg bak et gitt telefonnummer. Selv om man kan undertrykke nummervisning overfor den man ringer opp, kan man ikke skjule nummeret sitt for operatøren. Denne lagrer loggdata om alle samtaler for å kunne fakturere riktig. Eneste mulighet til lovlig å telefonere anonymt i dag er således å bruke offentlige telefonkiosker.

Når det gjelder IP-adressene på internett er det ikke like enkelt å knytte en bestemt bruker til en slik adresse. Dette fordi det finnes gode muligheter for den som vil være anonym til å treffe tiltak som gjør det vanskelig å finne ut hvem som faktisk har gjort bruk av en gitt IP-adresse. På internett er det altså fortsatt mulig å opptre anonymt, men for de fleste brukerne er det et faktum at de selv på internett er langt mindre anonyme enn de liker å tro.

For vanlige hjemmebrukere vil det normalt være en smal sak for internettleverandøren å finne ut hvem som har brukt hvilke IP-adresser til hvilke tider. Den som vil være helt anonym på internett må ta i bruk spesielle anonymiseringstjenester eller sette seg på internett-cafe. Utbredelsen av trådløse lokalnett (WLAN) blant både bedrifter og hjemmebrukere de siste årene har åpnet en ny metode for å komme seg anonymt på internett. En stor andel av slike nettverk beskyttes ikke mot utenforstående, og står således vidåpne for alle i nærheten som har et WLAN-kort i PC-en. Mange som bor i blokk har erfart at egen PC automatisk har logget seg på et trådløst nettverk hos en av naboene. Blant brukere med tvilsomme eller kriminelle hensikter er det visstnok blitt populært å gjøre bruk av slike åpne nettverk, slik at de elektroniske sporene fra deres aktiviteter leder til en annen persons IP-adresse. Begrepet *war-driving* brukes nå i USA om det å kjøre rundt i gatene på jakt etter ubeskyttede WLAN-soner.

Ambivalent anonymitet

Nettopp det faktum at kriminelle gjør alt de kan for å forbli anonyme og slik unngå å bli stilt til ansvar for sine handlinger, gjør at mange mener at mulighetene til å opptre anonymt må være begrensede. Elektronisk kommunikasjon er et svært potent teknologiområde i den forstand at det lar mennesker kommunisere raskt og enkelt med andre nesten uansett hvor de måtte oppholde seg i verden. I den grad slik kommunikasjon kan gjennomføres fullstendig anonymt (usporbart), er den et hensiktsmessig hjelpemiddel i planlegging og koordinasjon av terrorhandlinger, eller annen alvorlig kriminalitet. Bilder av seksuelle overgrep mot barn (barnepornografi) utveksles angivelig også i ly av anonymiserende tjenester på internett. På bakgrunn av denne muligheten for kriminelle til å gjemme seg bak anonym kommunikasjon, har en rekke aktører tatt til orde for at anonymiteten på internett må innskrenkes. Denne tanken har unektelig mye for seg, men saken har også en annen side som taler for forsiktighet med innskrenkninger i anonymitetens kår.

Riktignok er det et faktum at anonymitet kan brukes til å gjemme seg unna og unndra seg ansvar for sine handlinger eller uttalelser. Men det er også slik at anonymiteten støtter essensielle elementer i et fungerende demokrati, og er en forutsetning for ivaretakelsen av grunnleggende friheter og rettigheter. For personvernet er det helt grunnleggende at man kan ha utstrakt kontroll med hvem som kan få vite hvem man er. Dette er en selvfølge i den fysiske verden, hvor man bare i helt spesielle situasjoner må fortelle hvem man er. Det er også en forutsetning for folks tillit til at de trygt kan bruke tjenester på internett, at ikke andre kan se hvem de er. Anonymiteten er nemlig også en viktig forutsetning for personlig sikkerhet i en verden hvor ikke alle er til å stole på. Det er gode grunner til at man er tilbakeholden med å oppgi navn, adresse og telefonnummer til fremmede man støter på. Slik informasjon tiltror man bare mennesker eller aktører man føler seg trygg på, og slik må det så langt som mulig være også på internett.

Følgende er sentrale grunner til å forsvare anonymiteten også på internett:

- *Personvern*
  Retten til å opptre anonymt bidrar til å sikre menneskeverdet og individets autonomi, gjennom at den enkelte i større grad kan trekke grensene mellom seg selv og omverdenen, og selv bestemme over frigivelsen av informasjon om seg selv. Anonymitet fungerer dessuten som en beskyttelse mot ulike myndigheters overvåkning av enkeltmenneskets gjøren og laden i hverdagen. Uansett om man måtte mene at den norske stat er fri for uforholdsmessig overvåkning, er internett et grenseløst sted hvor alle stater kan overvåke etter beste evne, og det er en kjent sak at flere gjør det. Anonym-

iteten beskytter også mot pågående kommersielle interesser som vet å utnytte de personopplysninger de måtte få tak i. Slike opplysninger har betydelig økonomisk verdi, og utnyttes blant annet til nærgående reklame og spam.

- *Demokratihensyn*
  Personvernhensyn som autonomi og frihet fra overvåkning underligger også et velfungerende demokrati. Valg i Norge er frie og hemmelige, og derfor må prosessen for stemmegivning sikre anonymitet knyttet til avgitte stemmer. Ingen skal kunne holdes ansvarlig for sin stemmegivning. Anonymiteten sikrer ikke bare frie valg, men støtter organisasjonsfriheten samt en robust ytringsfrihet, ved å skape rom for dissens og kritikk mot sterke parter som ellers kunne sanksjonere mot de annerledes tenkende.
- *Personlig sikkerhet*
  Flere former for kriminalitet vil kunne blomstre hvis elektroniske spor blir mindre anonyme og således lettere identifiserbare. Identitetstyveri er det fremste eksempelet på dette, hvor personopplysninger utnyttes til økonomisk vinning gjennom kredittkortsvindel, låneopptak i offerets navn eller lignende misbruk av offerets identitet. Personforfølgelse (stalking) og innbrudd i bolig kan bli enklere hvis kriminelle lettere kan identifisere sine utvalgte ofre på nettet. Bortfall av anonymitet ville gjøre utnyttelse av barn og unge enklere. Alle foreldre vet at anonymitet er grunnregel nummer én for barn på internett.

Et eksempel som kanskje ikke føles så relevant for nordmenn i dag, er at anonymitet kan være viktig for å beskytte grunnleggende menneskerettigheter under totalitære regimer. Lite visste de som laget registre over jødene i Norge før andre verdenskrig, at nazistene senere kom til å bruke disse for effektivt å spore opp og deportere jødene under krigen. Og selv om det kan synes søkt å ta høyde for at et totalitært regime igjen kan påtvinges vårt land, er dette med totalitære regimer noe man bør tenke minst to ganger på. Man skal ikke gå lenger enn til nabolandet Russland for å finne et land hvor presse- og ytringsfriheten har atskillig trangere kår enn her hjemme, og hvor behovet for beskyttelse mot statens intoleranse mot opposisjon gjør anonymiteten ekstra viktig. Hvilken vekt som skal legges på denne type hensyn i Norge kan diskuteres, men det er et faktum at den elektroniske verden på internett i liten grad kjenner nasjonale grenser, og at det er store muligheter for å overvåke elektronisk kommunikasjon for regimer som måtte ønske det.

Anonymiteten er som vi kan se et tveegget sverd som er alt for viktig til at vi kan leve uten den, men som samtidig kan gjøre det vanskeligere å holde borgerne ansvarlige for sine handlinger. Hvor grensene for anonymiteten skal gå er det ikke enkelt å gi et svar på.

Se Kapittel 8 for mer om hvordan man kan oppnå anonymitet i elektronisk kommunikasjon.

Pseudonymitet

Anonymitet utgjør et ytterpunkt på en skala hvor vi finner full identifikasjon på den andre. Pseudonymitet er et begrep som kan sies å dekke området mellom disse ytterpunktene. Ved pseudonym kommunikasjon opptrer en bruker under pseudonym, altså et brukernavn som fortrinnsvis avviker fra hennes virkelige navn. Avhengig av hvordan løsningen er utformet, kan det være alt fra svært vanskelig til ganske enkelt å finne ut hvem som står bak et pseudonym. Man kan lage løsninger hvor brukerne er anonyme med mindre de selv gjør noe for å identifisere seg – dette krever at løsningen er bygd på anonymiserende teknologi, ettersom infrastrukturen på internett for vanlige brukere ikke er anonym. Pseudonymitet

gjør det mulig å la brukeren opptre anonymt, samtidig som hun kan holdes ansvarlig for det hun gjør.

Den enkleste formen for pseudonymitet på nettet i dag, og den som alle brukere intuitivt forstår, er å bruke konstruerte brukernavn på chat-tjenester og i online diskusjonsfora, samt en "anonym" e-postkonto hos Hotmail, Yahoo! eller andre hvor man ikke har registrert sitt eget navn. Dette er det absolutte minimum av pseudonymitet som brukere blir anbefalt å skjule seg bak når man kommuniserer med fremmede mennesker på internett. Med unntak av små barn, skjønner de fleste at det er risikabelt å oppgi identifiserende person-opplysninger som adresse og telefonnummer til folk man ikke vet om man kan stole på.

Slik pseudonymitet kan i mange tilfeller være en god avveining mellom brukerens behov for å beskytte seg mot åpen identifikasjon på nettet og samfunnets behov for å kunne stille borgerne til ansvar for sine handlinger. Så lenge man ikke bygger pseudonymiteten på en anonymiseringsløsning, er det som regel mulig for politiet å finne ut fra hvilken internett-konto en gitt pseudonym bruker opererte på et gitt tidspunkt. Til det trenger de kun å vite hvilken IP-adresse som har vært i bruk, og så må de se på internettleverandørens IP-logg for å se hvilken konto som hadde den aktuelle IP-adressen på det aktuelle tidspunktet. Hvis brukeren har benyttet en pseudonymiseringstjeneste ser hun anonym ut for omgivelsene, men politiet vil etter en rettskjennelse kunne få vite av pseudonymitetsleverandøren hvem som skjuler seg bak et gitt pseudonym.

Samtidig vil det for de fleste brukere ligge tilstrekkelig anonymitet i det at andre nett-brukere ikke kan finne ut hvem de er, bare fra å se pseudonymet eller e-postadressen de har som brukernavn. Men det krever at brukerne faktisk ikke oppgir sitt riktige navn ved registrering på den aktuelle tjenesten, ellers vil navnet dukke opp sammen med e-postadressen når man sender e-post.

Det som er det springende punkt i forhold til om slik "svak" pseudonymitet er tilstrekkelig for en bruker, er i hvilken grad andre enn politiet kan skaffe seg kjennskap til hvem som opptrer under et bestemt pseudonym. I situasjoner hvor det er svært viktig at ingen andre enn politiet kan spore opp identiteten til en pseudonym bruker, kommer denne enkle løsningen til kort. Ansatte hos internettleverandøren med tilgangsrettigheter til IP-loggene kan for eksempel lett gå inn og finne ut hvem som til ulike tider har hatt hvilke IP-adresser. Riktignok skal ikke de gå inn å se på slike data med mindre det finnes et spesielt behov, men er det viktig å være anonym for omverdenen, kan man knapt stole på organisatoriske rutiner og ansattes taushetsplikt. Det er nok med ett bruddent kar blant de med tilgang for at data skal kunne kompromitteres. Og selv med omfattende sikringstiltak er selv ikke slike loggfiler garantert mot innbrudd fra hackere. Det er med andre ord fortsatt behov for å kunne tilby anonym kommunikasjon for spesielle behov.

Vi har her gitt forenklede beskrivelser av begrepene anonymitet og pseudonymitet. For mer presise og tekniske beskrivelser av disse og relaterte begreper, se [31].

Når det gjelder ulike grader av identifikasjon er det ikke bare snakk om anonymitet og pseudonymitet. I enkelte tilfeller må man bare vite hvem man forholder seg til. For en tjenesteleverandør som har behov for å kunne holde en bruker ansvarlig, er det nødvendig

[31] Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology http://freehaven.net/anonbib/cache/terminology.pdf

på et eller annet vis å verifisere brukerens identitet. Da må man sjekke hvem man faktisk har med å gjøre.

5.4 Autentisering

Identifisering handler om å finne ut hvem noen er. Det innebærer altså å finne svar på spørsmålet "hvem er du?" Nært knyttet til identifisering er begrepet *autentisering* som handler om å verifisere noens identitet, det vil si å finne svaret på spørsmålet "er du virkelig den du hevder å være?"

Autentisering vil normalt skje av to ulike grunner. I de fleste tilfeller dreier det seg om at adgangen til tjenester eller informasjon må begrenses, eller at ressurser må beskyttes. Da må det kontrolleres at kun de som skal ha adgang faktisk får det. For å gjøre dette er det nødvendig å autentisere brukeren, for å verifisere vedkommendes adgangsrettigheter før tilgang gis. Den andre grunnen til å autentisere brukere er et eventuelt behov for å kunne holde dem ansvarlige for sine handlinger.

Stadig flere tjenester tar i bruk systemer for autentisering for å gi brukere tilgang. Elektronisk handel og digitale forvaltningstjenester er to sentrale drivere for stadig mer sofistikerte systemer for autentisering. Det finnes et bredt utvalg av teknologier for dette formål, og en stadig større mengde av tjenester som krever en eller annen form for autentisering. Og selv om det ofte ikke er nødvendig, gjør nesten alle slike systemer bruk av personopplysninger i prosessen. Dette gir grunn til bekymring på personvernets vegne.

Autentisering er et komplekst begrep som er nært knyttet til både sikkerhet og personvern. Det er instruktivt å skille mellom autentisering på tre nivåer:

- Autentisering av et *individ*
  vil si å etablere en gitt grad av sikkerhet for at en identifikator refererer til et gitt individ, det vil si en fysisk person.
- Autentisering av en *identitet*
  vil si å etablere en gitt grad av sikkerhet for at en identifikator refererer til en gitt identitet (ofte virtuell). Det kan være mulig å knytte den autentiserte identiteten til en faktisk person, men det trenger ikke å være det.
- Autentisering av et *attributt*
  vil si å etablere en gitt grad av visshet om at et attributt eller en egenskap innehas av en gitt bruker, for eksempel alder.

Både hvorvidt man velger å autentisere eller ikke, samt hvilken form for autentisering man eventuelt velger for en bestemt tjeneste, har store konsekvenser for personvernet. Det er derfor viktig at graden av autentisering er tilpasset formålet, og at det ikke brukes sterkere og mer nærgående metoder enn nødvendig.

Individuell autentisering
Individuell autentisering innebærer at man sjekker hvilken fysisk person man har med å gjøre, ved at brukeren bes presentere et bevis på hvem hun er i den virkelige verden. Dette innebærer at alle elektroniske spor fra en persons bruk av den aktuelle tjenesten vil kunne knyttes til den personen som individ. En stor andel av den autentisering som skjer i den fysiske verden foregår på individnivå. Slik autentisering er knyttet til framvisning av identitetsbevis, som for eksempel pass eller førerkort. Dette er for mange den eneste form

for autentisering som de har et forhold til, og dessverre medfører dette at mange ikke er klar over at det finnes andre og mer personvernvennlige måter å gjøre det på i den virtuelle verden. Slik autentisering kan foregå på mange ulike måter, og styrken i valgt metode avgjør hvor sikker man kan være på at brukeren faktisk er den person hun hevder å være. Sterk autentisering (som for eksempel ved bruk av biometri) brukes mest til autentisering på individnivå, altså i tilfeller hvor man må vite hvem en bruker faktisk er.

Identitetsmessig autentisering
Autentisering av en identitet innebærer å sjekke at en bruker er den rettmessige innehaver av en gitt (gjerne virtuell) identitet. Ofte er det helt unødvendig for en tjenesteleverandør å få vite navn og nummer på den person som ønsker å gjøre bruk av en tjeneste, og da er det upassende å be om slik legitimasjon. Virtuelle identiteter vil vanligvis være pseudonyme, altså utformet slik at de under normale omstendigheter ikke kan knyttes til et individ. I helt spesielle situasjoner, som for eksempel i politimessig etterforskning, kan dette likevel være mulig. Tilknytningen til fysisk person vil da kunne foretas av den eventuelle identitets-leverandøren eller av internettleverandøren som kan spore IP-adressen.

Kommersielle tjenester kan for eksempel klare seg med å autentisere en virtuell bruker-identitet som en registrert kunde med bestemte rettigheter, og trenger ikke vite hvem som står bak med mindre det oppstår behov for kredittvurdering eller lignende. Mange brukere vil holde seg unna kommersielle aktører som krever autentisering av fysisk person, fordi de vil unngå altfor nærgående personprofilering og direkte markedsføring.

Tjenester for bygging av sosiale nettverk eller for å finne en partner (dating- eller chat-tjenester) er et annet eksempel hvor det normalt ikke vil autentiseres på individnivå, men på virtuell identitet. Slike tjenester må sikre seg at kun den rettmessige bruker anvender et bestemt brukernavn og at denne brukeren har tilgang til de tjenester som hun eventuelt har betalt for. En form for autentisering er derfor nødvendig – normalt kun brukernavn og passord. Brukerne er derimot lite interessert i at deres aktivitet i denne typen tjenester skal kunne knyttes direkte til deres person. Mange vil oppleve at dette kan utgjøre en trussel mot deres individuelle sikkerhet, selv om slik informasjon i utgangspunktet kun er tilgjengelig for enkelte ansatte hos tjenesteleverandøren.

Attributtautentisering
Ved å autentisere en bruker kun i forhold til et attributt (eller egenskap) er det mulig å sikre adgangen til anonym bruk av en tjeneste. For eksempel kan man ved online filmutleie autentisere brukeren i forhold til den aktuelle aldersgrense, slik at brukeren ikke får lastet ned en film med 18-årsgrense hvis hun ikke kan fremvise et bevis for at hun er minst 18 år gammel. Anonyme elektroniske penger bygger på løsninger for attributtautentisering. Butikken spør da ikke hvem brukeren er, men sjekker kun at hun har den nødvendige sum e-cash for den varen hun vil kjøpe.

Parallellen til denne mekanismen i den fysiske verden vil normalt måtte basere seg på at fysisk observasjon gjør ytterligere legitimasjon unødig. Kontante penger er et godt eksempel. For å få kjøpt avisen er det avgjørende attributt om man har 10 kroner på seg. Om så er tilfelle vil selgeren ikke spørre hvem kjøperen er. Et annet eksempel er en voksen person som går på kino for å se en film med 7-års aldersgrense. Billettkontrolløren vil da se at kunden er over 7 år, og gi adgang uten å be om bevis for alder.

Ved tvilstilfeller vil derimot kontrolløren kunne be om legitimasjon fra kinogjengeren. Til tross for at det kun er kundens alder som er av interesse i denne situasjonen, vil hun måtte vise legitimasjon som gjerne inneholder både navn, personnummer og ansiktsbilde i tillegg til fødselsdatoen. I den fysiske verden må man altså ofte ty til individuell autentisering, selv om kun et attributt er av interesse. Da resulterer autentiseringen i unødig behandling av tildels sensitive personopplysninger. Heldigvis vil kontrolløren normalt kun se på fødselsdato i slike tilfeller, og om hun skulle se kundens navn eller personnummer vil hun sannsynligvis glemme det etter kort tid.

Slike mekanismer som selektiv oppfattelse og at man glemmer detaljer er ikke egenskaper ved den elektroniske verden. All den overskuddinformasjon som måtte komme ut av en individuell autentisering vil bli lagret sammen med andre loggdata om transaksjonen, og vil umiddelbart vært sårbar for innsyn og distribusjon. Her er ingen glemsel, og identifiseringen gjør personnummeret like tilgjengelig som fødselsdatoen. Dette illustrerer hvorfor det er viktigere å begrense autentisering på individnivå i den elektroniske verden enn det er i den fysiske.

5.4.1 Teknologier for autentisering

Tre ulike typer av karakteristika brukes normalt for å autentisere noens identitet:

- Noe man *vet* (oftest passord eller PIN-kode)
- Noe man *har* (legitimasjon, smartkort eller annen type bevis)
- Noe man *er* (fysiske karakteristika - biometri)

Vi skal i denne rapporten ikke gå inn på hvordan ulike former for autentisering fungerer, men vi skal gi en oversikt over hvordan autentisering kan påvirke personvernet. For en nærmere innføring i teknologier for autentisering og med fokus på personvern, se Kent & Millett (2003).

Ulike autentiseringsteknologier har sine spesielle utfordringer også i forhold til personvernhensyn. Vi skal kort nevne hvordan de vanligste teknologiene kan virke på personvernet:

Passordløsninger
Autentisering ved hjelp av brukernavn og passord er fortsatt den vanligste metoden for å begrense tilgang til nettbaserte tjenester og ressurser. Metoden har klare svakheter fra et sikkerhetssynspunkt. For eksempel er passord ofte lette å gjette, de skrives ofte opp av brukeren, de sendes gjerne ukryptert over nettet slik at de lett kan fanges opp av utenforstående, og dessuten bruker gjerne en person samme passord på mange steder. Siden autentisering på nettet normalt ikke er toveis (brukeren autentiserer ikke nettstedet for å være sikker på at det er det riktige), er det fare for at brukeren kompromitterer sitt passord ved å oppgi det til en falsk nettside. For personvernet kan det være et problem at sikkerheten med metoden ikke er spesielt god. På den annen side er det gunstig for personvernet at brukere kan benytte tjenester hvor man selv kan finne på et brukernavn og passord, og ikke trenger å avsløre sin faktiske identitet.

PKI
Public key infrastructure (PKI) er en metode for autentisering som er basert på kryptografiske teknikker og en offentlig sertifiseringsmyndighet (tiltrodd tredjepart), som kan

verifisere at en gitt kryptonøkkel tilhører en bestemt bruker. PKI er allerede i bruk innenfor begrensede områder, men forventes innført på bred skala som autentiseringsmetode for den digitale forvaltning, med tilhørende utrulling av digitale identiteter og sertifikater til landets innbyggere. En svært omfattende PKI kan være problematisk for personvernet fordi en og samme ID da vil bli brukt i mange sammenhenger, noe som gjør det lettere å samle informasjon om enkeltindivider. Dessuten er det problematisk at så mye informasjon vil være samlet sentralt hos en offentlig sertifiseringsmyndighet, som slik bli særlig sårbar for angrep utenfra og for lekkasjer fra interne utro tjenere. Fra personvernståsted er det å foretrekke med flere mindre PKI-er hvor man har ulike identiteter som brukes i ulike sammenhenger.

Biometri
Biometri er automatisk identifikasjon eller verifikasjon av identitet basert på fysiologiske kjennetegn. Metoden skiller seg fra de andre på den måten at den ikke baserer seg på delte hemmeligheter. Snarere registrerer og lagrer man det som forutsettes å være et unikt fysiologisk kjennetegn, for senere å kunne matche nye registreringer med den lagrede. Mest vanlig er det å bruke fingeravtrykk, avbildning av regnbuehinnen (iris) eller stemmeanalyse til autentisering. Det faktum at biometriske kjennetegn ikke er hemmeligheter og ikke kan endres om de blir kompromittert, gjør at det er særdeles viktig å unngå at noen kan fange opp de dataene som representerer en biometrisk registrering. Systemer hvor biometriske data sendes over nettet og sammenlignes med lagrede versjoner på sentrale servere bør unngås. Årsaken er faren for at data kan kompromitteres ved angrep på den sentrale serveren eller ved avlytting av overføringen. Sikker kryptering av data både under overføring og ved lagring på server, kan gjøre sentrale systemer mer akseptable, men risikoen vil fortsatt være så høy at slike løsninger ikke er å anbefale.

Av personvernhensyn bør derfor biometri kun brukes helt lokalt, for eksempel for å aksessere beskyttet informasjon på et smartkort eller for å logge seg på en bærbar PC, mens man bør unngå lagring av biometriske data på sentraliserte autentiseringsservere.

5.4.2 Autentisering og personvern

Autentiseringsteknologier er gjerne i utgangspunktet mer nøytrale i forhold til personvern enn det mange tror[32]. Autentisering kan anvendes på måter som både styrker og svekker personvernet. Hvordan teknologiene implementeres i systemer og kommer til anvendelse er det som primært avgjør hva som blir de personvernmessige konsekvensene. Autentiseringsløsninger som er beregnet på å begrense tilgangen til personopplysninger er for eksempel svært viktige for å sikre personvernet forbundet med lagret informasjon som kan knyttes til personer. På den annen side er det på grunn av lav bevissthet omkring personvern svært vanlig å implementere autentisering på en måte som kan være til belastning for personvernet.

Følgende fire risikoområder for personvernet er de viktigste knyttet til bruk av autentiseringsløsninger:

- *Skjult identifisering*
  Enkelte autentiseringsteknologier gjør det mulig å identifisere et individ uten at den

[32]Kent og Millett (2003)

berørte vet om det. Slike skjulte identifiseringsmetoder unndrar seg samfunnets og den enkeltes innsyn og kontroll, og er derfor svært sårbar for misbruk.

- *Overbruk av autentisering*
  Ulike trender drar i retning av en sterk økning i bruken av autentisering av brukere, både i privat og offentlig sektor. Ettersom prisen på autentiseringsløsninger synker og tilgjengeligheten av slike løsninger øker, kan man vente at mange vil velge å autentisere brukere, også i tilfeller hvor dette strengt tatt ikke er nødvendig. Dette kan virke svært negativt på personvernet fordi
- *Uforholdsmessig aggregering av personopplysninger*
  Bruk av en enkelt identifikator (som for eksempel personnummer) eller et lite antall identifikatorer, gjør det lettere å koble tidligere separate registre med personopplysninger. Hvis ett enkelt autentiseringssystem innføres på tvers av offentlig og privat sektor, vil dette kunne uthule personvernet ved at det blir alt for lett å koble informasjon som er lagret hos ulike aktører.
- *Innskrenkning av frihet og autonomi*
  Alle tilfeller av individuell autentisering innebærer en mulighet for sosial kontroll. Mens dette er på sin plass i spesielle situasjoner som krever høy grad av sikkerhet og ansvarliggjøring, kan det ha uønskede effekter i forhold til livsutfoldelse og deltakelse i samfunnet hvis det brukes på andre områder.

Den amerikanske organisasjonen Center for Democracy and Technology (CDT) framhever følgende seks personvernprinsipper for autentiseringsløsninger [33]:

- *Gi brukeren kontroll*
  Brukere bør gi informert samtykke før informasjon brukes til autentisering og påfølgende bruksområder. Brukere bør ikke tvinges til godta at informasjon deles med andre for sekundære formål som forutsetning for å bruke autentiseringssystemet.
- *Støtte ulike typer autentiseringstjenester*
  Brukere bør kunne velge fra et utvalg av leverandører av autentiseringstjenester. Personvernet er utsatt hvis en enkelt identifikator må brukes til mange ulike formål. Autentisering bør ikke fungere som en "universalnøkkel", men brukerne bør ha en nøkkelring med ulike "nøkler" for ulike formål. Ulike aktører vil antakelig ha behov for ulike typer av autentisering.
- *Bruke individuell autentisering kun når dette er nødvendig*
  Autentisering som bruker identitet er utsatt for misbruk og kan øke faren for identitetstyveri. For å muliggjøre brukerkontroll bør man så langt som mulig bruke autentiseringssystemer basert på pseudonyme identifikatorer eller anonyme attributter.
- *Gi informasjon til brukeren*
  Brukere bør ved bruk av autentiseringstjenester informeres klart og enkelt om hvilken informasjon som samles inn og hvordan den vil bli brukt, slik at de kan ta informerte beslutninger om bruk av systemet.

[33] Center for Democracy and Technology: *Privacy Principles for Authentication Systems* http://www.cdt.org/privacy/authentication/030513interim.pdf

- *Minimere innsamling og lagring*
  Et autentiseringssystem bør ikke samle inn og lagre annen informasjon enn den som er nødvendig for å gjennomføre autentiseringsfunksjonen.
- *Ansvarliggjøre autentiseringsleverandører*
  Leverandører av autentiseringstjenester bør kunne verifisere om de opererer i henhold til gjeldende personvernlovgivning og aktuelle personvernprinsipper. Retningslinjer for ivaretakelse av brukeres personvern er sentralt for å sikre brukernes tillit til autentiseringsløsninger. Opplæring og jevnlig kontroll er nødvendig for å sikre etterlevelsen av aktuelle krav og retningslinjer.

Oppsummerende skal det sies at både mengden av aktiviteter og tjenester som krever autentisering, samt måten mange slike systemer er utformet på, gir grunn til ettertanke omkring konsekvenser for personvernet. Foreløpig er sterke autentiseringsløsninger som PKI/digital signatur og biometri lite utbredt, men når vi ser noen år framover er det grunn til å tro at konsekvensene av unødig autentisering kan bli mer akutte. Grunnene til dette er at teknologier for autentisering blir mer nærgående samtidig som den strøm av elektroniske spor som vil kunne knyttes til personer blir stadig tettere og mer avslørende i forhold til personopplysninger.

Kapittel 6 IKT og elektroniske spor

Når vi ser på nye informasjons- og kommunikasjonsteknologier og deres innvirkning på personvernet, er det en fare at man kan betrakte følgene som uunngåelige. Faktum er at teknologiene ikke i seg selv bestemmer hvordan de skal virke på personvernet. Avgjørende i så måte er spørsmålet om hvordan teknologiene kommer til anvendelse og under hvilke forutsetninger. De fleste av teknologiene vi beskriver her kan utnyttes på en måte som ivaretar personvernet, men de kan også brukes på måter som medfører belastninger for personvernet. Vi vil i dette kapitlet konsentrere oss om teknologienes potensial til å utfordre personvernet og si noe om på hvilke måter de kan gjøre dette.

Digitaliseringen av informasjonsstrømmene i samfunnet, kombinert med utviklingen innen datakommunikasjon og datalagring, har medført at informasjon er mye enklere og billigere å lagre og distribuere enn tidligere. Informasjon kan således mye lettere enn tidligere komme på avveie, enten som følge av bevisst handling eller som resultat av et uhell eller sikkerhetssvikt. Det er videre et faktum at mye av den elektroniske kommunikasjon som foregår sendes via usikrede linjer på internett, noe som medfører betydelig risiko for utilsiktet spredning av informasjon. I denne situasjonen er det interessant å se nærmere på hvilken informasjon man bevisst eller ubevisst kan legge fra seg i form av elektroniske spor i ulike sammenhenger. Før vi gjør dette, tar vi en rask gjennomgang av hvilke viktige teknologier som ligger bak digitaliseringen av informasjonsstrømmene og økningen i kapasiteten til raskt og effektivt å behandle store informasjonsmengder.

6.1 Muliggjørende teknologier

Et sett av grunnleggende informasjons- og kommunikasjonsteknologier kan sies å legge grunnlaget for den utviklingen vi ser med utbredt innsamling, lagring, prosessering og distribusjon av elektronisk informasjon.

Datalagring og prosesseringskraft
Generelt blir alle lagringsmedier billigere, samtidig som kapasiteten øker. Dette gjør det mulig å lagre stadig større datamengder til en rimelig kostnad. Selv om det fortsatt på ingen måte er trivielt å håndtere lagring av svært store datamengder, bidrar dette faktum til at det blir mulig for stadig flere å lagre stadig mer informasjon over tid. I mange tilfeller gir dette seg utslag i at behovet for å slette informasjon forsvinner.

En illustrasjon på dette er Google som nå tilbyr en gratistjeneste for web-basert e-post som de kaller Gmail og som gir brukerne en postboks med 1 GB (1000 MB) lagringsplass[34]. Fram til 2004 tilbød aktører som Hotmail og Yahoo! kun 2-4 MB lagringsplass til slike gratis e-postkontoer. Ideen bak Gmail er at brukerne ikke skal behøve å slette e-post, men snarere i framtida fortsatt skal kunne søke seg fram til all gammel e-post. Google ønsker også å tilby skreddersydd reklame basert på innholdet i brukernes post. Slik tjener dette eksemplet som en god illustrasjon på hvordan økt datalagring kan bidra til å utfordre personvernet.

[34]CNet News.com, 01.04.2004: *Google to offer gigabyte of free e-e-post* http://news.com.com/2100-1032-5182805.html?tag=nl

Stadig økende prosesseringskraft gjør det lettere å behandle store mengder data. Det finnes i dag sofistikert teknologi for å bedre kunne nyttiggjøre seg store mengder informasjon. Uviklingen innen avansert databaserelatert teknologi som datavarehus (data warehousing) og datautvinning (data mining) gjør det mulig å lete i data på tvers av en rekke databaser, og å finne skjulte sammenhenger i det som kan oppfattes som en uhåndterlig stor mengde data. Slik teknologi gjør det mulig å effektivt nyttiggjøre seg spor som lagres, til tross for at det lagres enorme mengder spor fra et stort antall brukere.

Datakommunikasjon
Utviklingen innen teknologier for datakommunikasjon har antakelig hatt den aller mest merkbare effekten for brukerne de siste 10-15 årene. Mens PC-er tidligere for det meste var isolerte maskiner, ble de i 90-årene koblet opp mot omverdenen. Billige modemer ble tilgjengelige, og internett bredte for alvor om seg fra rundt 1993. En grunnleggende teknologi som underligger dette kvantespranget i kommunikasjonsteknologi er det som kalles pakkesvitsjing. Mens datakommunikasjon fra A til B tidligere måtte legge beslag på en hel linje mellom de to punktene (linjesvitsjing) og derfor var relativt kostbar, er pakkesvitsjede nettverk mer fleksible, robuste og kostnadseffektive. I pakkesvitsjet kommunikasjon sendes for eksempel en e-post som mange små pakker som alle er adressert til samme sted, men som ikke trenger ta samme veien gjennom nettet. Denne teknologien gjør det mulig å la kommunikasjonstjenester være ”alltid på” siden de ikke beslaglegger en linje, men bare sender datapakker ved behov.

Av andre viktige grunnleggende teknologier er det verdt å framheve fiberoptisk kommunikasjon og teknologier for trådløs kommunikasjon. Fiberoptikk står i en særstilling som den teknologi som muliggjør den utbredelse av bredbåndsforbindelser vi ser i dag. Elektronisk kommunikasjon overføres gjennom tykke bunter av fiberoptiske kabler mellom knutepunktene i det norske stamnettet. Vanlige brukere kobler seg normalt til nettet gjennom kobberkablene i telefonlinja (oppringt forbidelse over modem eller ADSL) eller via koaksialkabelen til kabel-TV (kabelmodem), mens de aller mest avanserte bredbåndstjenestene krever fiberoptisk kabel helt fram til husveggen.

Utbredelsen av bredbåndslinjer både i de fleste bedrifter og organisasjoner, samt hos stadig flere private brukere, bidrar til å øke mengden av elektronisk kommunikasjon. Dette fordi tjenestene da blir tilgjengelige hele tiden, og fordi bruken ikke utløser ekstra kostnader. Samtidig gjør dette at tilbøyeligheten til å dele og distribuere informasjon blir større, ettersom dette kan gjøres uten kostnader. Det er også grunn til å tro at bredbåndstjenester øker bruken av internett til ulike typer kommunikasjonsaktiviteter ettersom et stort tilbud av tjenester og sosiale arenaer blir enkelt og som regel gratis tilgjengelige.

6.2 Elektroniske spor

Elektroniske spor kan være alt fra digitale ”fotavtrykk” som forteller at man har vært et sted til en gitt tid, til detaljerte personopplysninger man legger fra seg ved bruk av en webtjeneste på internett. Mange typer elektronisk utstyr lagrer av ulike hensyn logger over bruken. Typisk forteller elektroniske spor om aktiviteter, transaksjoner, kommunikasjon eller bevegelser og vil gjerne inneholde informasjon om hva, når, hvor og ofte også hvem.

I mange tilfeller er det helt nødvendig at det lagres slik informasjon og i disse tilfellene vil da også brukeren som regel forvente at så skjer. Et eksempel på dette er uttak i minibank, hvor det elektroniske sporet av transaksjonen gjør det mulig å trekke riktig beløp fra riktig konto.

I andre tilfeller er det ikke åpenbart at det må lagres informasjon om bruken av elektronisk utstyr, og i mange slike tilfeller vil brukerne heller ikke være klar over at så skjer. For eksempel er det ikke vel kjent at mange moderne kopimaskiner lagrer de scannede bildene av alle sidene den har kopiert på en harddisk som normalt aldri slettes. En slik disk vil etter hvert kunne inneholde mye sensitiv informasjon uten at brukerne er klar over det, men som potensielt kan misbrukes av en som vet.[35]

Velkjente eksempler
Følgende er eksempler på velkjente og klassiske former for elektroniske spor. Vi vil i denne rapporten ikke bruke mye plass på disse teknologiene og anvendelsene ettersom de anses relativt velkjente:

- *Betalingskort og nettbank*
  Alle økonomiske transaksjoner som er knyttet til bruk av betalingskort eller nettbank vil registreres elektronisk og lagres i en database. All betaling av regninger og overføring mellom konti vil også registreres elektronisk selv om brukeren ikke bruker nettbank. Transaksjoner knyttet til en konto vil for en gitt periode listes opp i en kontoutskrift som sendes brukeren, og således kan tjene som et svært håndgripelig eksempel på elektroniske spor. Nettopp på grunn av denne kontoutskriften må brukerne forventes å være seg bevisst at økonomiske transaksjoner setter spor, så dette skulle ikke overraske noen.
- *Autopass*
  En stor andel av bilistene i de største byene har etter hvert skaffet seg en abonnementsbrikke til å klistre på frontruta som lar dem passere bomstasjoner uten å stå i kø. Passeringen registreres elektronisk av en antenne ved bomstasjonen og betaling skjer automatisk, for eksempel ved trekk fra et forhåndsbetalt "klippekort". En bieffekt av at det blir enklere å betale bomavgift er at informasjon om en bils passeringer gjennom ulike bomanlegg registreres og lagres for en periode av hensyn til evt. klager.
- *Adgangskort*
  Stadig flere arbeidsplasser beskyttes mot uvedkommendes adgang gjennom bruk av adgangskort istedenfor nøkkel. En konsekvens av dette er at det blir lagret informasjon om hvem som går inn på arbeidsplassen og til hvilke tidspunkter.
- *Overvåkningskamera*
  Installasjon av faste videokameraer til overvåkning av offentlige steder, private butikker og andre steder med beskyttelsesbehov har bredt om seg de senere år og oppfattes av mange som en trygghetsskapende faktor. Kameraene har primært til oppgave å forhindre kriminalitet samt bidra til oppklaring av lovbrudd eller forsvinninger. Bilder fra slike overvåkningskameraer gir som regel ingen entydig identifikasjon av menneskene på bildene, slik at noen må granske bildene på jakt etter en person man kjenner utseende til for å ha utbytte av dem. Teknologi for videobasert, automatisk fjerngjenkjenning av mennesker basert på ansiktsgeometri finnes allerede og blir stadig bedre, men foreløpig fungerer dette relativt dårlig. Bilder fra overvåkningskameraer lagres i mange tilfeller ikke, og sjelden over lenger tid.

[35] Ibas, 17.11.2003: Sensitiv informasjon lagres på kopimaskiner. http://www.ibas.no/nyheter/articles/NO-2003-11-17.news

6.2.1 Kommunikasjonsdata

Teletrafikk har lenge vært forbundet med lagring av store mengder elektroniske spor i form av kommunikasjonsdata. Hovedformålet med slik lagring har vært og er fortsatt behovet for å fakturere kunden etter bruk av teletjenester. Det er vanlig å betrakte data om elektronisk kommunikasjon som bestående av følgende tre typer: trafikkdata, lokasjonsdata og innholdsdata. Slike kommunikasjonsdata kan igjen ved behov knyttes til abonnementsdata, slik at de kan henføres til en spesifikk person som eier av det benyttede abonnementet.

Trafikkdata
Trafikkdata forteller noe forenklet hvem som har kommunisert med hvem, når kommunikasjonen fant sted og hvor lenge den varte. For fast- og mobiltelefoni vil trafikkdata fortelle hvilke telefonnumre som har vært involvert i samtaler, tekstmeldinger, telefakser, oppringt datakommunikasjon eller annen kommunikasjon som går over et fastlinje- eller mobilnettverk. Siden trafikkdata er knyttet til kommunikasjonsutstyr og ikke personer, er det ikke alltid mulig å fastslå hvilke personer som har kommunisert. Offentlige telefonbokser er eksempler hvor det ikke er en nær sammenheng mellom telefonnummer og person. I de fleste tilfeller er det derimot nær knytning mellom et telefonnummer og en enkelt person (for eksempel innehaveren av aktuelt mobilabonnement), eventuelt et lite antall personer (for eksempel en familie eller en arbeidsgruppe). Trafikkdata kan som regel knyttes til bestemte personer og er således å oppfatte som personopplysninger.

Lokasjonsdata
Lokasjonsdata forteller hvor de kommuniserende partene befant seg geografisk under kommunikasjonen. Dette er mest aktuelt for mobiltelefoni og i praksis lagrer en teleoperatør informasjon om hvilken basestasjon som ble brukt under et kommunikasjonsforløp. I GSM-nettet betyr dette at nøyaktigheten i de geografiske data som lagres om kommunikasjon er relativt lav, men god nok til å si med noen hundre meters nøyaktighet hvor telefonen befant seg da det ble kommunisert. I byer med større tetthet mellom basestasjonene vil nøyaktigheten være større enn andre steder. Man kan også ved bruk av flere basestasjoner eller satellitter beregne mer nøyaktige posisjoner for bruk til en lokasjonsbasert tjeneste. For fasttelefoni lagres ikke spesielle lokasjonsdata, men i slike tilfeller vil lokasjon være knyttet til nummeret ettersom denne type telefoner står fast installert på en bestemt adresse.

Innholdsdata
Innholdsdata er selve innholdet i kommunikasjonen. Det er hva som blir sagt i samtaler og skrevet i meldinger. Innholdsdata skal ikke lagres av teleoperatøren. Unntak fra dette kan kun skje i tilfeller hvor politiet ber om avlytting i forbindelse med etterforskning av en sak hvor det foreligger skjellig grunn til mistanke mot en bestemt person.

Tjenesteleverandører på internett kan derimot til en viss grad lagre også innhold fra kommunikasjon. Dette gjelder for eksempel nyhets- eller diskusjonsgrupper hvor poenget nettopp er å legge ut og lagre meningsytringer fra brukerne. Et annet eksempel er chat-rom hvor mennesker ”prater” skriftlig sammen på en slags ”åpen linje”. Slike åpne chat-rom modereres gjerne for å luke ut brukere som ikke holder seg til reglene for chat-rommet, og innhold fra chattesamtaler loggføres i mange tilfeller av tjenesteleverandøren for å kunne brukes i en eventuell politietterforskning.

Lagringstid for kommunikasjonsdata
Teleoperatører kan i dag lagre trafikk- og lokasjonsdata i inntil 3 måneder ved månedlig fakturering og i inntil 5 måneder ved kvartalsvis fakturering. Etter dette skal dataene slettes eller anonymiseres. Hvis en faktura er omtvistet, kan data likevel lagres inntil tvisten er løst. Lagring av kommunikasjonsdata er ikke obligatorisk, så operatører som ikke trenger trafikk-dataene for faktureringsformål, behøver heller ikke lagre dem. For mer om forslag til lagringsplikt for kommunikasjonsdata, se delkapittel 7.2.

IP-adresser og oppkoblingslogger
Et spesialtilfelle av trafikkdata er loggdata fra oppkoblinger til internett. Dette er data som oppbevares hos internettleverandører både av hensyn til fakturering (ved oppringt for-bindelse) og for å kunne treffe tiltak ved misbruk av abonnementsbetingelsene, eller utlevere data til politiet i en eventuell etterforskning. Slike oppkoblingslogger vil inneholde informasjon om når brukerne har koblet seg opp på internett, og hvilke IP-adresser de for hver gang har blitt tildelt.

IP (Internet Protocol) er den protokollen som brukes for entydig å adressere alle enheter som er tilkoblet internett. Alle data på internett må sendes mellom entydige adresser for å komme fram til riktig datamaskin. Slike adresser kalles IP-adresser, og for hver gang man skal på nettet må man ha en slik adresse. De fleste større bedrifter og organisasjoner har fast IP-adresse, slik at IP-adressen kan brukes direkte til å finne ut fra hvilken organisasjon en bruker kommer. De fleste private brukere ringer opp for hver gang de skal på internett og får da tildelt dynamisk IP-adresse, hvilket vil si at det vil være ulike adresser for hver gang de kobler opp forbindelsen til nettet. Private brukere med xDSL-linje (for eksempel ADSL), eller annen "alltid på"-forbindelse til nettet kan få tildelt fast IP-adresse, men det vanligste for slike er også dynamisk IP-adresse. Da får også disse en ny IP-adresse hver gang de slår på sin PC og bredbåndsmodem, men siden de gjerne er oppkoblet svært lenge hver gang, vil internettleverandøren med jevne mellomrom (typisk hver tredje time) loggføre hvilken IP-adresse som er knyttet til en linje.

Vernet om loggdata fra oppkobling til internett med tilhørende IP-adresser er svakere enn vernet om trafikkdata fra telefoni. Når politiet i forbindelse med en etterforskning har behov for tilgang til en oversikt over trafikken knyttet til en persons telefonnumre, er de avhengige av en rettskjennelse for å få dette. Ved etterforskning som innebærer undersøkelser av en persons kommunikasjon over internett trenger de derimot ingen slik kjennelse, men kan uten videre få utlevert informasjon fra internettleverandører om hvilken brukerkonto som på et gitt tidspunkt hadde en gitt IP-adresse. En brukerkonto med tilhørende IP-adresse vil derimot ikke alene entydig identifisere en person, ettersom andre enn abonnementets eier kan bruke vedkommendes konto for å koble seg til internett, for eksempel gjennom usikrede trådløse nettverk.

Mens private brukere tildeles en IP-adresse ved pålogging på internett som er helt unik for dem akkurat da, vil bedrifter og organisasjoner med fast IP-adresse som regel ha teknologi som gjør at alle brukerne deler på samme IP-adresse. Da vil alle brukerne derfra opptre med samme IP-adresse for omverdenen, mens adressekonvertering i brannmuren vil sørge for at innkommende trafikk likevel vil nå riktig bruker.

6.2.2 internett-relaterte teknologier

Internett og relaterte teknologier representerer en kommunikasjonsmessig revolusjon og det er ikke så lett å huske at internett for mindre enn 15 år siden var et heller ukjent begrep utenfor spesielt interesserte akademiske kretser. Spesielt i løpet av de siste 10 år har bruken av internett vært i sterk vekst og stadig flere tjenester har kommet til blant tilbudene man kan finne på nettet. E-post har vært den store "killer-applikasjonen", som har gjort at så mange har blitt internett-brukere. Akademisk kunnskapsspredning og kommersiell produktinformasjon har også lenge vært dominerende bruksområder for internett.

De siste seks-sju årene har vi sett en kraftig vekst i bruken av internett til økonomiske transaksjoner (nettbank), handelstransaksjoner (kjøp og salg av varer og tjenester) og etter hvert også transaksjoner knyttet til den offentlige forvaltning. Både i forretningsmessig virksomhet og i ikke-kommersielle organisasjoner er internett blitt et sentralt medium for informasjonsflyt og koordinering. Privatpersoner bruker nå dette mediet også til å bygge sosiale relasjoner som å finne nye venner, eller søke en partner. En stadig større del av menneskelig livsutfoldelse finner altså sin plass også på internett, og dette har konsekvenser for i hvilken grad elektroniske spor fra menneskers kommunikasjon og aktiviteter på nettet kan være problematisk i forhold til deres personvern[36].

E-post

Når en e-postmelding sendes fra en avsender til en mottaker vil meldingen bli lagret på flere steder. Primært skjer en mellomlagring av meldingen på avsenders og mottakers e-post-servere, hvor den blir liggende inntil mottakeren har lastet ned meldingen til sin PC. Det kan også skje en ytterligere mellomlagring av meldingen, for eksempel hvis mottaker bruker en ekstern leverandørs e-postserver for mottak av e-post, eller hvis en av serverne eller andre deler av forbindelsen har vært nede en periode. Mellomstasjoner ved transport av e-post vil altså normalt ligge i enten avsenders eller mottakers organisasjon, eller hos internett-leverandøren for private brukere. En person med de riktige adgangsprivilegier til slike mellomstasjoner vil kunne lese de midlertidig lagrede e-postmeldinger og ta kopi av disse.

Mens en e-post normalt vil ligge kun kortere tid på mellomliggende servere vil disse likevel ta vare på informasjon om meldingers avsender, mottaker og størrelsen på meldingen. Skulle det oppstå problemer med avleveringen av e-posten, kan den bli liggende et sted mellom 1 og 14 dager på en mellomstasjon utenfor både avsenders og mottakers kontroll, før den slettes og melding om dette sendes avsender.

Når en e-post er kommet fram til mottakeren, vil den enten automatisk bli slettet fra e-postserveren eller den vil fortsatt bli liggende der inntil brukeren aktivt sletter den. Hva som skjer avhenger av hvilken e-postprotokoll serveren bruker, samt hvordan e-postprogrammet på mottakerens PC er satt opp. Ved bruk av POP-protokoll (mest utbredt blant privatbrukere) vil meldinger bli slettet fra serveren når de lastes ned på brukerens PC, med mindre e-postprogrammet er satt opp til å la nedlastet post bli liggende på serveren. Ved bruk av IMAP-protokoll blir alle e-postmeldinger liggende på serveren inntil de slettes av brukeren. Også ved bruk av web-basert grensesnitt for lesing av e-post vil posten ligge på serveren inntil brukeren selv sletter den. Med Web-basert e-post kan innholdet i meldinger kan bli liggende igjen på maskinen i form av midlertidige filer som nettleseren lagrer, og som ikke

[36]Følgende beskrivelse er basert på IT-Sikkerhedsrådet (2002)

nødvendigvis slettes når nettleseren avsluttes. Slike filer kan derimot slettes manuelt av brukeren.

All e-post som lagres på server vil enkelt kunne leses og kopieres av systemadministrator og andre med riktige tilgangsrettigheter på serveren. Den eneste måten å sikre e-post mot uautorisert innsyn under transport og ved lagring på server, er ved å sende meldinger sikret med krypteringsteknologi (se Kapittel 6).

Enhver e-post vil utover selve innholdet i meldingen bære informasjon om avsenders og mottakers IP-adresse, samt hvilke adresser e-posten har passert underveis på internett. I Norge gjennomføres ingen systematisk lagring av trafikkdata fra e-post, ettersom dette normalt ikke er nødvendig for fakturering. En rekke andre land har derimot innført obligatorisk lagring av slike trafikkdata, og på grunn av internetts globale karakter kan e-post fra norske borgere likevel gjøres gjenstand for slik logging i den grad de passerer gjennom servere i land med loggingsplikt. For eksempel vil bruk av e-postkonto hos en amerikansk leverandør (som for eksempel MSN Hotmail eller Yahoo! Mail) medføre at e-posten omfattes av amerikanske krav til logging.

Sikkerheten til e-post som er lastet ned på brukerens PC og slettet fra serveren, er avhengig av beskyttelsen lokalt på PC-en. Med mindre ulike brukere på samme PC har adskilte og passordbeskyttede brukerkontoer, vil brukerne kunne lese hverandres e-post, og hvis brukerens PC ikke er beskyttet mot virus og hacking, kan e-post være utsatt for innsyn eller spredning selv om den kun er lagret lokalt.

Tilkobling til tjenester på web
Når en bruker besøker et nettsted på internett, innebærer det at det etableres kommunikasjon med en webserver hvor de aktuelle sidene ligger. For å finne denne trengs et domenenavn, for eksempel www.teknologiradet.no, som ved hjelp av en DNS-server (Domain Name System) oversettes til en IP-adresse, slik at det kan opprettes en forbindelse med akkurat den riktige webserveren. Brukerens nettleser (browser) vil på sin side oppgi egen IP-adresse til den server som besøkes for at denne skal kunne sende data tilbake til riktig PC.

Den besøkte webserver vil ofte lagre informasjon om brukerens besøk på de aktuelle websider. Typisk vil slik informasjon omfatte tidspunkt, brukerens IP-adresse, brukernavnet for den aktuelle internettkonto og navnet på de dokumenter (websider) som ble forespurt. Avhengig av brukerens tilknytningsform til internett vil den aktuelle tjenestetilbyder kunne anvende brukerens IP-adresse til i større eller mindre grad å identifisere brukeren.

For brukere som har fast IP-adresse, og som ikke går igjennom en brannmur, vil brukerens maskin entydig kunne bestemmes ut fra IP-adressen. Hvis det videre er knyttet et domenenavn til denne IP-adressen, vil navnet på maskinen kunne slås direkte opp på en DNS-server (domenenavntjenesten). I forhold til brukere som tildeles en dynamisk IP-adresse hver gang de logger seg på nettet, er det kun mulig for den besøkte webserver å fastslå hvilken internettleverandør brukeren benytter. Internett-leverandøren vil derimot som regel kunne identifisere en bruker på bakgrunn av et tidspunkt og en IP-adresse. Hvis leverandøren kan logge hvilket telefonnummer som er brukt til å etablere forbindelsen, vil dette kunne brukes til å avgjøre nøyaktig hvor den aktuelle PC befant seg på det gitte tidspunkt. Internett-leverandøren vil logge både hvilket brukernavn (login) som var knyttet til en oppkobling, og

hvilken IP-adresse som ble tildelt. Dette kan så brukes til å finne identiteten til innehaveren av det aktuelle internett-abonnementet.

HTTP-henvisninger
HTTP (HyperText Transfer Protocol) er den protokoll som brukes til overføring av websider mellom en server og en nettleser. Denne protokollen er slik at når man følger en lenke fra ett nettsted til et annet, vil adressen (URL – Uniform Resource Locator) til den siden som inneholder lenken bli sendt med når nettleseren ber om den nye siden. Da kan det nettstedet man til enhver tid besøker hele tiden se hvilken side man kommer fra, og slik samle informasjon om brukerens aktiviteter på nettet.

Et særlig problem i denne forbindelse er knyttet til felter for inntasting av informasjon fra brukerens side. Et eksempel er søketjenester, hvor man kan taste inn et eller flere søkeord i et felt. Av tekniske årsaker vil adressefeltet til resultatsiden fra et slikt søk som regel inneholde nettopp de ord som det ble søkt på. Når brukeren da klikker på et av treffene, vil den webserver man kommer til kunne se hvilke ord det ble søkt på, og hvis mulig knytte dette til annen informasjon om den aktuelle brukeren for å bygge en profil på vedkommende.

En mer vanlig variant av dette oppstår når søkemotoren har reklame fra ulike annonsører på de sidene som angir treff fra et søk. Slike reklamer er lastet direkte ned fra annonsørens server, og også alle annonsørene på siden vil få tilsendt informasjon om brukeren og hvilke ord hun har brukt i sitt søk. Dette kan resultere i at mange aktører kan bruke slike søk til å bygge profiler på brukeres interesser og surfevaner.

Informasjonskapsler (cookies)
En informasjonskapsel (cookie) er en liten tekstfil som en webserver kan lagre på brukerens harddisk når denne laster ned sider fra den aktuelle serveren. Formålet med en slik fil er primært å lagre opplysninger om brukerens interaksjon med serveren for å kunne gjenkjenne brukeren ved senere anledninger og effektivisere senere besøk på samme nettsted. For eksempel lagres gjerne eventuelt brukernavn og passord for tjenesten, slik at brukeren kan logges automatisk inn neste gang. De nettsidene som presenteres for brukeren, kan også tilpasses til hva vedkommende har gjort der tidligere. I nettbutikker brukes informasjonskapsler for eksempel til å bygge opp en ”handlekurv” med ting brukeren ønsker å kjøpe, og enkelte foreslår utvalgte tilbud for brukeren basert på tidligere kjøp, tidligere besøkte sider eller foretatte søk.

Informasjonskapsler kan lagres hos brukeren av to ulike typer aktører. Førsteparts informasjonskapsler opprettes av den webserver brukeren besøker, altså av det nettsted hvis adresse brukeren har skrevet i adressefeltet i sin nettleser. Tredjeparts informasjonskapsler kan derimot opprettes av en tredjepart som direkte leverer innhold til den websiden som besøkes. Typisk vil dette gjelde for annonsører på nettstedets sider. En annonse på en webside ligger normalt ikke på nettstedets egen webserver, men lastes ned fra annonsørens server. Slik får også denne anledning til å lagre en informasjonskapsel hos brukeren. Slike kapsler vil normalt brukes til å samle informasjon om brukerens websurfing på sider hvor det aktuelle selskapet har annonser og brukes i markedsføringsøyemed. Det finnes et antall nettverk av reklamebyråer som samarbeider for å utveksle informasjon om brukeres surfevaner og preferanser, for slik å kunne bygge mest mulig treffsikre personprofiler.

Det kan knyttes ulik levetid til informasjonskapsler. Noen slettes automatisk etter kort tid, mens andre aldri slettes med mindre brukeren gjør det selv. En server kan kun lese en kapsel

som den selv har lagret på brukerens PC og kan således ikke se hvilke andre informasjonskapsler som måtte finnes på brukerens PC.

Personvernmessige problemer med informasjonskapsler er knyttet til flere forhold. Det er et faktum at slike informasjonskapsler brukes til å gjøre brukeren gjenkjennelig overfor serveren, og slik muliggjør etablering av profiler med informasjon som aggregeres over tid. Vanligvis er det likevel først hvis brukeren selv oppgir personopplysninger at et nettsted kan henføre informasjonen til en faktisk person. Dette fordi et hvilket som helst nettsted normalt ikke kan knytte en IP-adresse direkte til en person. I forbindelse med netthandel er det som regel nødvendig å oppgi personopplysninger, så ved besøk på nettbutikker kan informasjonskapsler bidra til faktisk å identifisere brukeren, også de gangene han bare er innom og titter uten å kjøpe noe. Siden mange brukere har få motforestillinger mot å oppgi personopplysninger på nettet, og gjerne oppgir personalia mot å få noe gratis (tilgang til en tjeneste, være med i trekningen av noe, gratis SMS-er eller lignende), vil mange gjøre seg lett identifiserbare på nettet gjennom informasjonskapsler knyttet direkte til deres personalia.

Det er mulig for brukere å beskytte seg mot informasjonskapsler som kan være skadelige for deres personvern. En av mulighetene er å fullstendig blokkere adgangen til å lagre informasjonskapsler, men dette innebærer at mange nettsteder ikke vil kunne aksesseres. Alle moderne nettlesere (som for eksempel Internet Explorer, Opera, Firefox og Safari) kan la brukeren bestemme kriteriene for i hvilke tilfeller nettleseren skal akseptere at det lagres informasjonskapsler på harddisken. Så vil nettleseren automatisk akseptere eller avvise slike kapsler på grunnlag av disse kriteriene. Slik kan brukeren for eksempel si at informasjonskapsler fra tredjepart aldri skal aksepteres, og at kapsler fra førstepart skal aksepteres kun hvis nettstedet opererer med et betryggende personvernløfte (privacy policy).

Søkemotorer og katalogtjenester

En av de helt sentrale tjenestetyper på internett i dag, er de såkalte søkemotorene som hjelper brukerne til å finne den informasjon de søker. Søkemotorer samler løpende inn informasjon fra alle websider og nyhetsgrupper (diskusjonsfora) som er tilknyttet internett. Dokumentene indekseres i forhold til spesifikke søkeord, slik at det går svært raskt for en bruker å få svar på et søk. Det finnes mange slike søkemotorer hvorav den mest kjente i dag heter Google. Dette selskapet revolusjonerte i sin tid søking på internett, ved å ta i bruk metoder som gav bedre kvalitet på treffene gjennom å rangere dem etter kriterier for popularitet (i praksis hvor mange andre nettsider som har lenke til stedet og hvor stor trafikk det har). Selskapet gav også opphav til et nytt begrep: googling, nemlig det å lete opp informasjon om en person ved bruk av søkemotor.

Katalogtjenester er en annen type tjeneste som gjør det enklere å finne spesifikke opplysninger om en person. Typisk gjelder dette kontaktinformasjon som e-postadresse, telefonnummer og lignende. Eksempler på slike tjenester i Norge er e-postkataloger som gjerne tilbys av internettleverandører, samt Telefonkatalogen online som tilbys gjennom Gule sider på nettet og som lar brukere lete opp informasjon om abonnenters fast- og mobiltelefonnumre samt adresse. Informasjon om e-postadresse, arbeidssted og tittel kan også finnes her hvis abonnenten selv har lagt det inn. Denne tjenesten kan også brukes til å søke på telefonnummer og få svar om hvem som er eieren. Med mindre telefonabonnementet er uregistrert eller eieren har reservert seg mot oppføring i offentlige kataloger, vil det således være enkelt for en person som har fått tak i en annens telefonnummer og finne hvem denne er.

Effekten av søkemotorer og katalogtjenester er at når man først har lagt informasjon ut på nettet, vil denne relativt enkelt kunne søkes opp av andre internett-brukere. Slik innformasjon har også en tendens til å være svært varig i den forstand at den ikke forsvinner så lett. Flere har fått seg en overraskelse ved at de kan gjenfinne uttalelser de har kommet med i en diskusjonsgruppe (news-group) for lenge siden og som de ikke nødvendigvis fortsatt vil stå ved. Informasjon på hjemmesider kan også være overraskende varige, ettersom de ofte fortsatt kan gjenfinnes også etter at siden er slettet. Dette fordi søkemotorer gjerne lagrer statiske bilder av websider ved gitte tidspunkt, og kan presentere disse såkalt cachede sidene selv om originalen er slettet. Mange brukere er lite bevisst på at det er så lett å finne innformasjon om dem som er lagt ut på nettet, og er muligens derfor noe uforsiktige med hva de sender ut av informasjon som kan føres tilbake til dem som person.

6.2.3 Sporlagring lokalt

I tillegg til at elektronisk kommunikasjon etterlater seg elektroniske spor rundt om hos operatører, tjenesteleverandører og andre, lagres i mange sammenhenger slike spor også lokalt på brukerens eget terminalutstyr. Et velkjent eksempel her er de logger med utgående og inngående samtaler, SMS-er og MMS-er som lagres på en mobiltelefon. Nysgjerrige familiemedlemmer eller andre som får tilgang til en annens mobiltelefon, kan utnytte dette til å snoke i dennes private kommunikasjon, noe som mange vil oppleve som et overtramp inn i den private sfære.

Også på andre bruksområder enn mobiltelefonen lagres lokale spor av brukerens elektroniske kommunikasjon. Mange av disse er både mer nærgående og detaljerte, samtidig som færre er bevisste på slik sporlagring og på at andre faktisk kan ha mulighet til å kikke dem i kortene. Vi skal her se på to slike eksempler – PC og brannmur.

Brukerens PC
Ved kommunikasjon over internett er det ikke bare teleoperatøren, internett-leverandøren, og tjenesteleverandøren på det aktuelle nettsted som lagrer spor fra kommunikasjonen. Også det lokale utstyr som brukeren anvender lagrer slike spor. For privatbrukere gjelder dette primært selve PC-en, men i en jobbsituasjon vil det som regel også finnes en separat brannmur som foretar slik lagring.

På brukerens PC vil nettleseren (browseren) lagre en rekke spor fra bruk av internett. For det første loggføres alle besøkte nettsider og denne historikken tas vare på for en kortere eller lengre tid. Hvor lenge kan brukeren selv bestemme, men i utgangspunktet er perioden ofte satt til ca 3 uker. Historikken hjelper brukeren til å finne tidligere besøkte adresser ved at hun kan gå inn og se hvilke nettsteder hun har besøkt i løpet av de siste dager og uker. Besøkte adresser vil også poppe opp i adressefeltet når man begynner å skrive en ny adresse, for at man raskere skal komme seg til en adresse man har brukt tidligere. Det vil på grunn av denne historikken være mulig for andre brukere som får tilgang til PC-en å se hvilke adresser som har vært besøkt. I nyere versjoner av alle nettlesere er det mulig for brukeren å slette denne loggen, hvis hun ikke ønsker å dele sine surfevaner med andre som kan bruke PC-en.

For det andre vil nettleseren mellomlagre (cache) ulike filer med for eksempel tekst (HTML-filer) og bilder (JPEG- og GIF-filer) i en mappe kalt Cache, Temporary Internet Files eller lignende. Innholdet i disse filene kan ses direkte av andre brukere som får tilgang til PC-en. Disse midlertidige internett-filene slettes ikke automatisk når nettleseren lukkes, men blir gjerne liggende inntil nye filer overskriver tidligere lagrede filer. Størrelsen på mappen hvor

midlertidige filer mellomlagres avgjør hvor fort en fil blir overskrevet med en ny. Brukeren kan selv justere størrelsen på denne mappen, og når som helst slette alle filer som ligger i mappen.

Lagring av midlertidige filer på harddisken er kanskje ikke spesielt problematisk så lenge det er snakk om brukerens egen PC. Verre er det ved bruk av offentlig tilgjengelige PC-er på biblioteker, internettcaféer eller undervisningsinstitusjoner. Her er man mer sårbar for at noen kan gå inn og forsøke å snoke i informasjon fra andre brukere. Skriving av e-post i weblesere kan være spesielt problematisk i denne sammenheng, etter som innhold kan bli liggende igjen i en midlertidig fil på PC-en selv om man lukker nettleseren etter seg.

Brannmur
De fleste større arbeidsplasser og et økende antall private brukere med "alltid oppe" tilkobling til internett har installert en såkalt brannmur som fungerer som et filter mellom det interne nettverket og det eksterne internett og som beskytter mot eksterne trusler, som for eksempel innbrudd fra hackere. En arbeidstaker som bruker internett på et sted med installert brannmur foretar all surfing og alle søk gjennom denne brannmuren. En sentral funksjon ved brannmurer er at de loggfører all innkommende og utgående trafikk på nettet. Ved bruk av oppfølgingsverktøyer som følger med en brannmur, kan systemadministrator eller andre med riktige tilgangsrettigheter se nøyaktig hvilke websider den enkelte ansatte har besøkt, hvor mange ganger, til hvilke tider og så videre. Denne teknologien muliggjør altså detaljert overvåkning av de ansattes ferd på internett.

6.3 Lokasjonsteknologi og lokasjonsbaserte tjenester

Lokasjonsbaserte tjenester er tjenester som tilbys med utgangspunkt i brukerens lokasjon eller geografiske posisjon. Slike tjenester forutsetter således teknologi som med større eller mindre nøyaktighet kan beregne hvor brukeren befinner seg. Faktum er at den teknologien vi omgir oss med til daglig i stadig større grad gjør bruk av lokasjonsinformasjon for å tilby forbedret funksjonalitet for brukeren. Samtidig lagres langt flere data om hvor brukere befinner seg samt om deres bevegelser.

Lokasjonsbaserte tjenester utnytter mobil informasjons- og kommunikasjonsteknologi som brukeren bærer med seg i hverdagen. Typiske eksempler på slik teknologi i dag er mobiltelefon, bærbar PC, PDA (personlig digital assistent eller lomme-PC), eller utstyr som støtter satellittbasert navigasjon (GPS). Trådløse teknologier som formidler lokasjonsinformasjon kan bidra til å forbedre og effektivisere ulike sider av brukernes dagligliv gjennom å knytte informasjon om fysisk lokasjon sammen med de tjenester som tilbys i den virtuelle verden, for eksempel på brukerens PC eller mobiltelefon. Hver gang en bruker aksesserer en lokasjonsbasert tjeneste kan kontekstrelevant informasjon leveres til brukeren og slik være til stor hjelp.

Lokasjonsbaserte tjenester opplevde en periode av kraftig hype under dot-com perioden, spesielt gjaldt dette *m-commerce* – mobil handel. Så langt har disse tjenestene ikke vært i nærheten av å innfri alle de forventinger som ble skapt, og i dag er de gjenstand for langt mindre oppmerksomhet enn tidligere. Ettersom de underliggende teknologiene modnes, blir slike tjenester derimot sakte, men sikkert en realitet. Enkelte lokasjonsbaserte tjenester har allerede hatt sitt gjennombrudd og brukes daglig av et økende antall mennesker. Spesielt kan dette sies å gjelde tjenester for satellittbasert navigasjon. Slike var tidligere i praksis forbeholdt militære formål og spesielle sivile områder som luftfart og skipstrafikk, men

finner i dag stadig nye bruksområder for privatpersoner. Navigasjonssystemer i biler er et eksempel på dette.

Dagens og morgendagens lokasjonsbaserte tjenester gjør bruk av to typer av teknologier som produserer data om personers lokasjon. Den ene er teknologier som gir trådløs tilgang til kommunikasjonsnettverk, og som er avhengige av å detektere hvor en kommunikasjons-terminal befinner seg for å kunne etablere en forbindelse med nettverket. Lokasjonsdata oppstår i dette tilfellet som et biprodukt av at det opprettes en kommunikasjonsforbindelse, og posisjonen man får er gjerne lite nøyaktig. Dette dreier seg i hovedsak om nettverk for mobiltelefoni samt teknologier for trådløs datakommunikasjon. Den andre typen er teknologi som er utviklet spesielt for å beregne geografisk posisjon, og som ofte kan gjøre dette med høy presisjon. Da er det primært snakk om posisjonering ved hjelp av satellitter, eller ulike typer basestasjoner for mobil kommunikasjon.[37]

6.3.1 Trådløse kommunikasjonsteknologier

Mobiltelefoni
Mobiltelefoni er en trådløs kommunikasjonsteknologi som har oppnådd svært stor utbredelse, og som er av spesiell interesse nettopp fordi den har blitt allemannseie. En mobil terminal som for eksempel en GSM-telefon etablerer kommunikasjon gjennom såkalte basestasjoner. Disse er store antenner med sendere/mottakere som formidler signaler mellom telenettet og mobile terminaler (telefoner). Trafikk fra en mobiltelefon sendes med radiobølger inn til nærmeste basestasjon, derfra går signalene i de fleste tilfeller gjennom det kabelbaserte transportnettet og videre ut enten til en fastabonnent via aksessnettet (som går ut til sluttkundene) eller til en mobilabonnent, via den basestasjon som er nærmest til det stedet hvor mottakeren befinner seg. For å kunne etablere slik kommunikasjon må mobilnettverket til enhver tid holde rede på hvor hver enkelt telefon befinner seg. Når man så kommuniserer fra en mobil terminal, lagrer operatøren data om hvilken basestasjon som ble brukt som del av de trafikkdata som oppbevares om samtalen av hensyn til fakturering.

Dagens mest utbredte teknologi for mobiltelefoni er GSM-systemet (Global System for Mobile communications) som ved utgangen av januar 2004 hadde over én milliard brukere fordelt på mer enn 200 land[38]. Båndbredden for datatrafikk på GSM (2G, dvs andre generasjons mobiltelefoni) har tradisjonelt vært så lav (9,6 – 14,4 kbit/s) at bruken til dette formålet aldri har blitt noen stor suksess. Nyere såkalte 2,5G-teknologier brer nå om seg og bidrar til å forlenge levetiden til GSM. Viktigst blant disse er GPRS (General Packet Radio Service) som innebærer overgang til pakkesvitsjet overføring. Dette egner seg bedre for dataoverføring fordi forbindelsen alltid er oppe, og dessuten har høyere hastighet med en teoretisk båndbredde på inntil 115 kbit/s. En videreutviklet standard under navnet EDGE (Enhanced Data rate for GSM Evolution) ble innført i Norge i 2004 med en teoretisk båndbredde på inntil 384 kbit/s. Til sammenligning er båndbredden på en ISDN-kanal 64 kbit/s og på en normal ADSL-forbindelse i privatmarkedet rundt 700 – 1000 kbit/s.

Tredje generasjons mobiltelefoni (3G) etter standarden UMTS (Universal Mobile Tele-communications System) er allerede innført i flere europeiske markeder. Telenor har lansert

[37]Fremstillingen er i hovedsak basert på Institute for Prospective Technological Studies (2003)
[38]GSM World - http://www.gsmworld.com/news/press_2004/press04_10.shtml

sitt UMTS-nett i Norge ved slutten av 2004, mens Netcoms UMTS-nett er på lufta fra mars 2005. Denne type tredjegenerasjons mobilnett vil gi brukerne en båndbredde på minimum 144 kbit/s, mer typisk 384 kbit/s. Innen utløpet av 2005 forventes en videreutviklet UMTS-teknologi under navnet High Speed Downlink Packet Access (HSDPA) introdusert internasjonalt med båndbredde på rundt 2 Mbit/s.

Så langt dominerer tale samt meldingstjenester som SMS (tekst) og MMS (multimedia) bruken av mobiltelefoner. Kun relativt få aksesserer internett via mobilnettverk. Etter at pakkesvitsjet "alltid-oppe" kommunikasjon har blitt mer utbredt med GPRS, har bruken av forenklede internett-tjenester over WAP (Wireless Application Protocol) økt noe, men ikke dramatisk. Det forventes derimot at mobilt internett vil bli et raskt voksende tjeneste-område, ettersom båndbredden ut til telefonene øker med utbredelsen av teknologi som EDGE og UMTS. Foreløpig er det usikkert i hvilken grad bruken av disse teknologiene vil ta av, men tross tidligere overdrevne forventninger og påfølgende skuffelser, er det god grunn til å tro at bedre båndbredde kombinert med bedre skjermer på terminalene vil bidra til at flere i framtida vil benytte mobiltelefonen til å aksessere e-post og internett.

Det faktum at så mange har mobiltelefon og har den med seg omtrent hvor enn de går, gjør den til en naturlig plattform for å tilby lokasjonsbaserte tjenester. Den kraftig forbedrede båndbredden i teknologier som EDGE og 3G/UMTS muliggjør mer avanserte og medierike tjenester, og forventes blant annet å drive innføringen av nye lokasjonsbaserte tjenester.

Trådløse lokalnett

Trådløse lokalnett, kjent som *WLAN* (Wireless Local Area Network), er en teknologi hvor bredbåndskommunikasjon formidles via en ruter som er tilkoblet nettet, og som kommuniserer med datamaskiner og annet brukerutstyr ved hjelp av radiobølger. Så lenge en datamaskin har støtte for slik teknologi (nesten alle nye bærbare PC-er har det), kan den kommunisere trådløst via ruteren og ut på internett. Teknologien ble i sin tid introdusert som et alternativ til å trekke kabler til hver enkelt maskin i et kontorlokale. Introduksjonen av en ny standard for trådløse lokalnett kalt IEEE802.11 (kjent som Wi-Fi) har derimot brakt prisene på slikt utstyr så lavt at trådløse nett i løpet av de siste par årene har bredt om seg på mange fronter.

Trådløs tilgang til internett er blitt et produkt som kan tilbys av aktører som for eksempel cafeer, restauranter og bensinstasjoner, enten som en gratistjeneste for å lokke kunder eller som en tjeneste kundene må betale for. I slike sammenhenger kalles området som dekkes av senderen (typisk fra noen titalls og opp til ett hundre meter) for en "hot spot" eller en "IP-sone". Den amerikanske kaffebarkjeden Starbucks og bensinstasjonene til Statoil gjorde seg tidlig bemerket ved å tilby trådløse internett-soner til sine kunder. Flyplasser var også tidlig ute med å tilby slike "hot spots", og nå er det blitt vanlig med trådløst internett på bedre hoteller. Salget av slikt WLAN-utstyr til privatmarkedet har også tatt helt av, så stadig flere har nå et slikt nett i sitt eget hjem. Viktige grunner til dette er at et WLAN gjør det enkelt å koble flere maskiner samtidig til internett, samt at det gir mulighet for internett-tilgang i hele huset og sågar på balkongen eller i hagen.

Trådløse personnære nett

Teknologier for trådløs kommunikasjon i et lite område omkring en person finnes allerede på markedet, og forventes å bli langt mer utbredt i løpet av få år. Slik teknologi er kjent som *WPAN* (wireless personal area networking) og brukes blant annet til å få ulike typer personlig elektronisk utstyr til å kommunisere trådløst. *Bluetooth* er en slik teknologi for

trådløs kommunikasjon over korte avstander, normalt innenfor ca 10 meter, og med en båndbredde på 1 Mbit/s. Bruksområdet er stort sett å erstatte kabler med en trådløs forbindelse ved sammenkobling av elektronisk utstyr. Eksempler er tilkobling av PC eller PDA til mobiltelefon for mobil tilgang til e-post eller internett, tilkobling av periferiutstyr som tastatur og mus til PC, samt tilkobling av hodetelefoner til bærbar musikkspiller.

Ultrawideband (UWB) er en teknologi under utvikling og standardisering som forventes innført i 2005, og som mange mener etterhvert vil erstatte Bluetooth. Denne teknologien opererer over tilsvarende korte rekkevidde som Bluetooth (innenfor ca 10 meter), men med mye høyere båndbredde – inntil 480 Mbit/s[39] Denne teknologien vil således kunne brukes til overføring av store datamengder for eksempel knyttet til underholdningsutstyr i hjemmet, slik som for eksempel høyoppløselige TV-signaler (High Definition TV – HDTV). UWB har også svært lavt strømforbruk og egner seg således til bruk i små enheter med begrenset batterikapasitet. Følgelig kan denne kommunikasjonsteknologien forventes å spille en betydelig rolle i et fremtidsscenario hvor stadig flere av de ting vi omgir oss med til daglig kommuniserer med hverandre, og hvor mennesker i økende grad bærer IKT-utstyr på kroppen (*wearable computing*).

6.3.2 Lokasjonsteknologi

Vi har så langt vært innom teknologier som er utviklet for å muliggjøre mobil kommunikasjon, og som i tillegg kan gi omtrentlig informasjon om hvor brukeren befinner seg. I tillegg til dette er det utviklet teknologi spesifikt for å kunne beregne mer nøyaktige posisjoner. Disse er basert på at man beregner posisjonen til brukerens mobile kommunikasjonsutstyr, heller enn bare å formidle hvilken basestasjon som etablerte en forbindelse med brukeren. Da er det snakk om teknologier som bruker flere faste eller kjente punkter for å beregne hvor brukeren befinner seg. Slike teknologier kan være bakkebaserte, satellittbaserte eller en kombinasjon av disse to.

Basestasjoner på bakken
Bakkebaserte metoder gjør bruk av basestasjoner for mobil kommunikasjon, normalt knyttet til mobiltelefoni. Som tidligere nevnt vil mobiloperatører i dag normalt kun lagre informasjon om benyttet basestasjon i sine trafikkdata fra mobilkommunikasjon. Dette gir en svært omtrentlig posisjon med nøyaktighet på fra noen hundre meter i tettbygde områder, opp til flere kilometer i spredt bebodde områder. Første trinn ved økning av nøyaktigheten i en posisjon er å bruke signalforsinkelsen mellom basestasjon og brukerens terminal til å anslå omtrent hvor langt fra basestasjonen brukeren befinner seg. Denne metoden er brukbar kun hvis avstanden til basestasjonen er mer enn 500 meter, og den sier ingenting om i hvilken retning fra basestasjonen brukeren befinner seg.

For mer nøyaktig posisjon er det mulig å bruke metoder som *Enhanced observed time difference* (for GSM) eller *Observed time difference of arrival* (for UMTS). Disse utnytter det faktum at brukere som regel befinner seg innenfor dekningsområdet til flere basestasjoner samtidig. Da kan relative forskjeller i signalenes tidsforsinkelse inn til de ulike basestasjonene brukes til å beregne en posisjon med høyere presisjon, typisk ca 100-300 meters nøyaktighet.

---

[39]CNet News.com, 16.04.2004: Ultrawideband groups band together http://news.com.com/2100-7351-5193541.html?tag=nefd.hed

Samme prinsipp kan brukes også på andre typer basestasjoner, som for eksempel WLAN, Bluetooth og UWB. Siden dette er teknologier med mer begrenset rekkevidde enn mobilmaster, vil disse komme til anvendelse i mer avgrensede settinger, for eksempel innendørs. Ettersom basestasjoner for disses tilfelle vil stå mye tettere, vil nøyaktigheten i posisjonen kunne bli svært høy.

Satellittnettverk

Mens bakkebasert posisjonering kan gi god presisjon innendørs og innenfor et begrenset område, har de generelt for lav presisjon for mange andre bruksområder. Satellittbasert posisjonering er i de fleste tilfeller det beste hvis man trenger høy presisjon i angivelsen av posisjoner over et større område. De fleste typer navigasjonssystemer og personlig posisjoneringsutstyr gjør bruk av satellittberegnede posisjoner. Et sett av satellitter går i bestemte baner rundt jordkloden og kan sammen beregne nøyaktige geografiske posisjoner på jorda og formidle disse videre til elektronisk utstyr på bakken.

Denne type systemer er kjent som *GPS* (Global Positioning System). Det finnes i dag to slike nettverk: amerikanske NAVSTAR (Navigation Signal Timing and Ranging) som styres av det amerikanske forsvarsdepartementet, og det russiske GLONASS-systemet (Global Navigation Satellitte System). Det amerikanske systemet er det som i dagligtalen refereres til som GPS.

Et nytt europeisk satellittnettverk for posisjonering er under utvikling under navnet Galileo. Systemet vil fungere etter de samme prinsipper som GPS, og er ment å gjøre Europa mindre avhengig av systemer hvor henholdsvis USA og Russland kan begrense nøyaktigheten i posisjoneringen til utenlandske og sivile brukere hvis de finner det nødvendig av militære grunner. Dette svært kostbare prosjektet understreker hvor viktig pålitelig og eksakt posisjonsinformasjon har blitt i moderne samfunn. Galileo utvikles primært for sivile formål og planlegges å være operativt i 2008.

Etter mange år med begrenset suksess i massemarkedet, er bruken av satellittbasert posisjonering i ferd med å ta av[40]. Det er flere grunner til dette, men en viktig grunn er at GPS-brikker er blitt mye mindre av størrelse, og langt billigere i innkjøp. Dette gjør GPS-brikkene aktuelle på stadig nye bruksområder. En annen grunn er at amerikanske teleoperatører er blitt pålagt av myndighetene å sikre at 95% av deres mobiltelefonbrukere skal kunne posisjoneres, slik at nødetater kan finne brukere som ringer nødnummeret 911. Flere av de største mobiloperatørene i USA satser på GPS-brikker i telefonene for å kunne møte dette kravet. Også i Europa og Asia tilbyr stadig flere mobilnettoperatører muligheten til å spore telefoner og andre enheter med GPS-brikke. I Japan og Korea tilbys allerede et sett av mobiltjenester basert på GPS-beregnet posisjon, og i Japan er det et krav at alle mobiltelefoner skal ha GSM innen 2007..

Satellittbaserte systemer har høy presisjon, og gir posisjoner med en nøyaktighet ned til få meter. En begrensning knyttet til satellittbaserte metoder er at de krever tilnærmet fri sikt opp mot himmelen, og således ikke fungerer innendørs. Ved å kombinere satellittbasert og landbasert posisjonering, kan man få både høy presisjon og innendørs dekning.

---

[40]CNet News.com, 09.04.2004: *After years of struggle, GPS is taking off* http://news.com.com/2102-1033_3-5187758.html?tag=st.util.print

6.3.3 Anvendelser

Lokaliseringsteknologi og lokasjonsbaserte tjenester er et område som allerede bringer stor nytte til mange brukere, men som like fullt befinner seg i en tidlig fase. I årene som kommer vil slike tjenester innføres på en bredere skala enn hva vi har sett så langt. Innføringen av slike tjenester har gått tregere enn hva mange trodde for noen år siden. De kommer derimot sakte, men sikkert. Mer av den teknologien vi omgir oss med vil kunne posisjonere oss geografisk, og tilbudet av tjenester som bruker lokasjonsinformasjon vil bli utvidet til stadig nye områder. Samtidig som dette representerer både gode forretningsmuligheter for tilbydere og stor nytte for brukerne, er det personvernmessige utfordringer knyttet til slike tjenester. Kjernen i dette er i hvilken grad brukeren kan ha kontroll med hvem som kan få tilgang til informasjon om hvor hun er eller har vært.

Data om hvor mennesker eller ting befinner seg kan brukes innenfor en lang rekke områder, for eksempel å gi økt trygghet, lette hverdagslige oppgaver eller effektivisere enkelte arbeidsoppgaver. Vi skal her kort nevne noen eksempler på tjenesteområder hvor lokaliseringsteknologi har kommet eller kan forventes å komme til anvendelse.

Nødassistanse
Den amerikanske bilprodusenten General Motors har så langt levert 2,5 mill biler med systemet OnStar. Hvis førerens airbag i en slik bil skulle utløses, vil bilen automatisk ringe opp et eget assistansesenter og opplyse om dette samt oppgi nøyaktig GPS-posisjon. En operatør på dette senteret vil da ringe opp sjåføren for å høre om assistanse er nødvendig. Hvis sjåføren ikke svarer, vil operatøren alarmere nødtjenestene og oppgi bilens posisjon. Systemet kan også brukes til å spore opp bilen om den skulle bli stjålet.

Et annet eksempel er situasjoner hvor brukeren selv ringer et nødnummer for å få assistanse. Blant annet som følge av at man i USA har pålagt operatørene raskt å kunne lokalisere hvor et nødanrop kommer fra, vil det etter hvert bli vanlig med GPS-brikke i mobiltelefoner. Da kan brukeren enkelt selv sende sin posisjon til den aktuelle nødtjenesten, så denne kan se hvor vedkommende befinner seg. Selv uten GPS-brikke kan basestasjoner brukes for å beregne en telefons omtrentlige posisjon, slik at det er lettere å finne den som trenger assistanse.

Voldsalarmer er enda et eksempel på en innretning som er laget for at brukeren på en rask og enkel måte kan gi beskjed om at hun trenger hjelp og samtidig sende data om hennes posisjon, slik at nødvendig assistanse kan komme hurtig til riktig sted. I Norge er det nylig blitt etablert en kommersiell tjeneste for dette, Trygghetsmobilen, som baserer seg på bruk av eierens mobiltelefon.

Trafikktjenester
Trafikken er et område hvor lokasjonsinformasjon kan være svært nyttig. Et område hvor lokasjonstjenester allerede er ganske utbredt i Europa, er navigasjonssystemer i biler. Slike systemer kombinerer nøyaktig GPS-posisjonering med kartinformasjon for å tilby kjøreanvisninger på veien fra A til B. Informasjon om trafikale forhold som køer, omkjøringer og føreforhold kan integreres i slike systemer, slik at sjåføren ledes til å kjøre den mest effektive ruten. Dessuten kan man etter hvert integrere informasjon som for eksempel hvor nærmeste parkeringshus med ledig plass befinner seg, hvor nærmeste bensinstasjon er eller hvor nærmeste verksted er å finne.

Også når det gjelder trafikksikkerhet vil lokasjonsinformasjon etter hvert komme til anvendelse. Med GPS-navigasjon i bilen kan man for eksempel gi føreren skiltinformasjon på dashbordet. Det forutsetter bare at noen utvikler og vedlikeholder et kart med slik informasjon. Aktuell fartsgrense vil da alltid være lett tilgjengelig for sjåføren, samtidig som spesielle fareskilt (som for eksempel vikeplikt eller stopp-skilt) kan lyse opp ved siden av speedometeret. Slik fartsgrenseinformasjon kan også kobles sammen med systemer for såkalt aktiv gasspedal, hvor bilens gasspedal yter ekstra motstand hvis fartsgrensen brytes.

Informasjonstjenester
Etter hvert som mobiltelefoner får GPS-brikke, raskere dataoverføring og bedre skjermer, forventes lokasjonsbaserte informasjonstjenester å kunne ta av også blant vanlige brukere. Slike tjenester tar utgangspunkt i brukerens posisjon og kan på forespørsel fortelle hvor man kan finne ulike tjenester, for eksempel nærmeste apotek, minibank, vinmonopol, Hennes & Mauritz eller greske restaurant. Siden mobiltelefonen er med de fleste brukerne rundt i hverdagen, vil de fleste som regel ha en terminal på seg som de kan bruke til lokasjons-baserte forespørsler. Også personlig navigering gjennom plotting av egen posisjon på et kart på telefonens skjerm vil etter hvert kunne gå fra å være kuriositet til å bli allemannseie.

Det er også mulig å tenke seg reklametjenester basert på lokasjon, hvor brukere, fortrinnsvis etter samtykke, kan motta eventuelle tilbud på SMS eller MMS fra butikker eller restauranter de går forbi.

Lokasjonsovervåkning og styring
I arbeidslivet er lokasjonsbaserte overvåknings- og styringssystemer allerede innført på mange områder. Mest utbredt i så henseende er nok flåtestyring av slikt som lastebiler og budtjenester. Her er det betydelig effektivisering å hente på at man kan sitte med en sentral oversikt over hvor ulike ressurser befinner seg, og styre tilgjengelige ressurser dit nye behov oppstår. Også i andre sammenhenger er posisjoneringsteknologi i bruk for å holde rede på hvor folk befinner seg. Helsearbeidere på sykehus og i hjemmehjelpstjenesten kan lettere spores opp ved behov hvis de bærer med seg en gjenstand som kan posisjonsbestemmes. Armbånd med GPS-posisjonering og GSM-brikke kan respondere på forespørsler med å sende en SMS med posisjonsinformasjon. Slik kan eksempelvis små barn eller institusjons-klienter (som for eksempel demente) overvåkes av hensyn til deres egen sikkerhet.

Eksempel: Bliv-Tryg-væk i Legoland
Et eksempel kan illustrere hvordan slik bakkebasert posisjonering kan brukes til å realisere en lokasjonsbasert tjeneste. Legoland har i sin park i danske Billund installert et pilotsystem som under navnet *Bliv-Tryg-væk* integrerer aktive RFID-brikker og WLAN-mottakere med mobilnettet for å kunne identifisere og posisjonere barn, og sende posisjonsdata på SMS til foreldrenes mobiltelefon[41]. Poenget er at man raskt skal kunne gjenfinne barn som kommer bort fra sine foreldre. For et pristillegg på DKK 30 kan man i denne parken leie et armbånd med en aktiv RFID-brikke til å sette på barnet. Denne brikken sender ut et signal som identifiserer barnet, mens et nettverk av 37 spesielle WLAN-mottakere fanger opp signalene og beregner barnets posisjon. Hvis barnet skulle komme bort, kan foreldrene sende en SMS for å aktivere posisjoneringen, og så kontinuerlig få tilsendt SMS-er som forteller hvor barnet befinner seg. Et eget kart over parken med et finmasket rutenett følger med

[41]TechWeb SecurityPipeline 28.04.2004: *Legoland uses Wireless and RFID for child security* http://www.securitypipeline.com/showArticle.jhtml?articleID=19202139

tjenesten slik at systemet lett kan fortelle i hvilken kartrute barnet er. Systemet varsler automatisk både foreldrene og alle vaktene hvis et barn skulle være på vei ut av parken.

Nøyaktigheten i posisjonen er her tilstrekkelig til at parken også kan utvide tjenesten til helt andre områder. For eksempel kan familien få en SMS idet de går forbi fornøyelsesparkens restaurant, med informasjon om dagens rett eller evt. ventetid for bord.

6.3.4 Utfordringer for personvernet

Vi har sett på noen eksempler som illustrerer den store nytteverdien lokasjonsbaserte tjenester kan ha. Når man så retter søkelyset mot konsekvenser for personvernet er det lett å tenke at ettersom disse tjenestene bringer så store fordeler, må eventuelle ulemper for personvernet kunne tåles. Faktum er at dette området er svært viktig for å sikre fremtidens personvern, ettersom denne type teknologi og tjenester har et særlig stort overvåknings-potensial. Dessuten er det ikke slik at et godt personvern vil blokkere for lokasjonsbaserte tjenester. Men ettersom det her står om vernet av informasjon om hvor man er og hvor man har vært, er det rimelig å forvente strenge regler for beskyttelse av slike lokasjonsdata. For de fleste av oss er det svært viktig for opplevelsen av bevegelsesfrihet selv å kunne bestemme over hvem som skal få kjennskap til denne type informasjon. Og for enkelte, nemlig mennesker som er utsatt for en forfølger (”stalker”), kan det sågar være livsviktig at slik informasjon er godt beskyttet.

Lokasjonsdata
Som tidligere nevnt i delkapittelet om kommunikasjonsdata (6.2.1), lagres de data som er nødvendige for et elektronisk kommunikasjonsforløp av operatøren. Slike data kalles trafikkdata og omfatter informasjon om hvilke kommunikasjonsterminaler (f.eks. telefoner) som har kommunisert, og når de gjorde dette. Ved mobiltelefoni vil også informasjon om de involverte basestasjoner være en del av trafikkdata. Således vil det til all kommunikasjon over mobiltelefon være knyttet informasjon om brukerens lokasjon ved kommunikasjons-tidspunktet. Slike data oppbevares inntil fakturering er foretatt og må etter dagens regler deretter slettes.

Lokasjonsdata som ikke faller inn under begrepet trafikkdata er ikke underlagt den samme eksplisitte sletteplikten. Det betyr at lokasjonsdata som er generert utelukkende for å bestemme brukerens lokasjon, og ikke for å etablere en kommunikasjonsforbindelse, ikke nødvendigvis må slettes etter en bestemt tid. Leverandører av lokasjonsbaserte tjenester vil således kunne oppbevare data om hvor brukernes bevegelser over lengre tid enn de 3-5 måneders slettefrist som gjelder for trafikkdata. Dette faktum gjør at konsekvensene for personvernet står i fare for å bli uforholdsmessig store for brukere av lokasjonsbaserte tjenester.

Man kan tenke seg at bevegelsene til brukere av lokasjonsbaserte tjenester kan spores i detalj, og brukes til å lage svært nærgående personprofiler. Ved å koble sammen ulike typer av elektroniske spor man setter, kan man oppnå mer innholdsrike og avslørende data. Hvis lokasjonsdata eller andre kontekstdata kan kobles til spor fra elektronisk kommunikasjon, vil overvåkningspotensialet være ekstra stort. Derfor er det viktig at også vernet mot utilbørlig bruk av lokasjonsdata er sterkt.

Selvbestemmelse over lokasjonsdata
Vi har tidligere nevnt hvordan mennesker endrer sin atferd hvis de tror at noen følger med på hva de gjør. Hvis folk oppfatter at deres bevegelser kan spores er det altså en fare for at mange vil oppleve dette som en innskrenkning av deres autonomi og bevegelsesfrihet. For å hindre dette er det viktig at brukere selv har en viss kontroll med innsamlingen og spredningen av egne lokasjonsdata. Ulike lokasjonsteknologier tilfredsstiller kravet til brukerkontroll i ulikt omfang.

Lokasjonsdata som genereres av teleoperatører ved hjelp av basestasjoner eller annet utstyr i telenettet, er kontrollert av operatøren. Brukeren kan ikke påvirke lagringen av slike data, og er henvist til å stole på at lover og regler krever sletting etter en viss tid eller sikker oppbevaring. Satellittbasert posisjonering foregår derimot som regel lokalt på brukerens egen terminal (telefon, GPS-mottaker), hvor brukeren selv kan kontrollere om posisjonsdata skal tilflyte andre. Slik sett kan det være enklere for bevisste brukere å sikre eget personvern ved bruk av GPS enn ved bruk av andre lokasjonsteknologier. Problemet er som vi tidligere har påpekt, at brukerne gjerne er lite bevisste på personvern og kan være tilbøyelige til å samtykke i utstrakt lagring og utnyttelse av lokasjonsdata mot å få et eller annet gode (som for eksempel et antall gratis SMS).

Lokasjonsdata og sikkerhet
Det er også viktige sikkerhetsaspekter knyttet til lokasjonsdata. Lokasjonsinformasjon må absolutt holdes beskyttet fra personer som kan ønske å utnytte informasjonen til kriminelle handlinger. For eksempel kan innbruddstyver finne ut at et potensielt offer er borte fra huset sitt, og en forfølger (stalker) eller voldelig forsmådd eks-partner kan finne ut hvor offeret befinner seg, og bruke denne informasjonen til å finne og angripe vedkommende.

Et konkret dilemma i forhold til avveining av personvernhensyn mot hensyn til sikkerhet gjelder lokasjonsdata om svake parter som for eksempel barn, gamle og syke. Teknologien muliggjør nå på en enkel måte for brukeren å overvåke disses bevegelser, for eksempel gjennom å utstyre dem med et armbånd med GPS-mottaker og GSM-sender. Slikt kan gi betydelig økt trygghet både for den berørte og for familien, men kan også innebære en reell frihetsberøvelse for den som overvåkes. Hvilken rett skal barn eller demente ha til et privatliv? Her er det noen interessante og delikate avveininger å foreta.

Og hvilken rett skal vanlige mennesker ha til personvern på jobben? Skal arbeidsgiver kunne følge de ansattes bevegelser i detalj for å kontrollere at de bruker tiden sin effektivt? Slike spørsmål blir aktualisert når lokasjonsteknologi blir integrert i utstyr vi bærer med oss i hverdagen, slik som mobiltelefonen. Ansatte i enkelte yrkesgrupper er allerede i en situasjon hvor de kan spores av arbeidsgiver av hensyn til effektiv ressursutnyttelse, for eksempel innenfor varetransport. Men hvilke muligheter bør arbeidsgivere ha til å spore de ansattes bevegelser av andre grunner, som for eksempel for å kontrollere at man er der man skal være for å gjøre jobben sin? De økte mulighetene til lokasjonsovervåkning aktualiserer denne type spørsmål.

Problemstillingene omkring dette begrenser seg ikke bare til lovregulering av rettigheter. Minst like viktig er det om det er sosialt akseptert å si nei til å la sjef eller ektefelle følge ens bevegelser i løpet av dagen. For hvorfor skulle man være i mot noe slikt dersom man ikke har noe å skjule? Med flere og bedre tjenester for sporing og lokalisering, er det en reell fare for at ærlige personer som ønsker å ivareta sitt personvern vil bli mistenkeliggjort.

6.4 Biometrisk identifikasjon

Biometri er et teknologiområde knyttet til identifikasjon av individer ved avlesning av kroppens unike biologiske kjennetegn. Mens andre typer av identifisering krever at brukeren enten har noe (som ID-bevis eller smartkort) eller vet noe (som PIN-kode eller passord), er biometrisk informasjon altså direkte knyttet til brukerens kropp. Typiske eksempler på biometriske teknologier er gjenkjenning av fingeravtrykk, avbildning av øyets regnbuehinne (iris) eller netthinne (retina), håndgeometri, ansikts- og stemmegjenkjenning.

Siden biometri er så nært knyttet til en person antas slik identifikasjon å være mer troverdig og bedre sikret mot glemsel, tap, tyveri, forfalskning og gjetning enn bruk av kort og koder. Biometri kan brukes til to ulike formål:

- *Verifikasjon av identitet (autentisering)*
  Biometri brukes primært til autentisering, det vil si for å slå fast at en person er den hun hevder å være. Dette kalles ofte *én-til-én* matching, da man skal sammenligne den målingen brukeren avgir kun med den lagrede målingen til den hun hevder å være.
- *Identifikasjon*
  Biometri kan også brukes til identifikasjon, det vil si å prøve å finne ut hvem en ukjent person er. Dette er kjent som *én-til-mange* matching, da målingen av personens biometriske egenskap må sammenlignes med tilsvarende fra alle personer som er registrert i en database. Hvis vedkommende finnes i basen vil man kunne få en match som avslører hvem den ukjente er.

De fleste biometriske systemer baserer seg på en innrulleringsprosess hvor man registrerer en prøve av det aktuelle biometriske kjennetegn, trekker ut et sett av nøkkeldata fra prøven og koder disse til en biometrisk mal. Denne malen lagres så i en database som senere prøver sammenlignes mot.

Verken identifikasjons- eller verifikasjonssystemer produserer perfekte matcher. For hver avgitte prøve genereres en score for hvor nært denne stemmer overens med den lagrede malen. Det vil alltid være en viss sjanse for at en person feilaktig får match fordi prøven ligner på en annens, eller at en rettmessig bruker feilaktig blir avvist fordi prøven avviker for mye fra malen. Ved å justere grensen for hvor nært en prøve må stemme for å aksepteres som en match, kan man bestemme graden av feilaktige matcher (false acceptance rate) i forhold til graden av feilaktige ikke-matcher (false rejection rate). Ved å senke den ene feilraten, vil den andre uvegerlig øke. Hvis man vil sikre seg svært godt mot at uvedkommende gis adgang til et sted, må man altså finne seg i en høyere andel av tilfeller hvor rettmessige brukere blir nektet adgang og må prøve på nytt.[42]

Typiske bruksområder for biometri er adgangskontroll til områder, personidentifikasjon, sikring av tilgang til utstyr (som for eksempel en PC) samt tilgang til elektroniske tjenester på nettet (for eksempel banktjenester). Biometri er for tiden spesielt aktuelt fordi slike data planlegges innført i pass og immigrasjonsdokumenter både i USA og Europa. Slik ser man for seg å få bedre kontroll med flyten av mennesker over landegrensene og gjøre det vanskeligere å reise under falsk identitet. Dette anses nå å være et element i bekjempelsen av alvorlig kriminalitet.

---

[42]Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag - TAB (2002)

Siden biometri er knyttet til kjennetegn ved kroppen, er det ikke bare en spesielt sikker metode – den er også svært brukervennlige for den enkelte. Man kan lage systemer som gjør det unødig å huske brukernavn, passord eller koder, men bare forutsetter at brukeren plasserer fingeren sin på en leser. Slik kan biometri anvendes også på områder hvor høy sikkerhet ikke er så viktig, men hvor enkel og brukervennlig tilgang er det sentrale.

6.4.1 Biometriske teknologiers funksjonalitet

Ulike biometriske teknologier har ulike egenskaper og befinner seg på ulike modenhetsnivåer. En rekke biometriske teknologityper har stort potensial uten at det foreløpig finnes tilgjengelig konkrete løsninger som kan oppfylle dette potensialet. Ved implementering av et biometrisk system må det således vurderes om det faktisk vil fungere etter hensikten, og om det er avansert nok til å gi den lovede effektivitet. Forhold som hvor nøyaktig teknologien er, hvor sårbar den er for å bli lurt og i hvilken grad brukere vil akseptere den, må også vurderes. Vi gir her en kort beskrivelse av enkelte av de mest utbredte biometriske teknologiene.

Iris-gjenkjenning
Iris-gjenkjenning er basert på avlesning av en persons regnbuehinne (iris), altså den fargede delen av øyet som omgir pupillen. Det er vanlig å avlese 173 distinkte elementer av denne for å lage den biometriske malen. Iris-gjenkjenning er enkelt og effektivt i bruk, gir få falske matcher og regnes ikke som særlig invaderende. Bruk av fargede eller bifokale kontaktlinser samt sterke briller kan være problematisk for slike systemer, og personer med enkelte øyesykdommer kan oppleve å ikke bli gjenkjent ved bruk av slik teknologi.

Håndgeometri
Gjenkjenning av håndgeometri er basert på målinger av fingrenes lengde, bredde og høyde, avstander mellom ledd og formen på knokene. 96 ulike målinger brukes normalt for å lage en biometrisk mal av en hånd. Dette er en moden teknologi med lav andel falske matcher og lav andel av feilaktig avvisning. Denne teknologien er også vanskelig å lure, siden en prøve ikke etterlater seg spor som kan misbrukes til forfalskning (slik fingeravtrykk gjør). Siden ikke alle hender er individuelt distinkte, kan denne teknologien brukes kun til autentisering og ikke til identifikasjon gjennom én-til-mange matching.

Fingeravtrykk
Gjenkjenning av fingeravtrykk er den mest utbredte og kjente biometriske teknologien. Den baserer seg på innscanning av fingeravtrykkets avbildning og uttrekk av et sett av distinkte elementer fra dette som konverteres til en biometrisk mal. Teknologien er moden og brukes i en rekke sammenhenger. Enkelte føler likevel ubehag ved å avgi fingeravtrykk fordi det gjerne forbindes med etterforskning av kriminalitet. Siden mennesker etterlater seg fingeravtrykk overalt, er det dessuten en bekymring at fingeravtrykk som samles inn til ett formål, kan bli brukt til å spore brukerens aktiviteter også andre steder.

Ansiktsgjenkjenning
Teknologi for ansiktsgjenkjenning kan identifisere mennesker ved å analysere utvalgte elementer av ansiktet. Denne teknologien kan brukes både til autentisering og til identifikasjon av ukjente personer. Dette er foreløpig den eneste biometriske teknologien som kan brukes til skjult identifikasjon og overvåkning gjennom videoopptak foretatt på avstand. Slik teknologi er på det nåværende tidspunkt ikke særlig pålitelig, men preget av svært høye feilrater. Den er således foreløpig brukbar bare i kontrollerte omgivelser og under spesielle forutsetninger.

Stemmegjenkjenning
Gjenkjenning av stemmen kan identifisere mennesker ut fra ulikheter i stemmens lydbilde som stammer fra fysiologiske forskjeller og innlærte talevaner. Ved innrullering registreres som regel en spesiell passordsetning som analyseres for distinkte taletrekk. Disse trekkes så ut og lagres i en biometrisk mal. Stemmegjenkjenning er kostnadseffektiv og lite invaderende teknologi, men den kan ha begrenset pålitelighet og fungerer dårlig i støyende omgivelser.

6.4.2 Personvernprinsipper for biometriske teknologier

En rekke personvernrelaterte utfordringer er forbundet med bruken av biometriske løsninger, og det kreves derfor spesiell forsiktighet ved utrulling av slik teknologi. Biometri er ikke i seg selv personvernfiendtlig om det implementeres på riktig måte, men det er mange hensyn som må tas i utformingen av biometriske systemer for å sikre personvernet.

En utfordring knyttet til enkelte former for biometri er at de kan gi sensitiv overskudds-informasjon som for eksempel informasjon om etnisk tilhørighet. Genetiske data vil etter hvert også komme i bruk i biometriske systemer. Systemer basert på DNA-gjenkjenning vil produsere særlig store mengder overskuddsinformasjon i form av data som kan si noe om brukerens genetiske status og sykdomsdisposisjoner. Dette vil stille spesielle krav til informasjonssikkerhet, pseudonymisering av data samt til forsiktighet med i hvilke tilfeller slike systemer tillates brukt. I tillegg til systemer for DNA-matching, foregår nå utvikling av biometriske teknologier for gjenkjenning av blant annet blodåremønstre, hudmønstre, negl-fester, ganglag og øreform. Hver av disse vil kunne gi ulike typer av overskuddsinformasjon.

Amerikanske Center for Democracy and Technology gir en rekke råd[43] til førende prinsipper for vurderinger av biometriske løsninger og avveininger som ivaretar både personvern og sikkerhet. Følgende er de viktigste:

- *Åpen innrullering*
  Innrullering i et biometrisk system vil si å foreta en registrering av det unike kroppslige kjennetegn, for eksempel fingeravtrykk, som senere registreringer vil sammenlignes mot. Slik innrullering bør ikke skje skjult og uten den enkeltes kjennskap, men åpent slik at den berørte vet at det skjer.
- *Verifikasjon fremfor identifikasjon*
  Generelt sett fungerer biometriske teknologier langt bedre til verifikasjon ved en-til-en matching enn til bruk for å identifisere ukjente individer. Biometriske prøver bør under normale omstendigheter ikke samles inn uten at brukeren er klar over det eller uten at innsamlingen er motivert av at brukeren søker aksess til spesielt beskyttede ressurser.
- *Lokal fremfor sentral lagring av biometriske data*
  Biometriske systemer bør så langt som mulig designes slik at biometriske maler er lagret lokalt (for eksempel på et smartkort), og ikke i sentraliserte databaser. Slike baser er mer utsatt for sikkerhetsbrudd, og gjør det også enklere å bruke innsamlede prøver til sekundære formål. Et viktig poeng i forhold til dette er alvorlighetsgraden dersom en biometrisk mal blir kompromittert: Dersom noen får tak i passordet ditt,

[43] CDT, 2004: *Biometric Technologies: Security, Legal and Policy Implications*
http://www.cdt.org/security/20040621biometric.pdf

kan du begrense skaden ved å bytte det ut. Dine biometriske kjennetegn er imidlertid permanente, og dersom et eller flere er kompromittert, betyr det at du ikke lenger kan bruke disse.

- *Verifisert pseudonymitet bør brukes hvis mulig*
  Ved innføring av biometriske systemer bør det vurderes om full identifikasjon er nødvendig eller om man kan bruke en form for verifisert pseudonymitet. Da kan tilgang til en ressurs autoriseres uten at brukerens identitet blir avslørt. Samtidig kan brukerens identitet etter spesiell tillatelse likevel avdekkes hvis det oppstår et spesielt behov for å holde vedkommende ansvarlig.
- *Tilsyn og kontroll for å hindre misbruk*
  Ethvert biometrisk system må underlegges betryggende kontroll og tilsyn slik at misbruk kan forhindres.

6.5 Radiobølgebasert identifikasjon (RFID)

RFID (Radio Frequency Identification) er et konsept for automatisert identifikasjon av objekter ved bruk av radiobølger. Små brikker, vanligvis påført klistrelapper eller direkte integrert i produkter, lagrer et identifikasjonsnummer eller et sett av data om det de er festet til. RFID-lesere i form av sendere/mottakere med antenne brukes til å avlese identifikasjonsnumrene til alle RFID-brikker som befinner seg innenfor en begrenset avstand.

Bomveisystemet Autopass er et eksempel på en velprøvd form for RFID-system. Her gjenkjennes biler automatisk ved at utstyr i bomstasjonen ved bruk av radiobølger avleser identifikasjonsdata på Autopass-brikken i passerende biler, slik at riktig abonnent blir belastet. Nyere varianter av RFID forventes blant annet å overta for strekkoder. Mens varer merket med strekkode automatisk kan gjenkjennes ved å peke en laserbasert leser mot strekkoden, kan varer med RFID-brikke gjenkjennes bare de er i nærheten av en RFID-leser.

Disse eksemplene er ment å illustrere hva dette dreier seg om, men viser bare en begrenset del av teknologiens muligheter. Allerede i dag brukes RFID innenfor en rekke ulike områder, og i årene som kommer kan man forvente stadig nye anvendelser av slik automatisert identifikasjon og sporing. I den grad slike identifikasjonsbrikker også kan knyttes til mennesker, kan utfordringene for personvernet bli betydelige.

Typer av RFID-brikker

RFID-brikker finnes i henholdsvis aktiv og passiv utgave.[44] Aktive brikker har eget batteri og kan derfor inkludere større lagringsplass, mer funksjonalitet samt virke over lengre avstander (over 100 meter) enn passive brikker. På den annen side er aktive brikker relativt dyre og betydelig større enn passive brikker. De minste aktive brikkene er i dag av en størrelsesorden tilsvarende en mynt.

Passive brikker har altså ikke eget batteri, men induserer energi fra radiosignalene som kommer inn fra en RFID-leser og reagerer med å sende ut en liten mengde data, som regel kun brikkens unike identifikasjonsnummer. Signalene fra slike brikker har normalt en rekkevidde i området fra 10 mm til ca 5 meter. Et oppslag i en database på det aktuelle ID-nummeret vil så kunne fortelle mer om det som brikken er festet til. Slike passive brikker er

[44]Parliamentary Office of Science and Technology (POST), 2004: *Radio Frequency Identification (RFID)* http://www.parliament.uk/documents/upload/POSTpn225.pdf

relativt billige og svært små av størrelse, så de fleste anvendelser av RFID er basert på passive brikker. Slike brikker kan nå fås helt ned i en størrelse på under 0,2 mm^2 med en tykkelse mindre enn et papirark.[45]

Slike brikker kan dessuten være read-only, slik at data på brikken legges inn bare én gang og senere kun kan avleses, eller de kan tillate skriving av data. Slik oppdatering av informasjonen på brikken er nyttig på områder hvor en brikke brukes til å følge et produkt gjennom dets livssyklus, slik det gjøres for eksempel med kyr og storfekjøtt.

Bruksområder i dag
RFID brukes i dag på en rekke områder hvor det er viktig å kunne spore og identifisere ulike typer objekter. La oss kort nevne noen eksempler:

- Biler med startsperre lar seg ikke starte uten at en nøkkel med riktig RFID-brikke settes i tenningslåsen.
- Kjæledyr kan merkes med RFID-brikke for identifikasjon slik at de kan returneres til eieren hvis de kommer bort.
- RFID brukes på biblioteker for å merke bøker og automatisere prosessen rundt utleie og tilbakelevering. Deichmanske bibliotek i Oslo har allerede tatt et slikt system i bruk.
- Kort med RFID-brikker kan brukes grad som elektroniske penger, for eksempel i form av forhåndsbetalte reisekort til offentlig transport.
- Kortsystemer for kontroll med aksess til bygninger er i økende grad basert på RFID-teknologi snarere enn magnetstripe.
- Papir kan nå merkes ved hjelp av svært tynne RFID-brikker for lettere gjenfinning av dokumenter. Aktører som håndterer store papirmengder, for eksempel advokatkontorer, er en naturlig kundegruppe for denne anvendelsen.
- Ved en skole i Osaka, Japan, merkes skolebarna med RFID-brikker av sikkerhetshensyn. Alarmer går hvis noen er i ferd med å bevege seg ut av skolegården. Slike systemer kan brukes også på andre områder hvor man vil sikre at noen holder seg innenfor et gitt område, fordi de ellers kan være en fare for seg selv eller andre.
- Husdyr merkes mange steder med RFID-brikker, og merkingen kan følge kjøttet helt til ferskvaredisken. Dette for at man skal kunne kjenne kjøttets opprinnelse og historie og gjenfinne farlig kjøtt ved eventuelle utbrudd av sykdom som kugalskap eller skrapesyke.
- Under SARS-epidemien i Asia i 2003 ble helsearbeidere og pasienter på et sykehus i Singapore merket med RFID-brikker for å forhindre sykdomsspredning gjennom muligheten til å spore opp hvem som hadde vært i kontakt med personer som senere fikk påvist sykdommen.

Det bruksområde hvor RFID i dag opplever aller sterkest vekst er innen varelogistikk, hvor paller og containere kan merkes for å optimalisere og automatisere vareflyt på ulike stadier av verdikjeden. Den danske potetgullprodusenten Kims har for eksempel tatt i bruk RFID til dette formål, og har som følge av dette kunnet holde lavere lagernivåer og redusere antall

[45]Wikipedia, 2005: *RFID* http://en.wikipedia.org/wiki/RFID

ansatte. Til forskjell fra individnære bruksområder har slik merking på pallenivå ingen merkbare konsekvenser for personvernet.

Nye bruksområder
Enkelte butikker utprøver RFID-merking av enkeltvarer i hyllene for å bedre lagerstyring, hindre tyverier samt effektivisere utsjekk og betaling i kasse. I motsetning til strekkoder som kun identifiserer hvilke produkter man kjøper, kan RFID unikt identifisere hver enkelt enhet av alle varer – slik at for eksempel hver melkekartong kan ha sitt eget unike nummer. Da blir det eksempelvis enkelt for butikken å følge med på om de har produkter med overskredet holdbarhetsdato. Dessuten kan tyverier bli svært vanskelige når alle varer er merket slik at de registreres med radiobølger ved kassene eller utgangen. Manuell behandling i kasser kan bli overflødig, og kunden kan selv ta varene gjennom et utsjekkspunkt med betalingsterminal.

Når varene er vel hjemme kan RFID-brikker potensielt brukes til å holde styr på hva man har. Intelligente kjøleskap kan avlese holdbarhetsdatoen på alle varene og si fra når noe er gått ut på dato. Og lurer man på hvor det er blitt av en ting som er merket med RFID, kan man ta en bærbar RFID-leser med seg rundt i huset inntil man ser at den savnede tingen er nær nok til å kommunisere med leseren. RFID-merkede klær kan også kodes med vaskeanvisninger, slik at morgendagens vaskemaskiner automatisk kan velge riktig vaskeprogram basert på hva man legger inn. Merking av enkeltvarer i butikker forsinkes av at RFID-brikkene fortsatt er litt for dyre til å merke annet enn kostbare produkter og av at protestene fra bekymrede kunder og interessegrupper har vært sterke i land som USA og Tyskland, hvor utprøvingen har kommet lengst.

RFID-brikker i identifikasjonskort som pass er også noe som forventes å bli mer vanlig. Slike kan for eksempel lagre biometriske data om eieren og gjøre det svært vanskelig å forfalske slike ID-kort. Dessuten kan slike kort forenkle og tildels automatisere autentisering i enkelte tilfeller. For eksempel kan man tenke seg aksesskontrollsystemer på flyplasser hvor scanning av en passasjers iris kombineres med automatisk avlesning av dennes RFID-baserte pass for å kontrollere at en passasjer er den hun hevder å være.

Faktisk er det omtrent slik at kun fantasien setter grenser for mulige anvendelsesområder for RFID. ”Radiomerking” av ting, dyr og mennesker for enkel identifikasjon kan finne en rekke framtidige bruksområder som vil være svært nyttige. Men de kan også være problematiske i forhold til menneskers vern mot unødig identifikasjon. Derfor er det viktig at ikke bare vår fantasi, men også personvernhensyn er med på å bestemme grensene for anvendelser av RFID.

Personvernutfordringer
RFID utfordrer personvernet på en rekke områder. Her er noen viktige eksempler på problemområder:

- RFID-brikker er små og lite synlige. Ofte vil de være integrert i produktene slik at kunden ikke kan finne dem eller ta dem bort fra varen etter at den er kjøpt.
- RFID-brikker kan avleses på noe avstand, uten at eieren av de merkede produktene merker noe til det. Utenforstående kan slik spore hva folk kjøper gjennom å stå strategisk plassert med en skjult RFID-leser.

- Hvis man betaler med kredittkort eller gjør bruk av et bonuskort vil identiteten til kjøperen lett kunne knyttes direkte til hva hun har kjøpt, noe som kan muliggjøre sporing av en person gjennom sporing av de RFID-merkede varer hun har kjøpt
- Bruk av unike ID-numre for hver enkelt enhet av et produkt (slik at to identiske brusflasker har ulike ID-numre) er i de fleste tilfeller unødig, men gjør det mulig å spore enkeltprodukter også etter at de er kjøpt og betalt.
- Implantering av RFID-brikker under huden på mennesker åpner muligheten for sporing av den enkeltes bevegelser.

De fleste problemene er knyttet til det faktum at RFID-brikker i utgangspunktet forblir funksjonelle også etter at kunden forlater butikken, og at det man kjøper på ulike måter kan scannes av utenforstående. Når store euro-sedler muligens blir RFID-merket fra 2005 kan kanskje lommetyver finne ut hvor mye penger du har i lomma før de avgjør om du er et passende offer. Selv om RFID-systemer primært er utformet for avlesning kun på relativt nært hold, er det mulig med spesielle antenner å lese RFID-brikker på relativt lang avstand. Slik kan man tenke seg at innbruddstyver kan scanne innholdet i et hus på avstand for å vurdere hvilke verdier som befinner seg på innsiden.

Pass eller andre identifikasjonskort med RFID har også noen alvorlige potensielle side-effekter. Man kan tenke seg at det blir svært enkelt å finne identiteten til de personer som er på et bestemt sted med et slikt ID-kort i lomma. Et eksempel som ofte nevnes er at myndighetene eller andre kan møte opp på politiske protestmøter eller andre kontroversielle samlinger og ubemerket samle inn data om alle de tilstedeværende som har ID-kort på seg. Problemstillinger knyttet til RFID i ID-bevis er svært aktuell ettersom pass med biometriske data lagt på usikrede RFID-brikker planlegges innført både i USA og i Europa. Nettopp det faktum at det er valgt en usikret løsning gjør at mange frykter at de nye passene skal kunne øke forekomsten av identitetstyveri.[46]

Et annet kontroversielt innsatsområde for RFID-brikker er knyttet til implantering av slike brikker under huden på mennesker. Det kan være flere grunner til å gjøre dette, men en konsekvens er at personens bevegelser langt på vei vil kunne spores ettersom nettet av RFID-lesere tetner til. Den vanligste grunnen til implantering av RFID-brikker så langt er at mennesker med spesielle medisinske tilstander er redde for feilbehandling hvis de bringes bevisstløse til sykehus og ikke kan fortelle om sin tilstand. Implanterte RFID-brikker kan scannes ved ankomst til sykehus, slik at behandlende personell kan finne den nødvendige informasjonen for å gi pasienten riktig behandling. Et annet profilert bruksområde er knyttet til adgangskontroll til sensitive områder, da som et slags alternativ til biometri. Mexicos generaladvokat og 160 medarbeidere på hans kontor fikk høsten 2004 implantert RFID-brikker som ledd i adgangssikring av de mest sensitive delene av deres kontorer.

De problemene vi her har nevnt kan synes så store at det er fristende å mene at hele RFID-konseptet bør forkastes i forhold til bruk på sluttprodukter, så er ikke nødvendigvis det noen hensiktsmessig konklusjon. Det er mulig å treffe sikringstiltak som motvirker de problemene vi har nevnt. For eksempel kan signalene fra en RFID-brikke sikres mot lesing fra andre enn helt spesifikke lesere, eller signalene som sendes kan krypteres slik at ikke hvem som helst skal kunne lese innholdet. På den annen side er sikringstiltak aldri ufeilbarlige, og ressurs-

[46]Teknologirådet i Danmark, 2005: *På vej mot biometriske pas* http://www.tekno.dk/pdf/nummer198.pdf

sterke kriminelle ligger gjerne i forkant av sikringstiltakene. Dessuten er det grunn til å tro at bruken av RFID i de fleste tilfeller vil basere seg på billige og enkle, usikrede varianter.

Den sikreste måten å unngå personvernproblemer på er å kreve at RFID-brikker på varer enten deaktiveres automatisk når man forlater butikken, eller i det minste plasseres på en avtakbar merkelapp slik at kunden selv kan fjerne den. Problemet med dette er at man går glipp av de mulighetene man ellers kunne ha til å dra nytte av merkingen i hjemmet, for eksempel i forhold til varer i kjøleskapet eller vaskeanvisninger for klær. Igjen har vi en situasjon hvor hensyn til personvern og brukervennlighet må avveies.

For mer om personvernkonsekvenser knyttet til RFID-teknologi, se uttalelsen fra EUs eget rådgivende organ for personvernspørsmål, den såkalte Artikkel 29-gruppen.[47]

6.6 DRM-teknologier

Teknologi for sikring av opphavsrettigheter til digitalt innhold (Digital Rights Management – DRM) er nå blitt en utfordring for personvernet, fordi disse teknologiene så langt har blitt utviklet uten særlig tanke for personvernet. Mens det er et legitimt krav fra innholds-leverandører at det må gå an å sikre åndsverk også i digital form mot kopiering og illegal distribusjon, er det samtidig et rimelig krav at det må gå an for konsumenter å nyte under-holdningsprodukter uten å måtte identifisere seg.

De fleste av dagens DRM-løsninger krever at brukeren identifiserer seg og beviser at hun har rett til å aksessere innholdet. Dette begrenser muligheten til anonymt innholdsforbruk og åpner for bygging av personprofiler med informasjon om hva brukere ser på, lytter til og leser. Slik nærgående informasjonsinnsamling er svært problematisk fra et personvern-synspunkt.[48] Teknologirådet vil i 2005 gjennomføre et prosjekt som ser nærmere på DRM-teknologier.

6.7 Sikkerhetsutfordringer på hjemme-PC

Begrepet IKT-sikkerhet oppfattes gjerne å omfatte sikring av informasjonssystemer, servere og annet IKT-utstyr i bedrifter og organisasjoner. Utviklingen i trusselbildet mot PC-er som er tilkoblet internett har derimot gjort det nødvendig også for private brukere å ta sikkerhet på alvor. Hensikten med sikring av hjemme-PC er primært å hindre uønskede hendelser som at informasjon som er lagret på harddisken kan komme på avveie, at utenforstående kan misbruke PC-en eller internettforbindelsen til tvilsomme eller ulovlige aktiviteter og å hindre ødeleggelse på eget og andres utstyr som følge av ondsinnet programvare, som for eksempel virus. Slike hendelser er ikke utelukkende et sikkerhetsproblem, men kan også ha personvernmessige konsekvenser. For eksempel kan utenforstående få tilgang til privat e-post eller dokumenter med sensitiv informasjon hvis slike er lagret på en hjemme-PC. Eieren av en hjemme-PC kan dessuten bli mistenkt for ulovligheter hvis en utenforstående har hacket seg inn og misbrukt hennes PC eller usikrede internett-forbindelse.

---

[47] Article 29 Data Protection Working Party, 2005: *Working document on data protection issues related to RFID technology*. http://www.statewatch.org/news/2005/feb/wp105.pdf

[48] For en nærmere beskrivelse av dette temaet, se Lee A. Bygrave, 2002: *The Technologisation of Copyright: Implications for Privacy and Related Interests* http://folk.uio.no/lee/publications/technologisation_copyright_eipr_final.pdf og Lee A. Bygrave, 2003: *Digital Rights Management and Privacy – Legal Aspects in the European Union* http://folk.uio.no/lee/publications/DRM_privacy.pdf

Svært mange privatbrukere sikrer ikke sin hjemme-PC tilstrekkelig, enten fordi de ikke er bevisst på behovet for dette, eller fordi de ikke vet hvordan de kan gjøre det. Dessverre er en fullgod sikring av en PC ofte for komplisert for ordinære brukere, så man kan knapt vente at de skal gjøre alt det riktige. Det ser heller ikke ut til at IKT-leverandører i noen særlig grad tar ansvar for å gi brukerne lettfattelig informasjon om hva de bør gjøre for å sikre det utstyret de kjøper. Mens det på større arbeidsplasser gjerne finnes noen som har et profesjonelt ansvar for å ivareta sikkerheten, må private brukere selv ta ansvar og så godt de kan være sin egen IKT-sikkerhetssjef. Behovet for sikringstiltak på hjemme-PCer forsterkes kraftig som følge av at stadig flere privatbrukere tar i bruk nye teknologier for tilkobling til internett, nærmere bestemt bredbåndsforbindelser og trådløse lokalnett.

6.7.1 Bredbånd og hacking

Bredbåndsforbindelser i hjemmene øker folks tilgjengelighet til nettressurser og muliggjør nye typer tjenester, men har den ulempe at de gir økt sårbarhet for hacking. Med begrepet hacking forstår vi her elektroniske innbrudd, altså at noen uten samtykke bryter seg inn på en PC for enten å hente ut informasjon, bedrive hærverk eller for å misbruke PC-en til tvilsomme eller kriminelle formål. Tradisjonelt har bedrifters servere vært mest utsatt for hackere, men ettersom sikkerheten i de fleste bedrifter har blitt bedre, har private brukere blitt mer attraktive mål for hackere. Nyere hjemme PC-er har ofte kraftige prosessorer og raske bredbåndsforbindelser, men svak sikkerhet – alt hva en hacker kan ønske seg.

Hackere bruker en metode som kalles *portscanning* for å lete etter sårbare PC-er som er tilkoblet internett. Brukere med oppringt forbindelse til internett er i praksis relativt godt beskyttet mot hacking av det faktum at forbindelsen er oppe bare en begrenset tid for hver gang og at brukeren får en ny IP-adresse ved hver pålogging. Dette begrenser uten-forståendes muligheter til å finne og utnytte en sårbar maskin før nettforbindelsen tas ned. Stadig flere går derimot over til bredbåndsforbindelser som for eksempel ADSL eller internett over kabel-TV. Da er PC-en normalt oppkoblet mot nettet over lang tid og som regel med samme IP-adresse for hver gang (med mindre bredbåndsruteren slås av). Slik blir eventuelle åpne logiske kommunikasjonsporter inn til PC-en mer eksponert for eventuell portscanning, samtidig som eventuelle angripere har god tid til å utnytte de mulighetene de måtte finne.

Følgelig er det viktig at bredbåndsbrukere har ekstra sikring mot hacking i form av en brannmur, enten innebygd i bredbåndsruteren eller installert lokalt på PC-en. En brannmur beskytter mot portscanning og sørger således for at angripere går videre til et enklere offer.[49] Det finnes gratis brannmurer som kan lastes ned fra nettet, dessuten har operativ-systemer som Windows XP og MacOS X brannmur innebygget – de må bare aktiveres av brukeren.[50]

6.7.2 Trådløse lokalnett

Det har i løpet av de siste par årene blitt stadig mer vanlig med bruk av trådløse lokalnett (WLAN) i hjemmene. Slikt utstyr har i løpet av de siste par årene blitt svært billig, slik at det nå selges i store mengder fra ordinære elektrovarehus. Et trådløst lokalnett gjør det mulig å

[49]For mer informasjon om brannmurer se 1984.dk: http://www.1984.dk/beskyt/firewalls.shtml
[50]For en beskrivelse av hvordan man enkelt kan sikre en Windows-PC se Microsoft: http://www.microsoft.com/security/protect/default.asp

være på internett fra ethvert rom i huset, og gjør det enkelt å dele en nettforbindelse mellom flere PC-er. Ulempen er at signalene fra det trådløse aksesspunktet som regel rekker langt utenfor husets vegger og således kan nå fram til utenforstående, som for eksempel naboer eller folk som kjører forbi med PC i bilen på jakt etter ubeskyttede nett. Dette kan potensielt være et alvorlig problem hvis man ikke gjør noe for å sikre det trådløse nettverket mot utenforstående.

Og det er et sørgelig faktum at de aller fleste private brukere ikke treffer nødvendige tiltak for å sikre de trådløse aksesspunkter de installerer i sine hjem. Årsakene til dette er nok både en manglende kjennskap til de potensielle problemer dette kan medføre, og det faktum at leverandører av slikt trådløst utstyr leverer utstyret slik at det er enkelt å ta i bruk, men slett ikke like enkelt å aktivere sikkerhetsfunksjonene. De som selger slikt utstyr ser heller ikke ut til å gjøre noe for å informere kundene om hvordan de bør sikre sine trådløse nett.

Hovedproblemet med usikrede trådløse nettverk er at uvedkommende lett kan misbruke internettforbindelsen. Slikt kan ofte være uproblematisk ettersom de fleste bredbånds-forbindelser har fastpris uavhengig av trafikk, men hvis den som tyvlåner forbindelsen begår ulovligheter, kan det bli ubehagelig. En eventuell sporing av tyvlånerens aktiviteter vil gjennom IP-adressen lede til eieren av det trådløse nettet, slik at denne kan bli mistenkt og etterforsket for de kriminelle forhold som måtte være begått av inntrengeren. I tillegg til slikt misbruk er det mulig å overvåke og sniklese i trafikken over usikrede trådløse forbindelser, og i mange tilfeller vil det også være relativt lett snoke i data på den eller de PC-er som er tilknyttet det trådløse nettverket. Det siste gjelder spesielt hvis PC-ene i det lokale nettverket er satt opp til å dele filer seg imellom. I motsetning til hva mange tror, kreves ikke spesielt stor kunnskap for å foreta slike hacker-aktiviteter. Gratis verktøy for slikt ligger åpent for nedlasting på internett, slik at nesten hvem som helst kan få til å utføre slik elektronisk ”spionasje” på noen som har et usikret trådløst nettverk.

Det brukere av trådløse nettverk kan gjøre for å sikre seg er å aktivere kryptering av signalene i det trådløse nettet, slik at det ikke er så lett å avlytte eller misbruke det. I tillegg kan man ved bruk av såkalte MAC-adresser tillate kun definerte PC-er å bruke det trådløse aksesspunktet. Begge disse tiltakene kan riktignok brytes av ressurssterke hackere, men de gir god beskyttelse mot mer tilfeldig eller opportunistisk misbruk. Brukere av trådløse nett bør dessuten ha en personlig brannmur installert og aktivert på sin PC, ettersom en brannmur i bredbåndsruteren ikke beskytter mot innbrudd via radiobølgene mellom det trådløse aksesspunktet og PC-en. [51]

6.7.3 Andre sikkerhetstrusler

Uavhengig av tilkoblingsmetode til internett, er det en rekke sikkerhetsmessige trusler som i økende grad rammer folks hjemme PC-er. De fleste av disse kan i større eller mindre grad sies å ha noe med personvern å gjøre. Mest kjent er virus, men fenomener som spyware og phishing (”fiskepost”) er minst like alvorlige for personvernet. Mange av disse truslene kan ikke møtes med tekniske sikringstiltak alene, men krever en viss fornuft og kritisk sans hos brukeren. De typer av trusler som i den senere tid har vært i spesielt sterk vekst er basert på det man kaller *social engineering*, det vil si at man forsøker å lure brukeren til selv å gjøre

[51] For veiledning til sikring av trådløse nett, se Rådet for IT-sikkerhet, Danmark: http://www.tst.dk/static/publikationer/pjecer/sikkerhed/index.htm

egen PC sårbar for innsyn (for eksempel ved å åpne vedlegg med virus) eller til å avsløre sensitiv informasjon (ved å respondere på "fiskepost").

Virus og ormer

Det mest utbredte og best kjente sikkerhetsproblem er virus. Et virus er et stykke ondsinnet programvare som er skrevet for å reprodusere seg selv og spre seg videre til andre PC-er. Dette gjøres ved at det knytter seg til et vertsprogram og utnytter dette til spredningen. Graden av skade et virus kan volde spenner fra det lett irriterende til det svært skadelige. I verste fall kan et virus utøve skade på programmer, maskinvare og dokumenter og dessuten spre privat informasjon til tredjeparter (for eksempel ved å videresende privat e-post).

Ormer er en underkategori av virus som utmerker seg ved at de ikke trenger et vertsprogram for å spre seg fra en PC til en annen. Hvis man får en orm på sin PC kan denne selv ta kontroll over den nødvendige funksjonaliteten for å sende ut kopier av seg selv, for eksempel til alle i adresseboken. Ormer kan også åpne såkalte "bakdører" på en PC og slik gjøre det mulig for andre å ta kontroll over PC-en og misbruke den til egne formål.[52]

Den viktigste måten å beskytte seg mot virus på, er for brukerne ikke å åpne vedlegg i e-poster uten at man er trygg på innholdet i dem. Dessuten bør man ha installert antivirus programvare som automatisk oppdateres når maskinen er tilkoblet nettet. En brannmur har begrenset effekt mot virus og ormer, men vil normalt kunne hindre en orm i å åpne en bakdør inn til PC-en.

Phishing ("fiskepost")

Begrepet *phishing* spiller på at noen "fisker" etter personopplysninger og viser til et fenomen som har eksistert en stund, men som i den senere tid har økt dramatisk i omfang. I flere år har såkalte "Nigeria-e-post" lurt både nordmenn og andre til for eksempel å oppgi sitt kontonummer for angivelig å hjelpe noen med en pengeplassering mot klekkelig betaling. I dag er både nigeriansk mafia og andre organiserte kriminelle blitt atskillig mer sofistikerte i sine forsøk på å lure penger fra folk på nettet. Phishing er en type spam hvor e-posten utgir seg for å være fra en kilde man normalt stoler på. Målet med dette er å lure mottakeren til å oppgi sensitiv informasjon som noen kan misbruke til egen fordel, som regel i form av identitetstyveri, eller annen økonomisk kriminalitet. Det vanligste er at e-posten ser ut som den kommer fra banken, og de beste eksemplene kan være svært vanskelige å avsløre som falske. Som regel vil en link i e-posten henvise mottakeren til en webside som ser mer eller mindre helt lik ut som bankens faktiske hjemmeside. Her bes brukeren for eksempel enten logge seg på med brukernavn og passord slik at disse kan snappes opp, eller man forsøker å lure brukeren til å oppgi konto- eller kredittkortnummer.

Fra å ha vært et relativt ukjent begrep i første halvdel av 2003, ble phishing et av de mest synlige sikkerhetsrelaterte problemene innen våren 2004. En undersøkelse fra MessageLabs viste en 800-dobling i mengden av phishing-eposter på seks måneder, fra 280 i september 2003 til 215.000 i mars 2004.[53] Andre undersøkelser bygger opp under inntrykket av en dramatisk økning i mengden av slik fiskepost, og dette er nå også blitt et alvorlig problem for store banker. Amerikanske Citibank advarer for eksempel på sine nettsider mot slik

---

[52]Senter for informasjonssikring: Ondsinnet kode
http://www.norsis.no/details.php?type=veiledninger&id=49

[53]Techweb SecurityPipeline: *Phishing e-e-posts jump 800-fold in six months*
http://www.securitypipeline.com/showArticle.jhtml?articleID=18902562

forfalsket e-post, og legger ut en liste over all oppdaget phishing-post som gir seg ut for å være fra denne banken.

En spørreundersøkelse gjennomført av Gartner viser at 57 millioner nettbrukere i USA mener seg utsatt for phishing-forsøk. Av disse var det 11 millioner, eller 19%, som innrømmet å ha klikket på lenken i e-posten, og av disse hadde nesten to millioner, eller 3%, faktisk blitt lurt til å gi sensitive opplysninger til den falske nettsiden. Gartner melder at det er en høy korrelasjon mellom ofre for phishing og de som blir utsatt for identitetstyveri. Grunnen til at phishing øker så dramatisk, er nettopp det at de som fisker etter personopplysninger såpass ofte har suksess og får opplysninger de kan bruke til å svindle noen. Samtidig sier den samme undersøkelsen at risikoen for å bli tatt for den som står bak et phishing-forsøk er så lav som en til 700. Gartner mener at hvis utviklingen fortsetter, vil phishing kunne ødelegge kundenes tiltro til all elektronisk handel og slik medføre et tilbakeslag for all netthandel.[54]

Spyware

Spyware er spionerende programvare som uten samtykke samler informasjon om en PC-bruker og hennes aktiviteter på nettet, og sender dette tilbake til de som står bak spionprogrammet.[55] Tidligere har dette vært betraktet som et begrenset problem som i første rekke har rammet uforsiktige brukere og som ikke har vært så farlig. Mesteparten av slike sladreprogrammer har tradisjonelt vært såkalt *adware*, det vil si programmer som brukes til markedsanalyse og reklame. Slike programmer vil for eksempel kunne overvåke brukerens internettvaner, og sende informasjon om brukerens interesser eller preferanser tilbake til det markedsføringsfirmaet som står bak.

I den senere tid har spyware derimot kommet mer fram i lyset som et alvorlig problem både for vanlige brukere og bedrifter. Spyware er ikke lenger bare et uttrykk for nærgående markedsanalyser, men brukes også av kriminelle som forsøker å skaffe informasjon som kan misbrukes til økonomisk vinning. Mens spyware har mye til felles med virus og ormer, skiller dette seg ut med at det normalt er knyttet et økonomisk motiv til å sende ut slike programmer. Gartner anslår at spyware og phishing til sammen har bidratt til svindel for 2,4 milliarder dollar i løpet perioden mai 2003 til april 2004, bare i USA.[56] De sier videre at det er en stadig økende andel av økonomisk kriminalitet som nå kommer gjennom elektroniske kanaler.

Trojanske hester og systemmonitorer er eksempler på alvorlige former for spyware. En *trojansk hest* (også kalt trojaner) er et program som gir seg ut for å være nyttig, men som når det først er installert viser seg å inneholde skadelig kode, på samme måte som virus og ormer. En *systemmonitor* er på sin side et stykke programvare som overvåker aktivitetene på en PC og kan rapportere om alt som skjer, for eksempel hva man sier til andre i chat-rom eller på e-post. Det mest utbredte eksempel på en systemmonitor er en *tastaturlogger* som loggfører alle tastetrykk i den hensikt å snappe opp sensitiv informasjon som brukernavn, passord og kredittkortnumre.

---

[54]Techweb SecurityPipeline, 06.05.2004: *Gartner: Phishing attacks threaten e-commerce*
http://www.securitypipeline.com/showArticle.jhtml?articleID=20000036

[55]For en grundig innføring i spyware, se Center for Democracy & technology, November 2003: *Ghosts in our machines. Background and policy proposals on the "spyware" problem*
http://www.cdt.org/privacy/031100spyware.pdf

[56]Techweb, 15.06.2004: *Key loggers, phishers sock consumers for $2.4 Billion*
http://www.techweb.com/wire/story/TWB20040615S0008

Spyware er ikke å betrakte som virus, og spres som regel heller ikke på samme måten. Riktignok kan spyware utplasseres også ved hjelp av virus, men den vanligste måten å få spyware på er gjennom nedlasting av gratis programvare. For å finansiere den gratis programvaren tillates ofte spyware å "følge med på kjøpet" uten at brukeren er klar over dette. Fildelingsprogrammer som for eksempel *Kazaa* er kjent for å komme med spesielt mye spyware. Fenomenet er i løpet av den senere tid blitt svært utbredt, og en undersøkelse fra april 2004 viser at hver PC i gjennomsnitt har ca 27 spyware-programmer på hard-disken[57]. Mens de fleste av disse er ganske harmløse, viser undersøkelsen at hver tredje PC er infisert med en trojaner eller en systemmonitor som er plassert av spyware. Ut over de rent personvernmessige problemene dette kan medføre, er det et faktum at den store mengden av spyware også bidrar til å gjøre PC-er tregere og mer utsatte for systemkrasj.

I tillegg til den type spyware som kommer fra utenforstående med økonomiske motiver knyttet til markedsføring eller identitetstyveri, finnes også rene overvåkningsprogrammer myntet på sjalu ektefeller, kontrollerende foreldre og mistenksomme arbeidsgivere som vil overvåke i detalj all aktivitet og kommunikasjon fra en PC. Slike programmer kan installeres direkte på PC-en av et familiemedlem, eller for eksempel sendes i e-post til offeret, gjerne kamuflert som et gratulasjonskort eller lignende.[58] Brukeren kan ikke på noen enkel måte selv finne ut at overvåkning foregår, ettersom slike programmer vil være usynlig for brukere. Men det finnes på internett gratis nedlastbar programvare for fjerning av spyware. Flere programmer som har gitt seg ut for å skulle fjerne spyware har vist seg selv å være spyware, men flere uavhengige kilder ser ut til å være enige om at i hvert fall følgende to programmer kan anbefales som trygge til dette formålet: *Ad-aware* og *Spybot Search & Destroy*.[59]

Lokale internettlogger

Etter å ha nevnt muligheten for at familiemedlemmer med stort kontrollbehov kan installere spionprogrammer på familiens PC-er, er det på sin plass å nevne at helt vanlige nettlesere (browsere) som Microsoft Internet Explorer, Opera og Safari også normalt vil loggføre mye av aktivitetene på PC-en. Slik er det faktisk mulig å spionere ganske nær-gående på familiemedlemmenes internett-bruk selv uten egne spionprogrammer.

Sporene som etterlates lokalt knytter seg primært til loggføring av alle besøkte nettsider over en periode på typisk 20 dager, midlertidige internett-filer og informasjonskapsler (cookies), alle ting som vil sladre om hvilke steder man har besøkt på internett. Mange vil mene at dette ikke er noe å bekymre seg over, men brukere som ikke ønsker at andre brukere skal kunne kikke en i kortene kan slette slik informasjon fra nettleseren.

E-postreklame (spam)

Selv om uønsket reklame i utgangspunktet ikke representerer noen fare for mottakerens personopplysninger, oppfattes det av mange som et brudd på retten til å kunne få være i fred, og til å unngå uønsket kommunikasjon. Et annet problem er at skadelig programvare som virus eller "fiskepost" ofte spres gjennom spam. Det faktum at det er så lett å bli rammet av spam illustrerer hvor vanskelig det kan være å beskytte personopplysninger som brukeren selv legger igjen ulike steder på nettet. Man trenger ikke oppgi e-postadressen sin

---

[57] Information Week, 17.06.2004: *Spyware is everywhere*
http://www.informationweek.com/showArticle.jhtml?articleID=22100609

[58] Aftenposten, 03.01.2004: *Skjulte programmer overvåker PC-en din*
http://www.aftenposten.no/nyheter/nett/article700685.ece

[59] Ad-aware kan finnes på: http://www.lavasoft.de/software/adaware SpyBot Search & Destroy kan finnes på: http://beam.to/spybotsd

mange steder før den blir sårbar for spredning til noen som sender spam. Følgelig er det beste tiltaket for å unngå spam å hemmeligholde sin primære e-postadresse for alle andre enn folk man stoler på, og heller oppgi en annen og mindre personlig e-postadresse (for eksempel hos Hotmail eller Yahoo!) til andre aktører på internett. Så kan man heller bytte denne adressen når den blir utsatt for spam.

6.8 Intelligente omgivelser

Konseptet *intelligente omgivelser* (Ambient Intelligence - AmI) representerer en visjon for informasjonssamfunnets framtid hvor det sentrale fokus for bruk av IKT er brukervennlighet, effektive og distribuerte tjenester, brukerfokus og støtte for menneskelig interaksjon. Man ser for seg at mennesker vil være omgitt av intuitive grensesnitt til intelligente objekter, og omgivelser som mer eller mindre umerkelig kan tilpasse seg brukerne. I stedet for at mennesker må tilpasse seg teknologien, vil da teknologiene måtte designes rundt menneskets behov og forutsetninger.

Såkalte smarthusteknologier er første steg på veien mot visjonen om intelligente omgivelser. Smarte hus integrerer IKT til å støtte eller automatisere prosesser som for eksempel styring av lys og varme, intelligente alarm- og varslingssystemer, automatisk styring av vinduer og dører samt systemer for kommunikasjon og underholdning. Intelligente omgivelser innebærer at IKT blir allestedsnærværende og integrert i de ting vi omgir oss med til daglig, både i hjemmet og andre steder. Slik skal hver enhet bli kontekstsensitiv slik at den kan detektere hva som er situasjonen for brukeren, og adaptiv slik at den kan tilpasse seg og reagere ulikt, alt etter situasjonen og den aktuelle bruker. For eksempel kan en mobiltelefon reagere ulikt på et innkommende anrop basert på hvor brukeren er. Hvis hun befinner seg i bilen, kan telefonen selv avgjøre at den ikke skal ringe, men heller ta imot en beskjed på svareren. På jobben kan det samme skje når man går inn på et møterom, mens et anrop hjemme kan medføre at radioen automatisk demper lyden eller at TV-en viser en melding om hvem sin telefon som ringer.

AmI er ikke et nytt teknologiområde, men snarere et resultat av konvergens mellom ulike IKT-områder. Allestedsnærværende IKT med tallrike, små og billige prosesseringsenheter knyttet sammen over trådløse nettverk utgjør kjernen i denne visjonen. Teknologien skal bli tilnærmet usynlig og integrert i våre naturlige omgivelser, den skal være tilgjengelig når vi trenger den og kunne fungere uten særlig innsats fra brukeren. Den skal dessuten kunne tilpasse seg brukere og situasjoner, og den må kunne handle selvstendig uten å bli instruert av brukeren.[60] Bruksområdene for intelligente omgivelser vil kunne dreie seg om områder som sikrere veitrafikk, smarte hjem og arbeidsplasser samt smarte tekstiler.

Intelligente omgivelser vil stille oss overfor forsterkede utfordringer i vernet av privatsfæren. Man kan forestille seg at når alt mulig skal tilpasse seg brukeren, vil denne konstant måtte identifiseres på et eller annet nivå. Da vil det bli mulig for alle de intelligente objektene i omgivelsene å loggføre data om brukernes bevegelser og handlinger, for så å utveksle disse dataene over nettet. Det faktum at teknologien forsvinner fra brukerens øyne og inn i omgivelsene forsterker problemet, ettersom den enkelte i svært liten grad vil være oppmerksom på når hun etterlater seg elektroniske spor.

---

[60]Menno Lindwer m.fl., 2003: Ambient Intelligence Visions and Achievements: Linking Abstract Ideas to Real World Concepts http://www.ece.cmu.edu/~sld/pubs/papers/DATE03.pdf

Trygghet for brukerne gjennom en god sikring av deres personvern vil være en forutsetning for at folk vil ønske å ta slik teknologi i bruk. Systemene må da utformes slik at brukerne forblir mest mulig anonyme eller pseudonyme overfor de intelligente omgivelsene, og slik at unødige loggdata ikke kan lagres over lengre tid. I de tilfeller hvor identifiserbare data blir lagret, må det stilles krav til effektiv sikring av disse dataene.

Visjonen Ambient Intelligence er integrert i EUs sjette rammeprogram for forskning og utvikling, og er gjenstand for betydelig forskningsinnsats fra både universiteter, forskningsinstitutter og kommersielle selskaper (som for eksempel Philips). For mer om intelligente omgivelser, se EU-rapporten AmI@Life[61] og scenarierapporten fra EUs ekspertgruppe IST Advisory Group.[62]

[61]European Science and Technology Observatory, IPTS, EU-kommisjonen, 2003: Science and Technology Roadmapping: Ambient Intelligence in Everyday Life (AmI@Life) http://esto.jrc.es/docs/AmIReportFinal.pdf

[62]Information Society Technologies Advisory Group (ISTAG), EU-kommisjonen, 2001: Scenarios for Ambient Intelligence in 2010 ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf

Kapittel 7 Samfunnssikkerhet og overvåkning

Trygghet for innbyggerne samt beskyttelse av samfunnets orden er verdier som folk setter svært høyt, både i vårt eget og i andre land. Folk tar det derfor langt på vei som en selvfølge at myndighetene innenfor rimelighetens grenser gjør det de kan for å bevare freden, og beskytte borgerne mot terror og annen alvorlig kriminalitet. Men hvilke tiltak er innenfor rimelighetens grenser og hvilke er utenfor? Hvilket overvåkningsnivå i samfunnet må til for effektivt å kunne bekjempe alvorlig kriminalitet, og hvilke tiltak kan vi tåle uten at personvernet lider uforholdsmessig mye? Disse spørsmålene finnes det ulike svar på alt etter hvem man spør. De fleste vil uansett være enige om at både frihet og sikkerhet må ivaretas. Da må alvorlig kriminalitet bekjempes, samtidig som personvernet må sikres. Dette krever en fornuftig og balansert avveining av to ulike, men likeverdige hensyn, i alle spørsmål som berører sikkerhet og personvern. Teknologirådet tar ikke stilling til hvor grensene bør gå, men søker å gi beslutningstakere innsikt i problematikken slik at de kan føre informerte diskusjoner.

7.1 Nye metoder i kriminalitetsbekjempelse

Som nevnt i Kapittel 2, er det en rekke faktorer som medfører et behov for nye metoder i kriminalitetsbekjempelse. Kriminalitetsbildet er endret i retning av grovere kriminalitet, økt internasjonal og organisert kriminalitet, mer datakriminalitet og økt terrorfare. Verden er blitt mer sårbar og et farligere sted å leve, arbeide og drive forretningsvirksomhet. Grunnen er at mennesket kan forflytte seg raskt og kommunisere uten forsinkelse over hele verden, og fordi det nå er mulig for enkeltpersoner og små grupper å volde stor skade både på materiell og på andre mennesker. Disse forholdene taler for adgang til sterkere virkemidler, også på politiets side. Og den økte avhengigheten av tilgang til spor fra elektronisk kommunikasjon i etterforskning og forebygging av kriminalitet, taler for at nye metoder også rettes inn mot elektronisk kommunikasjonsutstyr.

I USA så man i tiden etter 11.september 2001 en rekke initiativer i retning av økt kontroll og overvåkning. Mens mange av initiativene på områder som biometrisk autentisering, nettovervåkning og datautvinning går videre, er to av de mest ambisiøse systemene stoppet. Dette gjelder det presumtivt altomfattende systemet TIA (Total Information Awareness) som skulle finne potensielle terrorister gjennom å sette sammen informasjon fra alle tilgjengelige kilder, og CAPPS II (Computer Assisted Passenger Prescreening System), som blant annet skulle automatisere risikovurderinger av flypassasjerer og finne ut hvem som ikke kunne få fly, og hvem som måtte sjekkes ekstra grundig før ombordstigning. Disse to systemene ble stoppet primært fordi de etter hvert ble oppfattet som uakseptable av personvernhensyn.[63]

I Norge har det ikke vært aktuelt å utvikle denne type systemer, men også her er det nå snakk om å gi både vanlig politi og Politiets Sikkerhetstjeneste (PST) nye metoder i kriminalitetsbekjempelsen. Politimetodeutvalget avga våren 2004 sin innstilling[64] hvor de

[63]CNET News.com, 20.10.2004: *A global assault on anonymity* http://news.com.com/2009-1009_3-5405947.html?tag=dasec
[64]Politimetodeutvalget (2004)

blant annet foreslår lovfesting av følgende metoder av relevans i forhold til elektronisk kommunikasjon:

- *Teknisk sporing*
  Dette innebærer at politiet kan plassere teknisk peileutstyr på et objekt for å overvåke dets bevegelser. Senderen kan plasseres i personnære objekter som klær, veske eller lignende.
- *Kommunikasjonskontroll*
  Kommunikasjonskontroll handler primært om avlytting eller oppfanging av innhold i samtaler og annen kommunikasjon. Også telefoner den mistenkte forventes å ville ringe vil omfattes av slik kommunikasjonskontroll. Nytt er at det åpnes for bruk av dette tiltaket også i forebyggende øyemed.
- *Dataavlesning*
  Dette innebærer at politiet skal kunne bryte seg inn på en mistenkts datautstyr for å avlese i klartekst informasjon som sendes i kryptert form over nettet. Software- eller hardwarebaserte systemmonitorer brukes til dette formål. Tastatursniffere er et eksempel på slike

Felles for disse tre metodene er at det stilles relativt strenge krav til situasjonen for at politiet skal kunne ta dem i bruk. Det kreves at det må foreligge konkret mistanke om at vedkommende er delaktig i planlegging eller gjennomføring av en alvorlig straffbar handling med strafferamme på fengsel i minst 5 år. For kommunikasjonskontroll og data-avlesning kreves strafferamme på minst 10 år, og dessuten tillatelse fra retten. Selv om disse tiltakene er svært inngripende i de mistenktes personvern, er det betryggende at de skal brukes kun i svært alvorlige saker og at rettssystemet må utføre en kontroll med politiets ønsker om å bruke disse metodene. Man må forutsette at dette vil bidra til å hindre misbruk av slike metoder.

Politimetodeutvalget foreslår også å lovfeste et annet tiltak, nemlig plikt for tilbydere av teletjenester å lagre alle trafikk- og lokasjonsdata i 12 måneder av hensyn til eventuell fram-tidig politietterforskning. Dette tiltaket skiller seg skarpt fra de andre som her er nevnt, på den måten at det her ikke kreves noen form for mistanke for at data skal måtte lagres. Dette forslaget er derfor svært kontroversielt og vi skal se litt nærmere på denne problem-stillingen.

7.2 Mulig lagringsplikt for trafikk- og lokasjonsdata

Politimetodeutvalgets flertall foreslår altså pliktig lagring av trafikk- og lokasjonsdata fra teleoperatører og tjenestetilbydere i ett år. En eventuell slik lagringsplikt for kom-munikasjonsdata, inkludert data om e-post og internettbruk, er et svært omstridt tema både i Norge og internasjonalt. En rekke land innførte i tiden etter 11. september 2001 nye lover og reguleringer om pliktig lagring av kommunikasjonsdata, samt forlenget lagringstid av hensyn til kriminalitetsbekjempelse og avvergelse av terrorhandlinger. Flere europeiske land, deriblant Danmark, har allerede innført obligatorisk lagring av trafikkdata i 12 måneder. Italia har på sin side innført 5 års lagringstid for slike data.

Som en direkte konsekvens av terrorangrepene i Madrid 11.mars 2004, vedtok EU-landenes statsministere på et toppmøte i Brüssel, 25.-26.mars 2004, en tiltakspakke mot terrorisme.[65] Denne fokuserer blant annet på tiltak for overvåkning av elektronisk kommunikasjon, og inneholder en intensjon om å innføre lagringsplikt for trafikkdata i alle EU-land fra juli 2005. Det foreligger nå et konkret forslag om obligatorisk lagring i 1-3 år. Om tiltaket vil bli gjennomført er likevel foreløpig uvisst. EU-kommisjonen avsluttet i september 2004 en høring om forslaget, og det er ingen hemmelighet at det er betydelig motstand mot det. Hvis EU skulle vedta et slikt påbud, vil dette gjelde også for Norge som følge av EØS-avtalen. Lov om elektronisk kommunikasjon fra 2003 åpner også for at en utvidet lagringstid kan innføres i Norge. Ettersom det så langt ikke er kommet noe påbud fra EU om lagring av kommunikasjonsdata, må Politimetodeutvalgets forslag forstås uavhengig av dette.

Om politimetodeutvalgets forslag om lagringsplikt blir gjennomført, vil dette tiltaket medføre at detaljer omkring borgernes elektroniske kommunikasjon vil bli lagret for mulig bruk i en framtidig politietterforskning. Tjenester som fasttelefoni, mobiltelefoni, e-post, websurfing og chattetjenester vil bli omfattet av rutinemessig logging, og dataene vil altså måtte oppbevares over en periode på 12 måneder. Tiltaket kan oppfattes som en form for generell overvåkning av hele befolkningen, ettersom det vil måtte samles inn og lagres data om alle som bruker elektronisk kommunikasjon. Noen vil kunne oppfatte et slikt tiltak som lite målrettet og som en mistenkeliggjøring av uskyldige mennesker. Politimetodeutvalget gjør intet forsøk på å begrunne hvorfor dette er et godt forslag, og de har heller ikke foretatt noen konsekvensvurdering i forhold til personvern.

Det er grunn til å merke seg at lagring av trafikk- og lokasjonsdata fra dagens og morgendagens kommunikasjonstjenester har helt andre konsekvenser i forhold til personvern enn den oppbevaring av tradisjonelle trafikkdata fra telefonitjenester som i dag er vanlig av hensyn til fakturering. Mens trafikkdata tradisjonelt involverer data om telefonnumre, lengden på samtalen og telefonenes omtrentlige posisjon, er trafikkdata fra nyere former for elektronisk kommunikasjon atskillig mer nærgående. Trafikkdata fra internettbruk er for eksempel langt på vei å betrakte som innholdsdata. For eksempel vil nettadresser kunne si mye om innholdet på besøkte sider, og trafikkdata fra søk på nettet vil vise hvilke ord man har søkt på. Beregnede lokasjonsdata fra GPS-utrustede mobiltelefoner kan på sin side være så presise at de ikke bare forteller hvor en person har vært, men langt på vei også hva vedkommende har gjort.

Den britiske organisasjonen Privacy International (PI) har i samarbeid med sammenslutningen European Digital Rights utformet et tilsvar[66] til EU-kommisjonens høring om forslaget til obligatorisk lagring av kommunikasjonsdata i 1-3 år. Her går de i detalj gjennom hva som er de viktigste konsekvensene for personvernet av en eventuell lagringsplikt.

Privacy International konkluderer med at slik datalagring vil være:

- *Invaderende*
  Trafikkdata kan brukes til å kartlegge menneskers sosiale og profesjonelle nettverk,

[65] EUpolitix, 25.03.2004: *Special Report: 'Combating terror' in the EU*
http://www.eupolitix.com/EN/News/200403/a746daaf-9ddd-4948-b542-4a2630ad0f6b.htm

[66] PI, 15.09.2004: Invasive, Illusory, Illegal and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention.
http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html

samt til å gi en oversikt over hvert enkeltindivids aktiviteter og intensjoner. PI mener det er uforståelig at kommisjonen vil vurdere intensivert overvåkning av trafikkdata i en situasjon hvor slike data er blitt langt mer sensitive enn tidligere.

- *Illusorisk*
  Den sikkerhet man vil oppnå ved datalagring kan være illusorisk. Det er sannsynlig at trafikkdata som knyttes til en person faktisk representerer aktiviteter utført av en annen person. På internett er det svært vanskelig å vite hvem som skjuler seg bak en gitt IP-adresse. Man kan derfor i betydelig grad komme til å mistenke uskyldige personer, noe som vil være et svært alvorlig personvernproblem.
- *Ulovlig*
  Lagring av trafikkdata er ifølge PI og en vurdering[67] gjort av Covington & Burling i strid med artikkel 8 i den europeiske menneskerettighetskonvensjonen (EMK), som beskytter retten til et privatliv. Lagringen vil ifølge PI være så omfattende at den vil være helt ute av proporsjon med de hensyn til kriminalitetsbekjempelse den er ment å tjene.

Teknologirådet ser det ikke som sin oppgave å ta stilling til forslaget om lagringsplikt for trafikk- og lokasjonsdata. Det som uansett er et faktum er at en slik datalagring vil representere en omfattende inngripen i borgernes personvern, og at et slikt tiltak kun kan rettferdiggjøres hvis det kan medføre viktige gevinster på området kriminalitets-bekjempelse. Det faktum at de som står bak alvorlig eller organisert kriminalitet også er de som best vet å opptre under andre og uskyldige brukeres IP-adresse på nettet, understreker faren for at et slikt tiltak primært vil ramme uskyldige og småkriminelle. Politimetode-utvalget underbygger heller ikke sitt forslag med informasjon om tiltakets effektivitet i de landene som allerede har innført det.

Om det skulle bli innført obligatorisk lagring av trafikk- og lokasjonsdata, vil det måtte stilles svært strenge krav til oppbevaringen av disse dataene. De må underlegges strenge sikkerhetskrav slik at de ikke lett kan komme på avveie som følge av hacking eller innsyn fra interne utro tjenere.

7.3 Internasjonal etterretning

Den kalde krigen er over, men landenes etterretningstjenester lever videre. Det er utvilsomt et faktum at mange land også i dag driver ulike former for skjult innhenting av informasjon fra andre land. Dagens globale terrortrussel understreker at det fortsatt finnes et behov for denne type tjenester. Det er ikke overraskende at et av virkemidlene som slike tjenester bruker er signaletterretning, det vil si avlytting av ulike former for telekommunikasjon. Men et helt spesielt etterretningsnettverk – Echelon – fortjener omtale i denne rapporten, fordi det hevdes å utgjøre en betydelig trussel både mot vernet av privatpersoners konfidensielle kommunikasjon og private selskapers bedriftshemmeligheter.

Echelon
Echelon er navnet på et verdensomspennende avlyttingsnettverk drevet av en etterretnings-allianse mellom USA, Storbritannia, Canada, Australia og New Zealand[68]. Alliansen går under betegnelsen *UKUSA,* etter de to landene som utgjør dens kjerne. Echelon-systemet har vært

[67] Privacy International (2003)
[68] Informasjonen her er primært hentet fra EU-parlamentets Echelon-rapport fra 2001: http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_en.pdf

operativt siden den kalde krigen og var opprinnelig laget for å avlytte kommunikasjon i eller til Sovjetunionen og andre østblokkland. Eksistensen av dette systemet ble kjent i Europa etter omtale i en rapport fra EU-parlamentets eget teknologivurderingsorgan STOA (Scientific Technology Options Assessment) i 1997. Echelon ble lenge forsøkt holdt hemmelig og ikke kommentert fra noen av UKUSA-landene, så EU-parlamenetet nedsatte i 2000 en komité for å utrede spørsmålet om Echelon eksisterer, hva det eventuelt brukes til og hvordan det fungerer.

I sluttrapporten fra EU-parlamentets komité slås det fast ikke bare at systemets eksistens er udiskutabel, men også at dets hensikt er avlytting av privat og kommersiell kommunikasjon, og altså ikke militær kommunikasjon. Airbus og Thomson CSF er eksempler på selskaper som skal ha vært utsatt for industrispionasje gjennom Echelon. Spesielle satellittmottakere og spionsatellitter kombinert med bakkebaserte radiomottakere inngår angivelig i systemet, sammen med utstyr for avlytting av kabelbasert kommunikasjon. Det slås fast at systemet har kapasitet til å gjennomføre en kvasi-total overvåkning. Det innebærer at alle typer ubeskyttet elektronisk kommunikasjon kan avlyttes – det være seg telefonsamtaler, SMS-er, fakser, e-post og internett-trafikk. Kommunikasjonsmønstre kan analyseres, og innholdet i kommunikasjonen scannes for interessante nøkkelord. Meldinger som vekker systemets interesse kopieres for å kunne vurderes av en person i den aktuelle etterretnings-organisasjonen.

Mens man tidligere trodde at alliansen kunne ha tilgang til tilnærmet all internasjonal elektronisk kommunikasjon, slår EU-rapporten fast at systemets kapasitet har vært over-vurdert. Selv om det kan fange opp en betydelig andel av satellittbasert og radiobasert kommunikasjon, har de kun adgang til en begrenset del av kommunikasjon som sendes i kabler. Det er grunn til å tro at et system som Echelon vil være relativt lite effektivt i anvendelser hvor man leter gjennom all tilgjengelig kommunikasjon i håp om å avdekke planlegging av terrorhandlinger eller annen alvorlig kriminalitet. Faren med denne type systemer er at de lett kan produsere store mengder såkalt ”falskt positive” funn. Det vil si at et ord i en e-post kan trigge systemets interesse og utsette en intetanende, uskyldig bruker for interesse fra en organisasjon som amerikanske NSA (National Security Agency).

Et eksempel på dette ble berømt da historien ble fortalt i det amerikanske TV-programmet *60 Minutes*.[69] En canadisk mor opplevde å bli satt under etterforskning, etter at hun i en e-post til en venninne fortalte at sønnen hadde dummet seg ut i et skuespill på skolen. På engelsk: ”...my son *bombed* in the school play”. Et engelsk uttrykk for å dumme seg ut heter altså det samme som å bombe, og Echelon oppfattet derfor meldingen som mistenkelig. Det mest urovekkende med historien er knapt at systemet trigger på ordet bombe, men at ikke menneskelig inngripen stoppet saken før kvinnen var blitt satt under etterforskning.

Relevansen for norske borgeres personvern ligger i det at man må påregne at elektronisk kommunikasjon til utlandet, eller meldinger som på internett sendes via andre land (for eksempel ved bruk av e-postkonto hos Hotmail, Yahoo! eller Google), scannes av Echelon. Nå er det ikke kjent at noen er blitt etterforsket i Norge som følge av Echelon-scanning, så det er neppe grunn til å legge sterke bånd på sitt ordvalg i e-poster på grunn av dette. Men for de som eksempelvis har venner i Iran eller på Cuba, og ikke ønsker at NSA skal kunne lese hva man skriver, kan det være på sin plass å vurdere løsninger for kryptering av e-post. Dette vil

[69]Washington Post, 20.04.2004: *Data surveillance* http://www.washingtonpost.com/ac2/wp-dyn/A23488-2004Apr19?language=printer

ved bruk av moderne, sterke kryptoprodukter gjøre det umulig for andre enn mottakeren å se innholdet. EU-parlamentet råder i sin rapport både bedrifter og privatpersoner til å treffe tiltak for å beskytte sin kommunikasjon mot avlytting fra fremmede makters side. De mener at kryptering av kommunikasjon derfor må bli normen snarere enn unntaket i europeiske land.

Carnivore og elektronisk kommunikasjonskontroll

Carnivore (også kjent som DCS1000) er et system utviklet av det amerikanske føderale politiet, FBI, for å avlytte elektronisk kommunikasjon[70]. Systemet er en såkalt pakkesniffer som kan brukes til målrettet kommunikasjonskontroll. Det innebærer at i motsetning til Echelon, som scanner all kommunikasjon på jakt etter mønstre og nøkkelord, avlytter Carnivore all elektronisk kommunikasjon til og fra bestemte brukere som avlyttes som ledd i en etterforskning. Systemet skal også kunne loggføre alle kommunikasjonsadresser som den avlyttede utveksler meldinger med. For at systemet skal kunne operere, må egne PC-er fra FBI med Carnivore installert plasseres ut i lokalnettet hos den aktuelle internett-leverandør (ISP). Derfra kan systemet snappe opp all kommunikasjon til eller fra den kunden som er satt under kommunikasjonskontroll.

Det har vært utbredt skepsis mot et system som Carnivore på grunn av man har fryktet at det kunne invitere til misbruk og overtramp mot borgernes personvern. Nylig er det blitt kjent at Carnivore ikke har vært i bruk de siste par år.[71] Ifølge Olin Kerr har debatten rundt Carnivore lenge vært misforstått. Han sier programmet har vært spesielt utviklet for å ta tilstrekkelige hensyn til personvern, gjennom at overskuddsinformasjon filtreres ut av systemet. Kerr hevder at årsaken til at Carnivore ikke lenger er i bruk, er at kommersielle applikasjoner tok igjen Carnivore på dette området, slik at også slike systemer kunne brukes på måter som er forsvarlige med tanke på personvernet.[72]

Selv om Carnivore ikke lenger er i bruk, er det dog et faktum at norske borgere kan bli et mål for avlytting fra utenlandske myndigheter hvis de kommuniserer med noen som er satt under kommunikasjonskontroll i sitt hjemland. Ettersom kommunikasjonskontroll er en lovlig etterforskningsmetode i alvorlige saker også her til lands, er dette dessuten en type teknologi som må forventes brukt også her hjemme.

Magic Lantern

FBI har også tatt i bruk et annet verktøy som på sin side muliggjør den totale overvåkning av all aktivitet på PC-en til en person som er under etterforskning. Magic Lantern er navnet på et program av typen systemmonitor som når det er installert vil logge absolutt alle taste-trykk som foretas på PC-en. FBI kan utplassere programmet hos en mistenkt gjennom en hemmelig ransakning i vedkommendes hus, og senere hente de loggede tastetrykk på samme måte. Magic Lantern skal også tillate at tastaturloggeren oversendes elektronisk som et virus til den mistenktes PC, og senere sender informasjon om alle tastetrykk hjem til FBI. Hensikten med denne type program er primært å snappe opp passord, kryptografiske nøkler eller klartekstmeldinger som sendes kryptert over nettet.

---

[70]Center for Democracy and Technology (CDT), 06.09.2000: *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age* http://www.cdt.org/testimony/000906dempsey.shtml

[71]CNet News.com, 31.01.2005: *Carnivore redux* http://news.com.com/Carnivore+redux/2010-1071_3-5555323.html

[72]Politech: *Olin Kerr on why the FBI "retired" Carnivore* http://seclists.org/lists/politech/2005/Jan/0032.html

Dette er samme type teknologi som ligger bak Politimetodeutvalgets forslag om den nye etterforskningsmetoden de kaller *dataavlesning*. Dette er en målrettet metode som kun kan brukes mot personer som er mistenkt i sammenheng med et alvorlig kriminelt forhold. Men slik teknologi går et skritt lenger enn annen overvåkningsteknologi, i den forstand at den kan innebære overvåkning også av tankeprosesser. En tastaturlogger lagrer nemlig alle tastetrykk, også de man senere sletter fordi man bare satt og fabulerte litt på PC-en.

7.4 Elektronisk overvåkning

I offentlig debatt om personvern høres ofte uttalelser i retning av at vi i dag lever i eller er på vei mot et *overvåkningssamfunn*. Kontrolltiltak fra myndighetenes side som oppfattes å innskrenke personvernet møtes gjerne med utsagn om at *"storebror ser deg"*. Men hva ligger egentlig i disse begrepene, og i hvilken utstrekning er de treffende beskrivelser på vårt samfunn? Vi skal se litt nærmere på overvåkningsbegrepet slik det brukes i diskusjoner omkring borgernes frihet og personvern.

Mens ordbøker fortsatt ofte definerer begrepet *overvåkning* som direkte observasjon, gjerne av en mistenkt person, påpeker Marx[73] at en slik definisjon ikke lenger holder. Typisk for dagens elektroniske overvåkning er at den i mindre grad er rettet mot individer, men i større grad dekker kategorier av mennesker og geografiske områder. Slik har nye former for overvåkning mer karakter av *masseovervåkning,* hvor informasjon om menneskers aktiviteter samles inn uten at det foreligger spesiell mistanke. Marx mener at en bedre definisjon av dagens overvåkning rett og slett er bruk av tekniske hjelpemidler til å trekke ut eller sammenstille personopplysninger. Disse kan hentes fra individer, men også fra kontekster. Med kontekst menes her at informasjon kan trekkes ut ved å sette sammen data fra ulike situasjoner og kilder, og se mønstre som det ellers ikke ville være mulig å observere. Dagens overvåkning går altså mye lenger enn det som mennesker selv kan observere og rapportere.

Clarke[74] har innført begrepet *dataveillance* (data surveillance) som betegnelse på dagens IKT-baserte overvåkning. Han påpeker at forståelsen i befolkningen og blant politikere for hvordan elektronisk overvåkning fungerer og hvilken effekt den har, fortsatt er for lav. Clarke retter oppmerksomheten mot hvordan teknologien nå gjør det mulig å sammenstille personopplysninger fra ulike kilder, og effektivt utnytte dette til å se sammenhenger. Dessuten påpeker han effekten av identifikasjonssystemer som virker på tvers av ulike sammenhenger, og gjør det enklere å knytte sammen data om en person. Mens det tidligere alltid har vært dyrt å overvåke mennesker effektivt, er dette nå i høy grad automatisert og dermed langt billigere. Dette har muliggjort den utbredte masseovervåkning som i dag foregår gjennom innsamling av data om menneskers kommunikasjon og aktiviteter. Mens videoovervåkning er et tema som mange er oppmerksomme på, er folk mindre kjent med elektronisk overvåkning, ettersom den gjerne er mindre synlig. Elektronisk overvåkning er derimot mer nærgående og har langt mer alvorlige konsekvenser for den enkeltes personvern enn ren kameraovervåkning.

---

[73] Marx (2002)
[74] Roger Clarke, 2003: *Dataveillance – 15 years on* http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html

Storebror ser deg

Som antydet forbinder de fleste mennesker overvåkning med begrepet *storebror*. Bakgrunnen for dette er George Orwells berømte roman *1984*, som handler om en stat som bruker et stort byråkratisk apparat kalt *Tankepolitiet* til å overvåke sine innbyggere. Figuren *Big Brother* representerer det allmektige *Partiet,* og er den som via allestedsnærværende *teleskjermer* (toveis TV) overvåker alle innbyggernes handlinger og tanker og som griper inn ved behov. Orwells roman utkom i 1948 og er en mørk framtidsvisjon, en dystopi, som skildrer en virkelighet hvor en mektig og allvitende stat kan styre enkeltindividenes liv i minste detalj.[75]

Orwells visjon fra 1948 var svært forutseende, og har derfor bevart interessen fram til i dag. Den teknologiske utviklingen har derimot gått langt forbi de toveis TV-skjermer han forestilte seg, og Orwell kunne ikke forutsi hvor raskt overvåkningen skulle oppnå global rekkevidde. Han kunne heller ikke forestille seg at noen andre enn selve staten kunne bli dominerende innen overvåkning og inngrep i individets frihet. Overvåkning er i dag nettopp et globaliserende fenomen, og noe som dreier seg like mye om konsumenter som om borgere.

Den sentraliserte overvåkningen og den eksplisitte kontrollen over enkeltmenneskets atferd som er karakteristisk for Orwells *Big Brother* er nok mest treffende i forhold til gårsdagens overvåkningsbyråkratier, som for eksempel Ministeriet for statens sikkerhet (Stasi) i det tidligere Øst-Tyskland eller Sovjetunionens KGB. Dagens nettverks- og IKT-baserte overvåkning fungerer på måter som gjør *Storebror*-metaforen til en bare delvis treffende beskrivelse av den nye virkeligheten.

Panoptikon

Panoptikon (”altseende”) er betegnelsen på en modell for et fengsel foreslått i 1791 av den britiske filosofen Jeremy Bentham, og som senere er blitt en sentral metafor for forståelse av overvåkning. Benthams modell beskriver en halvsirkulær utforming med et observasjonspunkt i sentrum og fangeceller langs perimeteren. Modellen skulle sikre at fangene i cellene til enhver tid skulle kunne observeres av vaktene, mens et intrikat system av lys og skodder skulle sikre at vaktene ville forbli usynlige for fangene. Det ville således ikke være mulig for fangene å avgjøre hvorvidt de på et gitt tidspunkt faktisk var under observasjon eller ikke. Kontroll og disiplin skulle sikres ved å gi fangene en konstant følelse av å bli sett av usynlige øyne. Det ville ikke finnes noe sted de kunne gjemme seg for å unnslippe overvåkningen. Underkastelse ville således være fangens eneste rasjonelle valg i en slik situasjon.[76]

På 1970-tallet tok den franske filosofen Michel Foucault denne idéen til et fengsel et steg videre, og brukte den som en metafor på samfunnsnivå. Foucault mente at hvis man kunne samle full informasjon om individer, og samtidig iverksette omfattende overvåkning av dem, kunne man få mennesker til å endre sin atferd for å passe inn i aksepterte kategorier og unngå å påkalle seg overvåkernes oppmerksomhet.

Sosiologen Thomas Mathisen har med referanse til Michel Foucaults panoptikon, hvor de få overvåker de mange, lansert begrepet *synoptikon* for den type overvåkning som er skapt av nyere former for TV, hvor de mange overvåker de få. Nå i internett-alderen opplever vi

---

[75]Orwells roman kan leses online hos The Literature Network, http://www.online-literature.com/orwell/1984/

[76]Lyon (1994)

derimot ifølge Rosen[77] det man kan kalle et *omniptikon*, hvor de mange overvåker de mange, og hvor ingen vet hvem som til enhver tid overvåker eller blir overvåket.

David Lyon understreker at det er viktig å ta utgangspunkt i både den Orwellske og den panoptiske modellen for å kunne forstå dagens overvåkning, og for eventuelt å kunne finne enda bedre og mer treffende modeller. Disse to er verken de eneste eller nødvendigvis de mest treffende metaforer for forståelse av overvåkning, men ettersom de fleste studier som er gjort på området er informert av enten Orwells eller Foucaults idéer, er disse de best egnede som bakgrunn for diskusjoner omkring overvåkning.

Overvåkningens disiplinerende makt
Lyon sier sosiologien står i gjeld til Foucault for hans teorier omkring overvåkning. Foucaults tolkning av Panoptikon illustrerer ifølge Lyon på en treffende måte overvåkningens effekter.[78] Følgende er de to aspektene av overvåkningens disiplinerende makt:

- *Innsamling og akkumulering av informasjon*.
  Som i det panoptiske fengsel ble sikret gjennom å lage mapper med detaljert informasjon om hver enkelt innsatt
- *Direkte observasjon av de undergitte*.
  Som i et panoptikon ivaretas gjennom den arkitektoniske utforming, med potensial for kontinuerlig observasjon av den enkelte innsatte

Hvis det var slik at overvåkning ikke hadde annen effekt enn å gjøre det mulig å ta kriminelle, ville det ikke ha vært noe betydelig personvernproblem. Personvernets oppgave er ikke å beskytte kriminelle mot å bli stilt til ansvar for sine handlinger. Problemet er at overvåkning påvirker atferden også til den som har rent mel i posen. Det er et velkjent fenomen at de fleste mennesker oppfører seg noe annerledes når de kan observeres av andre mennesker, enn når de er helt alene. Dette har å gjøre med den enkeltes behov for å tilpasse seg det sosiale system hun lever i, med de konvensjoner som måtte gjelde omkring hva som er sosialt akseptert og ikke.

Når stadig flere livsområder omfattes av teknologi som på et eller annet vis kan overvåke den enkelte, er det en fare for at folk i større grad vil føle behov for å tilpasse sin atferd til det som anses som mainstream og ukontroversielt. Slik kan individet tape autonomi og frihet, ved at hun i mindre grad kan tillate seg å leve slik hun vil. Både bevegelsesfriheten, ytringsfriheten og friheten til å assosiere seg med andre mennesker kan oppleves som innskrenket, fordi den enkelte vil velge minste motstands vei og gjøre hva hun kan for ikke å tiltrekke seg myndighetenes uønskede oppmerksomhet eller mistanke.

Elektronisk kommunikasjon er et viktig eksempel her. Hvis det innføres ett års obligatorisk lagring av trafikk- og lokasjonsdata fra slik kommunikasjon, vil det medføre at tjenester som telefon, e-post og internett kan bli oppfattet av brukerne som overvåkede medier. Dette vil igjen kunne påvirke folks kommunikasjonsvaner, og mennesker som verdsetter sitt personvern høyt, kan føle at de bør være forsiktige med å bruke elektroniske kommunikasjonsmidler for ikke kontinuerlig å bli sett i kortene.

---

[77] Rosen (2004)
[78] Lyon (1994)

Det er ingen enkel sak å veie hensynene til samfunnssikkerhet og personvern knyttet til tiltak som kan øke overvåkningsnivået i samfunnet. Et problem her er at sikkerhet har mye høyere status i offentligheten enn personvern. Borgerrettighetsorganisasjoner i Storbritannia og USA har påpekt at en rekke tiltak som er iverksatt etter 11.september 2001 har mest symbolsk virkning i forhold til sikkerhet, men gjerne medfører reelle inngrep i personvern og individuell frihet. Statewatch har utarbeidet en oversikt over EUs antiterrortiltak som ble vedtatt etter terrorangrepet i Madrid, 11.mars 2004. Her redegjør de for tiltakenes relevans i arbeidet mot terror, samt hvilken effekt de vil ha på frihet og sivile rettigheter.[79]

Et minstekrav ved innføring av nye overvåkningstiltak må være at effekten av tiltaket er vurdert skikkelig på forhånd. Det må da vurderes både hvor godt tiltaket vil virke i forhold til sikkerhet og bekjempelse av kriminalitet, og hvilke negative konsekvenser det kan ha for den enkeltes frihet og livsutfoldelse. Tiltak som medfører en betydelig utøvelse av disiplinerende makt overfor enkeltindividet må gjennomføres kun hvis svært viktige gevinster kan hentes i forhold til sikkerheten i samfunnet.

7.5 Ivaretakelse av personvernet i kriminalitetsbekjempelse

En rådgivende komité (Technology and Privacy Advisory Committee – TAPAC) nedsatt av USAs forsvarsminister Donald Rumsfeld, leverte i mars 2004 en rapport om hvordan man kan ivareta personvernhensyn i kampen mot terrorisme[80]. Utgangspunktet for TAPACs arbeid var påpekte trusler mot personvernet fra initiativer for overvåkning av elektronisk kommunikasjon og for datautvinning (data mining). Målet for slike initiativer er å sammenstille informasjon på tvers av en rekke databaser og loggfiler med data om folks aktiviteter, transaksjoner og kommunikasjon, i håp om å identifisere potensielle terrorister. Komitéen fokuserte sitt arbeid på en setting hvor man søker å analysere personopplysninger (personally identifiable data) for å beskytte landet mot terrortrusselen. Et slikt fokus gjør komitéens arbeid relevant for mange situasjoner, og komiteens anbefalinger er verd å merke seg også for land med mindre ambisiøse planer for elektronisk overvåkning enn USA.

Komitéen påpeker at moderne informasjonsteknologi er et viktig verktøy i kampen mot terror, men at det er nødvendig og fullt mulig samtidig å beskytte personvern og fundamentale borgerrettigheter. De viser videre til at folks bekymring for landets sikkerhet gjør mange villige til helt eller delvis å oppgi slike grunnleggende borgerrettigheter og friheter. Men de antyder at det ville være ironisk om man av hensyn til forsvaret av landet skulle oppgi nettopp de friheter som gjør landet verd å forsvare.

TAPAC hevder at det er fullt mulig å bruke informasjonsteknologier i kriminalitetsbekjempelse uten å kompromittere personvernet for landets innbyggere. Løsningen ligger i klare regler og retningslinjer, supplert med opplæring og teknologiske verktøy som må utvikles som del av de teknologier som kan true personvernet. Prosessen må i følge komitéen underlegges administrativ, politisk og juridisk kontroll.

---

[79]Statewatch, 2004: *"Scoreboard" on post-Madrid counter-terrorism plans* http://www.statewatch.org/news/2004/mar/swscoreboard.pdf

[80]Department of Defence, USA (2004)

Følgende er et utvalg av de prinsipper TAPAC anbefaler:

- Utnevning av en personvernsjef (policy-level privacy officer) for den organisasjon som skal behandle personopplysninger for å prøve å finne potensielle terrorister
- Dataminimering må tilstrebes. Man bør minimere den mengden med data som aksesseres, spres og lagres i forbindelse med datautvinning.
- Data bør anonymiseres såfremt dette er mulig. Når man har funnet en person som må sjekkes nærmere, skal de aktuelle data kunne reidentifiseres etter en rettskjennelse
- Det må lages en aksesslogg (audit trail) som registrerer når data har blitt aksessert, og av hvem. Loggen må være motstandsdyktig mot manipulasjon og sletting.
- Systemer for datautvinning må sikres mot uautorisert aksess, og tilgangsstyring må implementeres slik at kun de med et legitimt behov kan få tilgang
- Opplæring i aktuelle lover og retningslinjer må gis til alle som er involvert i utvikling og bruk av systemer for datautvinning

Det bør utvikles en intern kultur i organisasjonen med økt bevissthet og sensitivitet for personvernhensyn.

Kapittel 8 Teknologistøtte for personvernet

Som vi har sett i foregående kapittel kan ny IKT på mange måter medvirke til å utsette personvernet for belastninger. Kort oppsummert har dette hovedsakelig å gjøre med hvordan teknologien gjør det enklere og billigere å samle inn, lagre, behandle og spre informasjon, hvordan den setter elektroniske spor fra stadig flere av folks daglige aktiviteter, og hvordan den kan være vanskelig å sikre mot aktører som på en utilbørlig måte forsøker å få tilgang til informasjon de ikke har rettmessig behov for.

Informasjonsteknologi kan på den annen side også settes direkte inn som et verktøy til støtte for personvernet. Slik teknologistøtte kan primært hjelpe innenfor følgende tre områder:

- Reduksjon i mengden av identifiserbare elektroniske spor
- Sikring av kommunikasjon ved bruk av kryptering
- Sikring av informasjonssystemer og PC-er mot innbrudd og uautorisert tilgang

Det er instruktivt å skille mellom personvern-*økende* teknologier, som i sin natur bidrar til å sikre personvernhensyn, og personvern-*vennlige* teknologier som lar brukeren selv ta valg som påvirker eget personvern, men som ikke nødvendigvis gir et positivt resultat for personvernet.

8.1 Personvernøkende teknologier

Teknologier som bidrar direkte til ivaretakelse av personvernhensyn kan kalles personvern-økende teknologier, internasjonalt kjent som ”privacy enhancing technologies” (PETs). Vi vil i denne rapporten anta en relativt bred forståelse av dette begrepet, og slik inkludere teknologi som direkte virker på alle de tre ovennevnte områder (sporreduksjon, innholds-sikring og IKT-sikkerhet). Dette innebærer at denne teknologikategorien overlapper sterkt med teknologier for IKT-sikkerhet, men dette er ikke unaturlig gitt at nettopp IKT-sikkerhet utgjør et sentralt element i sikring av personvernet.

8.1.1 Anonymiseringsteknologi

Anonymiteten har allerede i dag relativt trange kår i elektronisk kommunikasjon. Anonym mobiltelefoni er det som nevnt slutt på, og på internett gjør IP-adresser og oppkoblings-logger hos ISP-er (internettleverandører) at den fulle anonymiteten er svært vanskelig å oppnå. Med unntak av hackere og andre som er spesielt kompetente på hvordan man kan skjule sine spor, er det i de fleste tilfeller teknisk mulig å spore opp hvilke PC-er eller terminaler som har vært involvert i et kommunikasjonsforløp, selv om de involverte har gått inn for å være anonyme.

Det finnes derimot tjenester også for vanlige brukere som gjør det mulig å være mer anonym på nettet. Den klassiske og mest prominente personvernøkende teknologi er løsninger som muliggjør anonym elektronisk kommunikasjon. Dette er teknologi som skjuler knytningen mellom brukeren og sporene hun setter, og slik kan hindre uønsket identifikasjon. Slik framstår brukeren som anonym, og det vil være svært vanskelig eller umulig å spore opp hvem som står bak kommunikasjonen. Slik teknologi gjør det mulig å

sende e-post uten at mottakeren eller e-postleverandøren kan vite hvem som er avsenderen, og den gjør det mulig å surfe på internett uten at det settes spor som kan føres tilbake til brukeren.

Det skal her ikke redegjøres i detalj for hvordan denne typen tjenester kan fungere, men slike tjenester vil normalt innebære at en eller flere tredjeparter tjener som filter mellom brukeren og de tjenester hun vil bruke[81]. Anonymitet oppnås typisk gjennom mellomliggende tjenester knyttet til såkalte proxy-servere som formidler kommunikasjonen mellom brukeren og tjenester på nettet, og slik skjuler brukerens identitet for omverdenen. Dette innebærer at leverandøren av anonymiseringstjenesten kan finne ut av hvem brukeren er, så brukeren må kunne stole på leverandøren for at anonymiteten skal være sikret. Det tilbys også tjenester hvor kommunikasjonen passerer gjennom en rekke slike proxy-servere, og hvor det da er tilstrekkelig at én av dem er til å stole på for å sikre anonymitet.

Løsninger for anonym elektronisk betaling (ofte kalt e-cash) hører også til i denne kategorien. Dette er løsninger som lar brukeren betale for varer og tjenester på nettet uten å måtte oppgi personopplysninger som navn og fakturaadresse eller kredittkortnummer til butikken, og som slik hindrer at informasjon om hva man bruker pengene sine til kan komme på avveie.

Merk at vi med anonymitet i denne sammenheng snakker om det vi kan kalle sterk anonymitet, som sikter mot å gjøre det tilnærmet umulig å knytte elektroniske spor til brukerens identitet. I dagligtale er det vanlig å oppfatte anonymitetsbegrepet som mye bredere, slik at det dekker flere situasjoner hvor man ikke åpenlyst avslører sin identitet overfor andre. Dette kommenteres her under neste punkt om pseudonymisering.

Hvordan man kan oppnå anonymitet i elektronisk kommunikasjon er et komplekst problemområde som er gjenstand for betydelig forskning.[82]

8.1.2 Pseudonymisering

Det vi kan kalle ekte pseudonymiseringstjenester bygger på anonymiseringsteknologi. Men en slik tjeneste vil knytte en form for virtuell identitet til en bruker, og til denne identiteten vil det kunne knyttes et sett av egenskaper, eller konvertible autorisasjoner (credentials). En tiltrodd tredjepart må stå som garantist for de aktuelle autorisasjonene.

Et eksempel for å illustrere dette kan være systemer for nettbasert stemming ved valg. Siden anonymitet i valg er et essensielt element i vårt demokrati, må et slikt system sikre at en stemme ikke kan føres tilbake til en bestemt person. Derfor må løsningen baseres på fullstendig anonymitet. Samtidig må et slikt system sikre at kun de som har stemmerett får stemme, og at de kun stemmer én gang. For å få til dette må den tiltrodde tredjeparten utstyre brukeren med et digitalt sertifikat, som garanterer at brukeren har stemmerett og som gjør at valgsystemet vil vite når den aktuelle velgeren har stemt. La det i denne sammenheng være nevnt at nettbaserte valg fortsatt ikke er kommet forbi utprøvings-

[81]Eksempler på denne type tjeneste er: Amerikanske Anonymizer – http://www.anonymizer.com Tyske AN.ON (Anonymität Online) - http://www.datenschutzzentrum.de/projekte/anon/
[82]For en samling av artikler om elektronisk anonymitet, se http://freehaven.net/anonbib/

stadiet, og at det så langt ser ut til at mangelfull sikkerhet i internettets infrastruktur gjør det vanskelig å garantere den nødvendige sikkerheten i nettbaserte valg.

Pseudonymiseringstjenester gir brukeren større kontroll over i hvilken grad hun ønsker å være identifiserbar i de ulike sammenhengene hun opptrer. For eksempel kan hun være helt anonym når hun kjøper et nedlastbart produkt på nettet ved hjelp av elektroniske penger, samtidig som hun kan avsløre kun det som er nødvendig om seg selv for å få tilgang til ulike nettbaserte tjenester. Man kan også snakke om pseudonym kommunikasjon som ikke baserer seg på anonymiseringsteknologi, og som således ikke kan gi noen fullgod sikkerhet mot uønsket identifikasjon av brukeren. Da er det snakk om tjenester hvor man opptrer under et brukernavn, slik at det er vanskelig for andre å finne ut hvem brukeren egentlig er. Hvis man har dynamisk IP-adresse (oppringt forbindelse) og streng policy for aksept av informasjonskapsler (cookies) på egen PC, kan dette gi en akseptabel beskyttelse mot identifisering for de fleste nettbrukere. Dette er derimot ikke å betrakte som en personvern-økende teknologi, ettersom det fortsatt vil være mulig ved hjelp av IP-adressen å finne identiteten til en bruker.

8.1.3 Kryptografi

Kryptografi handler om forvrengning av innhold slik at det blir uleselig for uvedkommende. Metoden har vært i bruk siden Julius Cæsars tid for vel 2000 år siden, og oppsto som følge av behovet for å beskytte skrevne meldinger som måtte kommuniseres over avstand. Krypterte meldinger har siden spilt en stor rolle, spesielt i krigføring hvor det er avgjørende at fienden ikke på forhånd kan vite hva man planlegger å gjøre, samtidig som nødvendige ordre må kommuniseres ut til troppene. Et faktum som er kjent for mange er betydningen av at de allierte under andre verdenskrig knekket nøkkelen til tyskernes krypteringsmaskin ENIGMA, og etter dette kunne oppfange og dechiffrere viktige meldinger til tyske soldater. For eksempel medførte innsyn i en melding fra Hitler til en av hans generaler at de allierte kunne uskadeliggjøre en stor del av de tyske troppene i Normandie i 1944 (Johnsen, 2001).

I dag er kryptografi et helt sentralt teknologiområde knyttet til sikring av informasjon og kommunikasjon. Det er vanlig å betrakte dette mer som en sikkerhetsteknologi enn som en personvernøkende teknologi, men dens anvendelse er sentral også i forhold til vern av personopplysninger. Teknologien anvendes både for å sikre innhold mot avlytting under kommunikasjon over nettet, og for å sikre lagret informasjon mot innsyn. Kryptografi brukes både til å hindre innsyn i innhold, til å verifisere hvem avsenderen av en melding er, til å beskytte mot at innhold kan endres uten at dette blir oppdaget, samt til å sikre at avsender ikke kan benekte en transaksjon hun faktisk har foretatt. Et viktig bruksområde for kryptografi i dag er i implementering av digitale signaturer som brukes for å garantere at avsenderen av en melding er den han gir seg ut for å være. Sikker identifikasjon av brukere på nettet er altså også kryptografiens domene.

Siden enhver bruk av elektroniske kommunikasjonsnett i utgangspunktet er sårbar for avlytting, manipulasjon eller innsyn fra utenforstående, er det i mange tilfeller helt avgjørende at kommunikasjon enten skjer over krypterte forbindelser, eller at innholdet som sendes over åpne forbindelser selv er kryptert. Nettbanker, nettbutikker og andre som driver seriøs elektronisk handel baserer seg i svært stor grad på krypterte forbindelser. Ukrypterte forbindelser ville i slike tilfeller invitere kriminelle til misbruk av kredittkortnumre eller andre typer av personopplysninger.

Av personvernhensyn er det svært viktig at sensitive opplysninger lagres og sendes i kryptert form. Dette er nødvendig for å sikre at informasjonen ikke kommer på avveie. Mange utenforstående har adgang til å se på meldinger som sendes på e-post eller til å aksessere dokumenter som ligger lagret rundt omkring på ulike servere. Sikkerheten mot innsyn i en ukryptert e-postmelding er som illustrasjon å sammenligne med et postkort i offline-verdenen. Innholdet er helt ubeskyttet mot innsyn fra de som måtte komme i kontakt med meldingen. Kryptering kan på sin side sammenlignes med å legge innholdet i en tilnærmet ubrytelig konvolutt. Ved bruk av moderne og sterk kryptering vil en melding i overskuelig fremtid være sikret mot åpning uten tilgang til mottakerens nøkkel.

Kryptering brukes i dag i relativt stor utstrekning i større bedrifter og organisasjoner som behandler sensitive opplysninger. Det er likevel grunn til å tro at det er en klar underbruk av kryptering på flere områder, for eksempel blant mindre bedrifter som kan være utsatt for industrispionasje. Et grelt eksempel er mangelen på kryptering av politiradioer og den medfølgende avlytting som foregår. Både politiet og de andre nødetatene er nå blitt pålagt å sikre sine samband mot avlytting.

Blant private brukere kommer kryptering til anvendelse primært i forbindelse med tjenester på internett som automatisk sørger for kryptert kommunikasjon. Kryptering av e-post mellom private brukere er lite utbredt, blant annet på grunn av lav bevissthet omkring muligheten, samt behovet for en smule arbeidsinnsats knyttet til å implementere det. Inntil det kommer løsninger som er enklere å forholde seg til for brukerne, er det lite trolig at kryptering av privat e-post vil bli særlig utbredt.

Applikasjonen PGP (Pretty Good Privacy)[83] er den mest utbredte løsningen for kryptering av e-post for private brukere. Selv om denne har oppnådd en viss popularitet, er det en svært liten andel av vanlige brukere som er villige til å yte den nødvendige innsatsen for å kunne sikre sin e-post ved hjelp av dette programmet. For å sende kryptert med PGP må begge parter i en kommunikasjon ha installert PGP, og de må ha utvekslet sine offentlige krypteringsnøkler.

En ny løsning fra sveitsiske Ciphire Labs kan representere et gjennombrudd med hensyn til enkel bruk av kryptoløsninger for privat e-post. Applikasjonen *Ciphire E-post* tilbyr transparent e-postkryptering for vanlige brukere. Den fungerer sammen med alle e-postklienter og krypterer automatisk post til mottakere som også har Ciphire E-post, mens meldingene sendes ukryptert til mottakere som ikke har denne applikasjonen. I motsetning til PGP vil krever ikke dette programmet at brukeren selv bruker tid på vedlikehold av nøkler og sertifikater, ei heller at de må vite hvem som kan motta krypterte meldinger. Hvis slike løsninger for kryptering og signering av e-post blir utbredt, kan de bidra til å bedre tilliten til e-post og redusere problemene knyttet til spam og svindel.

Kryptering av innhold på private harddisker er så langt heller ikke særlig utbredt, men kan nok forventes å øke noe i utbredelse ettersom dette blir enklere i nye operativsystemer. Apples MacOS X operativsystem leveres for eksempel nå med enkel tilgang til et kryptert område på harddisken for oppbevaring av sensitive dokumenter. Om noen da skulle stjele harddisken, vil tyven ikke kunne lese det krypterte innholdet uten kjennskap til riktig passord (krypteringsnøkkel) for å dekryptere innholdet.

---

[83] http://www.pgpi.org/

8.1.4 Informasjonssikkerhet

Informasjonssikkerhet handler i denne sammenhengen primært om å sikre at data som lagres, for eksempel i et informasjonssystem eller på en PC, bevarer sin integritet og fortrolighet. Det innebærer at dataene er sikret mot manipulasjon og uautoriserte endringer, samt at ingen andre enn de som er autorisert for det kan skaffe seg tilgang til dataene. Det skal med en gang påpekes at det ikke er noen enkel oppgave å etablere fullgod sikring av data, så det vil alltid bestå en viss risiko for kompromittering, selv med omfattende sikringstiltak på plass. Hvor høyt sikkerhetsnivå som behøves henger sammen med graden av sensitivitet i de dataene som skal beskyttes. For eksempel opererer Forsvaret et datanett som er godkjent for informasjon gradert "Hemmelig" og hvor nivået på sikkerheten følgelig er svært høyt, mens for eksempel Teknologirådet som kun lager rapporter for offentligheten kan legge seg på et lavere sikringsnivå. Mer typiske eksempler er bedrifter eller offentlige etater som har informasjonssystemer med data om kundene eller innbyggerne. Disse må ha et nivå på sikkerheten som gir god beskyttelse både mot innsyn fra nysgjerrige ansatte, samt mot lekkasjer til eksterne aktører.

Informasjonssikkerhet kan sies å bestå av to separate aspekter: for det første det tekniske aspektet som har å gjøre med utformingen av informasjonssystemer og teknologiske sikringsmekanismer. Dernest det organisatoriske aspektet som har å gjøre med sikkerhetspolicy samt retningslinjer for hvordan brukerne skal anvende systemene, og hvilken informasjon de er autorisert til å se på. Svikt i informasjonssikkerheten innenfor et av disse aspektene vil medføre at personopplysninger kan komme på avveie. God sikkerhet krever en klar sikkerhetspolicy og god oppfølging av både tekniske og organisatoriske sikringstiltak.

Interne trusler

God sikring av informasjonssystemer mot datainnbrudd og skadeverk er en forutsetning for sikring av konfidensialiteten til de data en organisasjon oppbevarer. Derfor er beskyttelse av data mot for eksempel virus, datainnbrudd og hacking viktig også for personvernet. Vi skal i denne rapporten likevel ikke gå inn på hvordan ulike teknologier for IKT-sikkerhet kan anvendes for å sikre systemer mot eksterne trusler. Dette er et stort og komplisert felt som ikke passer inn i denne rapportens omfang. Vi skal derimot fokusere på beskyttelse mot interne trusler. Det vil si egne ansatte som gjerne er litt nysgjerrige eller litt uforsiktige, og som ofte lett kan få tilgang til sensitive data som de strengt tatt ikke har behov for å se på. Det er gjerne på innsiden av organisasjoner at vi finner de største problemene knyttet til personvern i informasjonssystemer.

Man kan spørre seg hvorfor dette er et så stort problem. Egne ansatte burde vel kunne forholde seg til retningslinjer om hva de skal se på og hva de ikke skal se på? Kan det være nødvendig å bruke teknologiske løsninger for å hindre egne ansatte i å kikke på sensitive data? To eksempler fra aktører som håndterer sensitiv informasjon kan illustrere at dette er nødvendig. Det første er fra helsevesenet, og gjelder sykehusansattes innsyn i informasjon om de som er innlagt. Som det kom fram under Teknologirådets høring om IKT & personvern i desember 2003, er det et utbredt fenomen på sykehusene at når det blir kjent at en kjendis er innlagt, kan man registrere stor trafikk av nysgjerrig helsepersonell på vedkommendes elektroniske pasientjournal. Dette skjer på tross av retningslinjer om at man ikke skal se på sensitiv pasientinformasjon, med mindre man har et profesjonelt behov for det. Overgangen til elektroniske pasientjournaler bidrar til å gjøre det enklere å snoke i journaler ettersom de blir lettere tilgjengelige. Samtidig er det enklere å avsløre snoking, ettersom slike informasjonssystemer normalt vil logge hvem som er inne og kikker på hvilken informasjon.

Det andre eksempelet gjelder politiregistre som inneholder sensitiv informasjon om personer som av en eller annen grunn er i politiets søkelys. Etter mordet på Sveriges utenriksminister Anna Lindth, skal en rekke personer i politi og helsevesenet ha vært inne og søkt i registre og journaler på navnet til den nå drapsdømte Mihailovic. En svensk politikvinne ble i mars 2004 dømt for datainnbrudd og bøtelagt etter at hun hadde søkt på Mihailovics navn i interne registre, til tross for at hun ikke jobbet med etterforskningen. Svensk politi etterforsket i 2004 hele 130 andre personer for tilsvarende misbruk av sin stilling.[84]

Begge disse eksemplene på uautorisert tilgang til sensitiv informasjon skjer på tross av retningslinjer som sier at man ikke skal se på slik informasjon uten et tjenstlig behov. Dette gjelder selv om informasjonssystemet ikke hindrer tilgang til informasjonen. Mye tyder på at menneskets nysgjerrige natur ofte gjør det vanskelig å unnlate å se på informasjon, selv om det ikke finnes et tjenstlig behov. Mange vil også mene at det ikke er så farlig å sniktitte på sensitiv informasjon, så lenge systemet ikke fysisk blokkerer tilgangen. I tillegg til organisatoriske tiltak for å bedre etterlevelsen av retningslinjer omkring sikkerhet og personvern, er det mulig å bruke teknologi også for å avhjelpe dette problemet.

Det IBM-utviklede programmeringsspråket EPAL (Enterprise Privacy Authorization Language) er utviklet nettopp for å styre tilgang til personopplysninger i informasjonssystemer. Se mer om dette i kapittel 8.2.1.

8.2 Personvernvennlige teknologier

Med begrepet personvernvennlige teknologier, forstår vi teknologier som lar brukere av informasjonssystemer selv ta valg omkring behandling av personopplysninger. Slike teknologier har potensial til å støtte vernet av personopplysninger, men kun hvis brukerne tar bevisste valg for å oppnå nettopp dette.

8.2.1 Personvern i informasjonssystemer

I dagens informasjonssystemer er det vanlig med en relativt grovkornet behandling av tilgangsrettigheter, hvor alle som har behov for tilgang til en eller annen form for informasjon i et system gjerne gis tilgang til hele systemet, eller i hvert fall til mye mer enn akkurat den informasjonen vedkommende trenger. Det kan være flere grunner til dette, men en viktig grunn er at de som har utviklet informasjonssystemer ofte ikke har vært særlig bevisste på personvernmessige konsekvenser, og heller ikke har fått spesifikke krav om å bygge personvernmekanismer inn i systemene. Som tidligere nevnt er det et betydelig problem at nysgjerrige ansatte snoker i sensitive data som de ikke har et reelt tjenstlig behov for å aksessere.

Det er mulig å bygge regler for vern av personopplysninger inn i informasjonssystemer for slik å sikre en bedre sammenheng mellom brukeres faktiske behov for tilgang til informasjon, og hvilke konkrete dataelementer de faktisk gis tilgang til. Ved implementering av en mer finmasket styring av tilgangsrettigheter til dataelementer i et informasjonssystem på basis av et need-to-know prinsipp, vil risikoen for lekkasje av personopplysninger

[84] Computerworld, 31.03.2004: *Politi dømt for datainnbrudd*
http://www.computerworld.no/index.cfm?fuseaction=artikkel&id=A008CCA3-05AA-4500-9863E4F1DFAEF8D0

gjennom nysgjerrige interne ansatte synke betraktelig. Slik innbygging av personvernregler må ta utgangspunkt både i lovgivning, og en intern policy for hvem som trenger tilgang til hvilken informasjon og under hvilke forutsetninger. Systemet må så implementere dette på en slik måte at tilgang til et dataelement kun gis til brukere med et berettiget behov for å se den konkrete informasjonen.

Vi skal nevne to ulike teknologier for å bygge personvernstøtte inn i informasjonssystemer. *Platform for Privacy Preferences (P3P)* er å betrakte som en "front-end" teknologi, hvor brukere av web-tjenester selv kan spesifisere krav til utvekslingen av data mellom egen PC og de nettsteder som besøkes. *Enterprise Privacy Authorization Language (EPAL),* er på sin side å betrakte som en "back-end" teknologi som brukes til å implementere regler for håndtering av personopplysninger basert på bedriftens egne retningslinjer eller policies.

Platform for Privacy Preferences (P3P)
P3P er en standard utviklet av standardiseringsorganet World Wide Web Consortium (W3C), med det mål å gi brukere en enkel måte å oppnå bedre kontroll med innsamling og bruk av personopplysninger på steder de besøker på internett. Et nettsted som støtter P3P vil presentere detaljene i sin personvernpolicy på maskinlesbar form til brukerens nettleser. Såfremt nettleseren støtter P3P, vil denne så sammenligne nettstedets policy for håndtering av personopplysninger med brukerens egne preferanser, og respondere i forhold til dette. Microsofts Internet Explorer er en av nettleserne som har en viss støtte for P3P, primært knyttet til styring av hvilke former for cookies brukeren ønsker å akseptere.

I sin enkleste form er P3P et sett av avkrysningsspørsmål som sammen gir et bilde av hvordan et nettsted behandler personopplysninger. Formålet er å gi brukerne større kontroll, gjennom at nettsteders personvernpolicy gjøres lettere tilgjengelig i en form brukeren kan forstå, og som lar henne gjøre valg på bakgrunn av informasjon om nettstedets praksis. For eksempel skal det være lett å se om et nettsted vil kunne videreselge de opplysninger man gir dem, og på bakgrunn av dette kunne velge å avslå å oppgi personopplysninger. Det er et håp at brukernes tillit til transaksjoner på internett skal forbedres som følge av at forståelig informasjon om nettsteders personvernpraksis gjøres lett tilgjengelig for dem, samtidig som de selv kan velge hvordan de vil forholde seg på bakgrunn av denne informasjonen.

Ni ulike aspekter knyttet til behandlingen av personopplysninger dekkes av P3P[85]. Fem temaer gir informasjon om hvilke opplysninger nettstedet samler inn:

- Hvem samler inn opplysningene?
- Nøyaktig hvilke opplysninger blir samlet inn?
- Til hvilke formål blir opplysningene samlet inn?
- Hvilke opplysninger blir delt med andre?
- Hvem er eventuelt mottakere av opplysningene?

De resterende fire temaene forklarer nettstedets interne policies for behandling av person-opplysninger:

[85]W3C, 2003: *P3P 1.0: A new standard in online privacy* http://www.w3c.org/P3P/brochure.html

- Kan brukerne selv endre hvordan deres opplysninger blir brukt?
- Hvordan løses uoverensstemmelser?
- Hvilke retningslinjer gjelder for lagring av opplysninger?
- Hvor kan de detaljerte retningslinjene finnes i en form brukeren kan lese?

P3P-protokollen setter ingen minstestandard for vern av personopplysninger. Ei heller har den noen mulighet til å sjekke at et nettsted faktisk følger de retningslinjer som de hevder å følge. Bruken av P3P i dagens form gir følgelig ingen garanti for at nettsteder ivaretar brukernes personvern. Likevel er protokollen nyttig også i dag, primært i forhold til å styre håndteringen av informasjonskapsler (cookies) på brukerens PC.

Enterprise Privacy Authorization Language (EPAL)
EPAL er et XML-basert formalisert språk utviklet av IBM for å støtte vernet av personopplysninger i informasjonssystemer. Det kan komme til anvendelse både ved håndtering av personrelaterte data innad i en bedrift, og ved utveksling av slike data mellom bedrifter. EPAL muliggjør en finmasket kontroll med behandlingen av ulike dataelementer.

Forenklet sagt fungerer dette slik at hver enkelt personopplysning som en bedrift samler inn, tilføyes informasjon om hvordan opplysningen kan behandles. Til hver enkelt personopplysning vil det da følge med en spesifikasjon av hvem som kan behandle opplysningen og til hvilke formål den kan behandles. Denne EPAL-spesifikke personverninformasjonen tjener kun til å avgjøre hvem som har rett til å behandle hvilke datakategorier, til hvilke formål og på hvilken måte. Dette skal fungere uavhengig av hvilke datamodeller de aktuelle informasjonssystemene benytter, og også uavhengig av brukerens generelle tilgangsrettigheter til IT-systemet.

EPAL definerer et sett av opplysningskategorier, brukerkategorier, behandlingsformål, behandlingskategorier, forpliktelser og betingelser. Ut i fra disse lages regler som på bakgrunn av dato, bruker og behandlingsformål enten tillater eller nekter en konkret behandling av personopplysninger. Kategoriseringen av ulike dataelementer fastsettes individuelt på bakgrunn av selskapets retningslinjer for vern av personopplysninger, samt den lovgivning man er underlagt ved behandling av slike opplysninger.[86]

Formålet med EPAL er å muliggjøre personvernstyring på tvers av ulike applikasjoner, avdelingsgrenser og selskaper, uten dermed å forhindre en desentralisert struktur for lagring og annen håndtering av personrelaterte data. De personvernregler som lages ved hjelp av EPAL skal være maskinlesbare, slik at de kan implementeres automatisk av informasjonssystemer. For eksempel kan sletting av personopplysninger utføres automatisk av systemet ved den dato som er definert som en opplysnings slettetidspunkt.

IBM overleverte i november 2003 spesifikasjonene for EPAL til standardiseringsorganisasjonen W3C (World Wide Web Consortium), under royaltyfrie lisensbetingelser for mulig implementasjon som åpen standard.[87] Hvis EPAL blir en slik W3C-standard, kan språket tas i bruk av ulike softwareselskaper for utnyttelse i informasjonssystemer hvor det

[86]Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *FAQ EPAL* http://www.datenschutzzentrum.de/faq/epal.htm
[87]http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

ønskes effektiv behandling av personopplysninger, samtidig som hensyn til vern av personopplysninger må ivaretas.

8.2.2 Teknologistøttet identitetshåndtering

Systemer for å støtte sluttbrukeres håndtering av identiteter er et svært omfattende og lovende område, som så langt har vært gjenstand for relativt begrenset analyse og utvikling. Oppgaven med å administrere og kontrollere identiteter vil sannsynligvis bli et område som vil kreve teknologistøtte. Et system for identitetshåndtering (identity management system – IMS) vil kunne spille en sentral rolle for å støtte brukernes håndtering av identiteter. Et holistisk verktøy for å støtte alle sider av identitetshåndtering på en personvernvennlig måte er derimot foreløpig intet mer enn en visjon.[88]

Begrepet IMS benyttes i dag noe misvisende om relativt enkle applikasjoner som primært støtter funksjonalitet som single sign-on (hvor én pålogging gir tilgang til et sett av tjenester) og tilgangsstyring til IT-ressurser. Fullt utviklede applikasjoner og systemer for personvernvennlig identitetshåndtering forventes av eksperter å være en salgbar realitet en gang rundt år 2012 – 2014, men viktige deler av slike systemer er allerede i dag en realitet.

Et slikt framtidig holistisk IMS vil blant annet kunne støtte retten til informasjonsmessig selvbestemmelse, og hjelpe brukerne med å velge hvordan de skal presentere seg i ulike sammenhenger. Alle mennesker gjør slike valg intuitivt når man omgås andre. Man presenterer seg på ulike måter, og framstår i ulike roller for ulike kommunikasjonspartnere. Dette gjenspeiler de ulike roller som mennesker inntar i sitt dagligliv, det være seg som arbeidstaker, foreningsmedlem, kunde, skattebetaler, venn, familiemedlem, kjæreste, kontaktsøkende og så videre. Hva man vil fortelle til andre om seg selv varierer alt etter hvilken rolle man befinner seg i.

Den hverdagslige sjongleringen med hvordan man ønsker å fremstå overfor ulike mennesker i den fysiske verden, er ikke direkte overførbar til den virtuelle verden. En viktig forskjell har å gjøre med den mengde av elektroniske spor som brukere ubevisst etterlater seg ved bruk av elektroniske medier. Online er det mulig å samle data fra ulike bruksområder, forbinde dem med hverandre ved hjelp av eventuelle felles identifikatorer (for eksempel IP-adresse eller en unik identifikator som personnummer), og sette dem sammen i omfattende personprofiler. Ved å skaffe seg tilgang til en slik profil kan andre så få vite ting om deg som du ikke ville ønske å fortelle til vedkommende.

Felles for offline- og online-verden er en utbredt mangel på autentisitet i hverdagen. Man vet ofte ikke hvem man har med å gjøre. Det er ikke vanlig å be om legitimasjon når man vil snakke med en person man ikke kjenner. På internett må man i tillegg klare seg uten den umiddelbare ansikt-til-ansikt kontakten som ellers kan være informativ. I mange tilfeller vil det således være mye lettere på nettet å utgi seg for å være en annen enn den man faktisk er. Skal man kunne handle med noen eller utføre andre typer transaksjoner på nettet, må det således finnes andre mekanismer for å sikre den nødvendige tillit til andre aktører.

I mange situasjoner vil for eksempel tjenesteleverandører eller andre aktører innen elektronisk handel ønske at brukerne opptrer under sitt virkelige navn, selv om dette ikke

[88] Beskrivelsen er basert på Köhntopp (2000) samt på Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein og Studio Notarile Genghini (2003)

strengt tatt er nødvendig. Ofte spiller det liten rolle for en leverandør hvem kunden eller brukeren er, men det kan være nødvendig å vite noe sikkert om vedkommende for å kunne avgjøre hvilken tilgang brukeren skal ha til de aktuelle tjenester.

Et framtidig personvernvennlig system for identitetshåndtering kan hjelpe ved å la brukeren selv bestemme når hun skal opptre under sitt egentlige navn, når hun skal opptre under et ansvarlig pseudonym, og når hun vil være mest mulig anonym. Det vil også hjelpe til med å avgjøre hvilken informasjon hun skal dele med de ulike aktørene hun kommuniserer med. Dessuten kan et slikt system tilby funksjonalitet for å garantere visse attributter knyttet til pseudonymer. Det vil si at kryptografiske teknikker kan anvendes for å bevise at visse egenskaper er knyttet til en identitet. Hvis for eksempel Drammen kommune tilbyr en nettbasert tjeneste for ungdom under 16 år som er bosatt i kommunen, er det ikke nødvendig å identifisere brukere som logger seg på tjenesten ved navn for å autorisere tilgang til tjenesten. Ved i stedet å kreve at brukere kan presentere et digitalt sertifikat som garanterer at brukeren er under 16 år og bosatt i Drammen kommune, er dette nok for å vite at brukeren har rettmessig tilgang til tjenesten.

Oppsummert kan følgende betraktes som sentrale behov og drivere for identitetshåndtering støttet av et IMS:

- Enkelhet og brukervennlighet knyttet til håndtering av ulike identiteter, brukernavn og adresser
- Autentisering og tilgangsstyring til tjenester med tilpasset nivå av identifikasjon
- Rollehåndtering for lettere å kunne skille ulike sfærer som arbeidsliv og privatliv
- Tilgjengelighetsstyring for bestemmelse av hvem som skal kunne kontakte en til hvilke tidspunkt
- Retten til informasjonsmessig selvbestemmelse gjennom valg av balanse mellom anonymitet og autentisitet samt implementering av brukerens personvernpreferanser

Følgende er en oversikt over det som oppfattes som relevante krav til personvernvennlige applikasjoner og systemer for identitetshåndtering, slik man ser for seg at disse vil kunne være om noen år.[89]

- *Funksjonalitet*
  Et system for identitetshåndtering (IMS) må primært hjelpe brukeren med identitetsadministrasjon, det vil si støtte håndtering og presentasjon av delidentiteter. Brukeren må gjøres oppmerksom på kontekst og situasjon for å foreta informerte valg om hvilke opplysninger hun ønsker å gi fra seg til ulike aktører. Et IMS må også fungere som en portvakt som all digital kommunikasjon fra brukeren går gjennom.
- *Brukervennlighet*
  Et IMS må enkelt kunne brukes uten kjennskap til hvordan systemet egentlig fungerer. Brukergrensesnittet må være brukervennlig og effektivt, slik at brukeren raskt kan se en relevant tolkning av aktuell kontekst, og på bakgrunn av denne velge

[89]Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein og Studio Notarile Genghini (2003)

riktig identitet. Det må samtidig ikke kreve stor innsats eller mye tid av den enkelte bruker.

- *Sikkerhet*
  Det er avgjørende at et IMS er svært robust mot angrep på dets tilgjengelighet, integritet eller konfidensialitet. Siden et slikt system vil inneholde betydelig informasjon om den brukeren det representerer, er det særlig viktig at sikkerhetsnivået er høyt. Ulike data kan være underlagt ulike sikkerhetsnivåer avhengig av deres sensitivitet. Tilgang til data i systemet må beskyttes mot uautoriserte brukere ved bruk av autentisering.
- *Personvernregler*
  Et IMS må støtte overholdelsen av lover og forskrifter om vern av personopplysninger. Det kan også designes i henhold til prinsipper for personvernøkende teknologier med støtte for transparens (bevissthet om hvilke data som utveksles), dataminimering (ved anonymisering eller pseudonymisering), systemintegrasjon (personvernregler bygd inn i informasjonssystemet), god informasjonssikkerhet og hjelp til selvhjelp for brukerne, slik at disse selv kan ta ansvar for å beskytte sine personopplysninger.

Teknologistøttet identitetshåndtering har blitt et viktig tema i EUs forskningsprogrammer. Prosjektet RAPID (Roadmap for Advanced Research in Privacy and Identity Management) leverte sin sluttrapport i 2003.[90] Gjennom EUs sjette rammeprogram for forskning og utvikling finansierer prosjektet PRIME (Privacy and Identity Management for Europe) som startet i 2004 og strekker seg over fire år.[91] Nettverket FIDIS (Future of Identity in the Information Society) er også finansiert gjennom sjette rammeprogram.[92]

[90]http://europa.eu.int/information_society/activities/egovernment_research/doc/rapid_roadmap.doc
[91]http://www.prime-project.eu.org/
[92]http://www.fidis.net/

Kapittel 9 Utfordringer og anbefalinger

Økt bruk av digitale teknologier som internett og mobiltelefoni, fører til at vanlige mennesker i sine hverdagslige aktiviteter uvegerlig etterlater seg stadig tettere stier av elektroniske spor. Det faktum at de nye teknologiene kan gi så detaljert informasjon om personer gjør dem egnet til overvåkning gjennom innsamling og lagring av data om menneskers gjøren og laden. Overvåkningspotensialet blir med andre ord mye større etter hvert som elektroniske teknologier blir mer sofistikerte.

Etter hvert som de teknologiske mulighetene blir større, blir samfunnet mer avhengig av effektive juridiske og moralske sperrer mot å utnytte alle mulighetene til å invadere eller kontrollere andre mennesker. I tillegg er det avgjørende at teknologien kommer til anvendelse på en måte som bidrar til å ivareta personvernet, ved å beskytte mot unødig innsamling og uautorisert spredning av personopplysninger. Det er et problem at informasjonsteknologi ofte kommer til anvendelse på måter som ikke tar tilstrekkelig hensyn til personvern.

9.1 Sentrale utfordringer for personvernet

Personvernet må sies å stå rimelig sterkt både juridisk og politisk i Norge som i store deler av Europa forøvrig. Dette er et godt utgangspunkt for å sikre personvernet også i framtida. Likevel er det flere utviklingstrekk som gir grunn til en viss bekymring for personvernets stilling både i dag og i årene som kommer. Felles for disse er at de er internasjonale i sin natur og ikke spesielle for Norge. Likefullt består et betydelig nasjonalt handlingsrom hvor politiske valg vil påvirke utviklingen for personvernet. Viktige utfordringer er knyttet til hvordan nye informasjons- og kommunikasjonsteknologier kommer til anvendelse, samt til kunnskap og holdninger hos brukere av IKT-tjenester.

Brukerrelaterte utfordringer
Innsamling og bearbeiding av personidentifiserbar informasjon blir mer automatisert og mindre synlig, og således også vanskeligere for folk å kontrollere eller ta forholdsregler mot.

Økt utbredelse av grasrotteknologier som mobiltelefoni og internett legger større ansvar på brukerne selv for å beskytte egne personopplysninger. Ingen andre kan ta dette ansvaret for dem.

Lavt kunnskapsnivå hos brukerne omkring elektroniske spor og om hvordan det er mulig å beskytte seg mot unødig identifikasjon, gjør at mange ikke tar de nødvendige forholdsregler for å sikre sine personopplysninger.

Ungdom ser ut til å være spesielt lite bevisst på personvernproblematikk og svært villige til å eksponere personlig informasjon om seg selv og andre, for eksempel på internett. Med kamera på mobiltelefonen kreves respekt for andres personvern, noe som ser ut til å mangle hos en del.

Svært mange ser ut til å være villige til å ofre personvernhensyn i bytte for en følelse av økt trygghet. Dette medfører en fare for innskrenkninger i vernet av privatsfæren, også i tilfeller hvor dette har kun symbolsk virkning for trygghetsnivået i samfunnet. Riktignok må

personvernhensyn veies mot hensynet til den kollektive trygghet i samfunnet, men personvernet kan ikke forsakes til fordel for en illusorisk følelse av økt sikkerhet.

Brukernes tillit til nye informasjons- og kommunikasjonsteknologier er ingen selvfølge. Om de skulle medføre omfattende og alvorlige negative konsekvenser for brukeres sikkerhet eller personvern, kan brukerne bli skremt fra å bruke dem.

Teknologirelaterte utfordringer
Sterk økning i bruken av teknologier som logger mange og til dels innholdsrike elektroniske spor, medfører at det rundt omkring finnes lagret mye mer personidentifiserbare data om folks kommunikasjon, transaksjoner og bevegelser enn tidligere.

Økningen i spormengde er ikke fulgt av en tilsvarende forbedret sikring av elektroniske data mot misbruk eller uautorisert innsyn. Teknologi for å samle inn og lagre data ligger langt foran teknologien for å beskytte data mot uønsket bruk.

Teknologiens overvåkningspotensial har økt betydelig de senere år. Mens man tidligere kunne trøste seg med at det ville være svært ressurskrevende å overvåke innbyggernes dagligliv i detalj, er det i mindre grad slik nå. Teknologien er i dag tilstrekkelig avansert til å muliggjøre utstrakt automatisert overvåkning og kontroll.

Teknologier som samler inn elektroniske spor gjør ofte dette på måter som er usynlige for brukerne. Ettersom brukerne derfor ikke legger merke til datainnsamlingen, finner de seg i mer av den enn de ville om mer synlige metoder var i bruk.

Til tross for store forhåpninger er det et faktum at personvernøkende teknologier så langt har hatt begrenset suksess. Teknologien gjør fremskritt, men det er liten grunn til å tro at personvernteknologier vil løse personvernets utfordringer, i alle fall på kort sikt.

Utfordringer knyttet til samfunnssikkerhet
Økt bruk av elektroniske nettverk til planlegging, koordinasjon eller gjennomføring av kriminelle handlinger, aktualiserer behovet for å kunne spore hvem som gjør hva på nettet.

Terrortrusselen møtes med tiltak for overvåkning av elektroniske kommunikasjonsnett med sikte på å kunne forebygge nye terrorhandlinger og etterforske gjennomførte aksjoner. Tiltakene er i enkelte tilfeller ikke rettet spesielt mot terrormistenkte, men har karakter av masseovervåkning hvor informasjon samles inn om alle brukerne.

Det er en sterk tendens til at data som er samlet inn i andre sammenhenger ønskes brukt til kriminalitetsbekjempende formål. Den gode hensikt gjør at lagrede data som regel tillates brukt i en slik sammenheng. Det er derimot grunn til å være på vakt mot for mye bruk av personopplysninger til sekundære formål, spesielt når disse kan være i strid med det opprinnelige formålet.

Utfordringer knyttet til handel og offentlig forvaltning
Aktører i elektronisk handel er gjerne de mest aggressive i jakten på personopplysninger om konsumentene. De bygger personprofiler som de kan bruke for å tilby tilpassede tjenester eller reklame skreddersydd til kundens interesser. Dette medfører at et stort antall aktører har en ”mappe” med detaljert informasjon om enkeltpersoner.

Den offentlige forvaltning ønsker på sin side god informasjon om borgerne for å tilby effektive, behovstilpassede tjenester, samt for å hindre misbruk av det offentliges midler. Ved overgang til en mer digital forvaltning må man unngå at personprofiler for hver enkelt borger lett kan sammenstilles på tvers av statlige etater. Ingen må enkelt kunne skaffe seg en helhetlig oversikt over en borgers alle forhold til staten.

Den generelt lave bevisstheten omkring personvern i befolkningen må antas å innebære at også medarbeidere i bedrifter og statlige etater som behandler personopplysninger, i utgangspunktet har en lav bevissthet omkring viktigheten av sikker håndtering av personopplysninger. Mye tyder på at organisatoriske tiltak for bedre informasjonssikkerhet og vern av personopplysninger er underprioritert, selv i organisasjoner som håndterer sensitive personopplysninger. Sykehus og legekontorer er eksempler på slike. Dette er lite betryggende i en situasjon hvor medarbeidere hos stadig flere aktører forvalter en økende mengde data om kundene og borgerne.

Generelle utfordringer
Personvernet er på vikende front som en følge av utviklingen innen IKT, samfunnssikkerhet, elektronisk handel og brukeratferd. Det er generelt svært vanskelig å reversere en utvikling hvor personvernet svekkes. Man bør med andre ord være forsiktig med å svekke dette vernet, ettersom man ikke kan regne med å kunne gjenopprette ubalansen.

Det er en utfordring at det i mange sammenhenger skapes overskuddsinformasjon, det vil si informasjon som er unødvendig i den aktuelle konteksten. Spesielt ille er dette når brukere identifiseres i tilfeller hvor dette er helt unødvendig. Spesielt innen elektronisk handel har mange aktører en tendens til å avkreve brukerne identifiserende informasjon kun fordi de ønsker data til sine brukerprofiler.

Spørsmål knyttet til personvern på arbeidsplassen er en stor utfordring. De fleste ønsker en uovervåket sfære også på arbeidsplassen, og forventer å kunne sende en privat e-post eller betale en regning i nettbanken uten at noen skal se dem i kortene. Retten til en privatsfære på jobb er derimot noe uklar, og sterkt begrenset av arbeidsgivers styringsrett. Det største problemet knyttet til personvern på arbeidsplassen er gjerne at bedriften ikke har gitt klare retningslinjer for privat kommunikasjon og overvåkning på arbeidsplassen, slik at den enkelte er usikker på hva som oppfattes som akseptabelt.

Personvernet har et imageproblem. Mange oppfatter at personvernet er en slags luksus man kan unne seg så lenge viktigere ting ikke står på spill. Stilt opp mot hensyn som sikkerhet og effektivitet, er det få som prioriterer personvernet. Det er en fare for at dette kan medføre ubalanserte hensynsavveininger hvor personvernet lider unødig.

9.2 Anbefalinger

I et prosjekt som redegjør for sammenhenger mellom IKT og personvern er det ikke enkelt å gi konkrete anbefalinger til tiltak. Hovedgrunnen til dette er at utfordringene personvernet står overfor ikke kan løses ved et sett av konkrete tiltak. Personvernet må stadig veies mot andre viktige hensyn, og det er ikke mulig å gå opp grensene mellom de ulike hensynene en gang for alle.

For at personvernet skal overleve den kontinuerlige strømmen av nye informasjons- og kommunikasjonsteknologier, må myndigheter og beslutningstakere vite hvordan man kan

vurdere konsekvensene av nye teknologier. Det avgjørende er å fokusere på hvilke valg som kan gjøres når teknologiene skal implementeres i systemer og tas i bruk. Når nye teknologier lover fordeler som automatisering, økt effektivitet eller enkelhet for brukere, må disse hensynene veies mot hensynet til den enkeltes personvern.

Følgende teknologiområder vil være sentrale for hvordan IKT nå og i framtida vil påvirke personvernet:

- Identifikasjons- og autentiseringsteknologier
- Trådløse kommunikasjonsteknologier
- Lokasjonsteknologier (posisjonering)
- Internett-relaterte teknologier
- Datautvinning (data mining) og søketeknologi
- Sensorteknologier
- Informasjonssikkerhet
- Personvernteknologier

9.2.1 Konsekvensvurderinger ved innføring av ny teknologi

Det som er typisk for IKT-området er at de fleste teknologiene ikke i seg selv er verken skadelige eller gunstige for personvernet, men at dette bestemmes av hvordan systemene designes og implementeres. Når man skal gjøre en overordnet, første vurdering omkring personvernkonsekvenser av en ny teknologi på IKT-området, er det hensiktsmessig å stille spørsmål som disse:

- Hvilke elektroniske spor i form av bruksdata vil teknologien produsere?
- Vil bruksdata bli loggført og lagret? Hvor lenge blir de eventuelt lagret?
- I hvilken grad vil teknologien identifisere brukerne? Kan man bruke teknologien uten å identifisere seg, eller vil brukerens identitet bli verifisert entydig?
- Hvordan vil den lagrede informasjonen bli brukt, og hvem vil få tilgang til den?
- Hva er faren for at dataenes eksistens vil lede til krav om at de må kunne brukes også til andre formål enn de som de ble samlet inn for?
- Hvor godt er brukerrelaterte data sikret mot utilsiktet spredning eller uautorisert innsyn gjennom datainnbrudd utenfra?
- Hva blir konsekvensene når sikkerheten svikter og data kommer på avveie? Er det gjennomført risikoanalyser for slike tilfeller?
- Hvis dataene er sensitive – er det implementert tekniske og organisatoriske tiltak for å sikre at informasjonen kun kan ses av brukere med et reelt tjenstlig behov?
- Finnes systemer for å avdekke misbruk og rutiner for oppfølging og sanksjoner mot interne snokere?
- Hva er individets forventning til hvor privat den situasjon hvor teknologien vil bli brukt er? Er teknologien i samsvar med disse forventningene?

- Er datainnsamlingen synlig og kjent for brukerne, slik at disse kan gjøre et informert valg om hvorvidt de ønsker å bruke den aktuelle teknologien?

9.2.2 Personvernprinsipper for elektroniske spor

Følgende prinsipper er spesielt sentrale for bevaring av personvernet i det elektroniske spors tidsalder. Jo flere sporsettende teknologier vi omgir oss med i hverdagen, jo viktigere er det at disse prinsippene følges.

- *Formålstilpasset nivå på personidentifikasjon*
  Når spormengden er blitt stor, er det avgjørende at det ikke er lett å knytte alle sporene til en spesifikk person annet enn i situasjoner hvor dette er strengt nødvendig. Unødig sterk identifikasjon er både et personvernproblem, fordi brukernes aktiviteter for lett kan etterspores, og et sikkerhetsproblem fordi identifiserbare data kan utnyttes av kriminelle. Spesielt viktig er det å unngå bruk av globalt unike identifikatorer (som for eksempel fødselsnummer) i informasjonssystemer, ettersom slike gjør det mulig å sammenstille sporene fra ulike kilder til helhetlige oversikter over den enkeltes aktiviteter.
- *God informasjonssikkerhet og behovsbasert tilgangsstyring*
  Alle identifiserbare elektroniske spor som registreres og lagres i informasjonssystemer må beskyttes, både mot eksterne sikkerhetstrusler og mot interne snokere. For å sikre konfidensialiteten til sensitive personopplysninger er tradisjonelle sikringstiltak som grovkornet aksesskontroll ofte ikke godt nok. Personvernhensyn bør bygges inn i slike systemer gjennom finsiktet tilgangsstyring til dataelementer, slik at kun autorisert personell med et konkret behov kan se de aktuelle dataene.
- *Restriktiv holdning til sekundærbruk ("mission creep")*
  Når det samles inn store mengder data om menneskers aktiviteter, er det i mange tilfeller fristende å bruke slike data til helt andre formål enn de ble samlet inn for. Her må man alltid veie ulike hensyn mot hver andre, men det er viktig å passe seg for "de gode hensikters tyranni" hvor konsekvensene for personvernet i sum kan bli for store til å rettferdiggjøre slik "mission creep".

9.2.3 Anbefalte tiltaksområder

Vi har i dette kapitlet pekt på noen sentrale utfordringer for personvernet i dag og i tiden som kommer. På bakgrunn av disse gir Teknologirådet følgende anbefalinger til tiltaksområder for om mulig å styrke situasjonen for personvernet.

Kunnskap og bevissthet hos IKT-brukere
Bevisstheten og kunnskapsnivået om elektroniske spor og personvern bør styrkes. Folk må hjelpes til selv å kunne ta ansvar for sitt personvern på de områder hvor dette er nødvendig.

Et offentlig tilsyn må uansett effektivt ivareta innbyggernes grunnleggende personvernbehov. Enkelte brukere må beskyttes mot seg selv. Brukere som verdsetter sin frihet og private sfære må ikke kunne tvinges av mindre bevisste brukere til å eksponere noe de oppfatter som privat.

Informasjonsetikk i skolen
Ungdom har svake kunnskaper om, og er lite bevisste på problemstillinger knyttet til personopplysninger og personvern. Uetisk eller ubetenksom spredning av person-

opplysninger er utbredt blant barn og unge. Uthenging av andre ved sladder på SMS, spredning av MMS-bilder, samt publisering av personrelatert informasjon på internett (for eksempel festbilder) er eksempler på dette.

Det er således et behov for å få personvern og informasjonsetikk inn som et tema i grunnskolen. En løsning kan for eksempel være at Utdannings- og Forskningsdepartementet integrerer disse temaene i sitt *Program for digital kompetanse* som løper fram til 2008. Utdanningsdirektoratet har allerede fått utarbeidet en lærepakke[93] om personvern for ungdomstrinnet. Denne er et godt utgangspunkt og det er nå viktig å motivere lærere til å ta pakken i bruk.

Identifikasjon og autentisering
Ved innføring av sterke metoder for autentisering som for eksempel digitale signaturer eller biometri, må man minimere bruken av personopplysninger. Autentisering på individnivå bør unngås såfremt dette ikke er strengt nødvendig.

Pseudonyme løsninger med bruk av virtuelle identiteter bør stimuleres som alternativ til full anonymitet og full identifikasjon. Løsninger for digital signatur må tilby pseudonyme sertifikater i tilfeller hvor dette er tilstrekkelig.

Anonyme tjenester må fortsatt tilbys i sammenhenger hvor det ikke er nødvendig å kunne holde brukerne ansvarlig. Autentiseringsløsninger basert på anonyme attributter bør være tilgjengelige i de sammenhenger hvor dette er hensiktsmessig, og hvor det ikke er nødvendig å kunne holde brukeren ansvarlig. For eksempel må det fortsatt være mulig å betale med anonyme penger på nettet, lese nettaviser og ytre seg offentlig uten å vise digital legitimasjon.

Gjennomsiktighet
I en situasjon hvor et økende antall aktører lagrer stadig mer elektronisk informasjon om hver enkelt borger, blir det vanskeligere å sikre informasjon mot spredning. Dette øker viktigheten av at borgerne kan kontrollere hvilke opplysninger som er lagret om dem, og hvordan både statlige og private datainnsamlere håndterer innsamlede personopplysninger.

En mer reell innsynsrett ville som nevnt under anbefalingen om internkontroll kunne spille en rolle her. Det er likevel grunn til å utrede nærmere om andre og mer effektive tiltak kan implementeres for å gjøre datasystemer mer gjennomsiktige for brukerne. Slik kan man sikre brukernes tillit til at myndigheter og selskaper ikke kan misbruke innsamlede personopplysninger uten risiko for å bli oppdaget.

Føre var-prinsipp på personvernområdet
Privatsfærens kår blir trangere ettersom elektroniske hjelpemidler brer seg inn på stadig flere livsområder. Siden reduksjoner i privatsfæren sjelden lar seg reversere, bør et føre var-prinsipp gjelde i forhold til innskrenkninger av personvernet.

Det må utvises forsiktighet ved innføring av nye teknologier som kan identifisere brukere. Konsekvenser for personvernet må utredes ved innføring av nye teknologier av denne type.

---

[93] http://www2.skolenettet.no/personvern/

Personvern i informasjonssystemer
Ved innføring av ny teknologi, eller nye IKT-baserte metoder som håndterer nærgående eller sensitive personopplysninger, må det stilles krav om at systemer må implementeres på måter som ivaretar sentrale personvernhensyn.

Personvernøkende mekanismer må brukes i større utstrekning i slike systemer, og de som ikke gjør bruk av slik teknologi må kunne begrunne hvorfor dette ikke er mulig eller hensiktsmessig. At systemer er enklere å implementere uten slike mekanismer kan ikke alltid være god nok grunn til å la det være.

Internkontroll
Mye tyder på at mange aktører som behandler personopplysninger ikke godt nok overholder kravene i personopplysningsloven med forskrift. Kravet om et system for internkontroll som dokumenterer hvordan lovens krav oppfylles, bør følges sterkere opp.

Innsynsretten fungerer for eksempel for dårlig hos en rekke aktører som behandler personopplysninger. Gitt at Datatilsynet ikke har kapasitet til å gjennomføre jevnlige kontroller hos alle som behandler personopplysninger, må større vekt legges på internkontroll og på etterprøving av at slike systemer finnes og er i bruk.

Så lenge teknologiske løsninger ikke kan garantere for datasikkerheten, må den menneskelige faktor utnyttes. Organisasjoner som behandler personopplysninger må derfor implementere organisatoriske tiltak for å sikre at medarbeidernes atferd er i henhold til retningslinjene for ivaretakelse av informasjonssikkerhet og personvern.

Sikkerhet på hjemme-PC
Det er et problem at sikkerhetsnivået på privatpersoners PC-er og trådløse nettverk er så lavt at det bidrar til å kompromittere private data og utsette brukere for personlig sikkerhets-risiko. Grove personvernbrudd knyttet til bruk av egen PC kan alvorlig skade brukernes tillit til digitale tjenester generelt.

Bredbåndstilknytning og trådløse nettverk er de primære problemproduktene i denne sammenheng. Siden sikker konfigurasjon av slikt utstyr kan være vanskelig for vanlige brukere, må det her stilles krav til bransjen. Bredbåndsoperatører må informere om behovet for brannmur på enhver bredbåndslinje, mens forhandlere av trådløse nettverk på sin side alltid må levere med en brukervennlig og enkel skriftlig veiledning for sikring av slike nett. Kryptering av signalene i lokalnettet samt installasjon av personlig brannmur på PC-en står sentralt her.

Referanseliste

Bogdanowicz, Marc og Beslay, Laurent, IPTS – 2001
Cyber-security and the future of identity, IPTS report vol 57
Institute for Prospective Technological Studies (IPTS), DG Joint Research Centre, EU Commission
http://www.jrc.es/pages/iptsreport/vol57/english/ICT4E576.htm

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag – TAB (2002)
Biometrische Identifikationssysteme. Sachstandsbericht.
http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf

Bygrave, Lee A. - 2002:
Data protection law. Approaching its rationale, logic and limits.
Kluwer Law International

Department of Defence, USA – 2003
Safeguarding Privacy in the Fight Against Terrorism
Report of the Technology and Privacy Advisory Committee
http://www.cdt.org/security/usapatriot/20040300tapac.pdf

Electronic Privacy Information Center (EPIC) – 2004:
Privacy and Human Rights 2004.
http://www.privacyinternational.org/survey/phr2004/

Giddens, Anthony – 1991:
Modernity and self-identity. Self and society in the late modern age
Polity Press

Institute for Prospective Technological Studies (IPTS) – 2003
Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview.
IPTS, DG Joint Research Centre, EU-kommisjonen
http://cybersecurity.jrc.es/docs/LIBE%20STUDY/LIBEstudy%20eur20823%20.pdf

IT-Sikkerhedsrådet – 2002
Privatliv på internet. Praktiske råd.
IT-Sikkerhedsrådet, Ministeriet for Videnskap, Teknologi og Udvikling, Danmark
http://www.videnskabsministeriet.dk/fsk/publ/2002/privatliv/PrivatlivpaaInt.pdf

Johnsen, Ben – 2001:
Kryptografi. Den hemmelige skriften.
Tapir Akademisk Forlag

Kent, Stephen T. og Millett, Lynette I. (red) – 2003:
Who goes there? Authentication through the lens of privacy.
Committee on Authentication Technologies and Their Privacy Implications,
National Research Council of the National Academy of Sciences, USA
http://books.nap.edu/html/whogoes/

Köhntopp, Marit – 2000:
Identitätsmanagement
http://www.koehntopp.de/marit/publikationen/idmanage/

Lyon, David – 1994:
From Big Brother to Electronic Panoptikon
Hentet fra D. Lyon: *The Electronic Eye: The Rise of the Surveillance Society*
University of Minnesota Press, 1994

Marx, Gary T. – 2002:
What's new about the "new surveillance" ?
Surveillance & Society, Vol 1 Issue 1, September 2002
http://www.surveillance-and-society.org/articles1/whatsnew.pdf

Pauer-Studer, Herlinde – 2003:
Privatheit: Ein ambivalenter, aber unverzichtbarer Wert
I Peissl (2003)

Peissl, Walter (red.) – 2003:
Privacy: Ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte.
Verlag der Österreichischen Akademie der Wissenschaften

Politiregisterutvalget – 2003:
NOU 2003 : 21 - Kriminalitetsbekjempelse og personvern
http://odin.dep.no/filarkiv/207785/NOU0303021-TS.pdf

Politimetodeutvalget – 2004:
NOU 2004 : 6 – Mellom effektivitet og personvern
http://odin.dep.no/filarkiv/207750/NOU0404006-TS.pdf

Privacy International – 2003
Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights
Utarbeidet av Covington & Burling for Privacy International, UK
http://www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf

Rosen, Jeffrey – 2004
The naked crowd. Reclaiming Security and Freedom in an Anxious Age.
Random House

Schartum, Dag Wiese og Bygrave, Lee A. - 2004:
Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.
Fagbokforlaget

Teknologirådet - 2004:
Holdninger til personvern. Rapport fra fokusgrupper om elektroniske spor og personvern.
http://www.teknologiradet.no/files/rapport_fokusgrupper_copy.pdf

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein og Studio Notarile Genghini – 2003:
Identity Management Systems (IMS): Identification and comparison study
http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf

Wiik Johansen, Michal; Kaspersen, Knut-Brede; Skullerud, Åste Marie Bergseng – 2001:
Personopplysningsloven. Kommentarutgave.
Universitetsforlaget

Vedlegg 1 – Teknologirådets 12 råd til nettbrukere

Ta ansvar for å beskytte dine personopplysninger
Vær forsiktig med å oppgi personopplysninger som navn, adresse, arbeidssted, telefonnummer eller lignende til tjenesteleverandører på Internett. Med mindre du er sikker på at dine opplysninger vil bli behandlet på en betryggende måte, bør du unngå å oppgi personopplysninger. Internett er en global arena, og ikke alle man besøker kan forventes å følge norsk personvernlovgivning. Det er ingen andre til å passe på deg der ute, så du må selv sørge for å beskytte deg gjennom å begrense mengden av informasjon du legger igjen om deg selv.

Vær selektiv med identifikasjon på Internett
Vær forsiktig med å oppgi identifiserende informasjon til fremmede mennesker eller ukjente firmaer på nettet. Det er god praksis å opptre under pseudonym (brukernavn) på Internett og kun oppgi riktig navn, adresse og andre personopplysninger til aktører man vet er til å stole på. Selv om mange tjenester ber om å få vite hvem du er, betyr ikke det at du må fortelle dem det. Det er ingen lov mot å oppgi pseudonyme opplysninger og dette er fullt legitimt i mange sammenhenger. Lag navn som er innlysende fiktive (som Dolly Duck fra Andeby), og bruk under ingen omstendighet noen andres identitet. Har du behov for å surfe helt anonymt slik at ingen kan finne ut hvem du er, er det mulig å bruke spesielle anonymiseringstjenester. Hvis du skal kjøpe noe, bruke nettbank, levere selvangivelsen eller foreta andre transaksjoner er det derimot selvfølgelig nødvendig å oppgi korrekt identitet.

Beskytt deg mot informasjonskapsler (cookies)
Informasjonskapsler er små datafiler som et nettsted lagrer på din PC med informasjon om din bruk av dette nettstedet. Personopplysninger som navn, adresse og kredittkortnummer, samt hvilke sider man har besøkt på det aktuelle nettstedet, lagres gjerne her. Tredjeparts informasjonskapsler kan utplasseres av en aktør som har en bannerannonse på det besøkte nettstedet. Slike kan benyttes til å sette sammen clickstream-data i en profil som beskriver detaljer fra din websurfing. Nyere utgaver av nettlesere lar brukeren enkelt justere nivået for personvernbeskyttelse, og slik bestemme vilkårene for aksept eller avvisning av informasjonskapsler. I Internet Explorer finnes innstillingen under Verktøy / Alternativer for Internett / Personvern. Det er god praksis å velge middels eller høyere beskyttelse. Informasjonskapsler kan også slettes slik at et websted mister historikken på deg.

Vær bevisst nettleserens internettlogg og midlertidige filer
Nettleseren lagrer historikk over din websurfing i en internettlogg. Denne gjør det lettere å gjenfinne adresser du har besøkt tidligere, blant annet ved at besøkte adresser kommer automatisk opp i adressefeltet når du begynner å skrive en adresse. Samtidig vil andre brukere på samme PC kunne se hvor du har vært på Internett. Midlertidige filer (cache) lagres for å gjøre surfingen raskere, men slettes ikke nødvendigvis når man lukker nettleseren. Trenger man å beskytte sine surfespor mot andre nysgjerrige brukere på PC-en, kan både logg, midlertidige filer og informasjonskapsler slettes. I Internet Explorer gjøres dette under Verktøy / Alternativer for Internett / Generelt.

Vær kritisk til tilbud om gratisytelser mot personopplysninger
Mange tjenesteleverandører av ulike slag tilbyr å gi deg noe gratis mot at du oppgir personlig informasjon. Spør deg selv hvorfor leverandøren er villig til å gi deg noe for å få

informasjon om deg. Kan det tenkes at du blir lurt eller at informasjonen om deg vil bli solgt videre? Er du usikker på leverandørens seriøsitet bør du avstå fra å oppgi identifiserbar informasjon.

Vær spesielt forsiktig på usikrede områder på Internett
Unngå å oppgi sensitiv informasjon som for eksempel kredittkortnummer over usikrede forbindelser. Sikre webområder oppretter en kryptert forbindelse med din PC som sørger for at innholdet er beskyttet mot innsyn fra uvedkommende under transporten mellom deg og tjenesteleverandøren. Sjekk at forbindelsen er kryptert ved å se at adresse-feltet starter med "https://", altså har en ekstra s sammenlignet med det vanlige "http://". Nettleseren vil også vise et symbol i form av en låst hengelås for å markere en kryptert forbindelse.

Husk at e-post ikke er beskyttet mot innsyn
Under normale omstendigheter sendes e-post ukryptert. Det vil si at informasjonen ikke er skjult for uvedkommende, og vil være sårbar for avlytting eller innsyn knyttet til mellomlagring på ulike servere under transport, samt på serverne hos e-postleverandørene til henholdsvis sender og mottaker. Vær derfor forsiktig med å sende svært sensitiv informasjon på e-post. Det er mulig også for privatbrukere å sende e-post sikkert gjennom å bruke et krypteringsprogram (som for eksempel PGP – Pretty Good Privacy). Mottakeren må i slike tilfeller også ha dette programmet installert. Hvis kryptering ikke er aktuelt, vurder om du kanskje heller skulle sende den sensitive informasjonen i lukket konvolutt med tradisjonell post i stedet.

Les personvernløfte før du oppgir identifiserende personopplysninger
Alle seriøse tjenester på Internett som ber om personopplysninger fra brukeren skal offentliggjøre et personvernløfte (privacy policy), som beskriver hva de vil bruke dine opplysninger til. Hvis denne ikke er betryggende (for eksempel hvis de vil videreselge dine opplysninger) bør du være svært forsiktig med hva du oppgir av opplysninger.

Invester i nødvendig sikring av egen hjemme-PC
Sikkerhetsrelaterte trusler på Internett er en alvorlig utfordring også for personvernet. Svikt i forhold til sikkerhet kan bidra til at privat informasjon kommer på avveie. Alle PC-er bør ha installert et antivirusprogram som automatisk oppdateres over nettet. PC-er som er tilkoblet nettet via ADSL eller annen "alltid på"-bredbåndsteknologi bør også ha installert en brannmur enten i form av software eller i form av hardware, da gjerne integrert med en ruter. Uten slik beskyttelse gjør man PC-en sårbar for innbrudd fra hackere eller kriminelle som kan gjennomsøke harddisken etter kredittkortnumre eller annen sensitiv informasjon, og sågar overta kontrollen over maskinen for å bruke den til egne formål (som for eksempel et tjenestenektangrep).

Bruk en ekstra e-postadresse på Internett
Det er god praksis både for å beskytte sitt personvern og for å beskytte seg mot reklamepost å holde sin foretrukne e-postadresse innenfor begrensede grupper og folk man kjenner. Ved bruk av chattetjenester er bruk av anonymt brukernavn en selvfølge, men også ved deltakelse i åpne diskusjonsfora, e-postlister eller andre åpne steder på Internett er det viktig å beskytte e-postadressen sin. Svar aldri på spam, ikke engang for å reservere deg mot slik post, ettersom det bare resulterer i enda mer spam i innboksen.

Beskytt deg mot spionprogrammer
Hvis du er av dem som laster ned mange gratisprogrammer fra Internett, er du sårbar for spionprogramvare som av og til kan følge med på lasset med slike nedlastninger, primært

fra mindre seriøse leverandører. Slik programvare kan overvåke dine aktiviteter på PC-en, snappe opp passord og sende informasjonen om deg tilbake til den som laget spion-programmet. Egne programmer er laget for å beskytte mot slike spionprogrammer - et eksempel er Ad-aware fra Lavasoft (www.lavasoft.de).

Ikke vær overdrevent paranoid

Tross alle gode råd om beskyttelse vil vi gjerne understreke at ved relativt enkle forholds-regler er Internett et sted du trygt kan være uten å kompromittere ditt personvern.

Vedlegg 2 – Åpen høring om personvern

Teknologirådet arrangerte 1. desember 2003 en høring om IKT og personvern. Statlige tilsyn, interesseorganisasjoner, forskere og næringsliv ble invitert til å presentere sine syn.

Inviterte høringsparter
Teknologirådet ba om innspill omkring statusen for personvernet i dag, om strategier for å sikre personvernet ved bruk av lovgivning og teknologi samt om hvorvidt den digitale forvaltning vil stille spesielle krav til personvernet. Resultatet ble interessante innspill til Teknologirådets ekspertgruppe.

I tillegg til disse generelle spørsmålene adresserer innspillene andre problemstillinger som for eksempel hvordan teknologi kan bidra til å sikre personvernet, hvordan markedsføring og e-handel kan true personvernet samt om tilsynsfunksjonen for personvernet.

Teknologirådet mottok høringsinnlegg fra følgende organisasjoner:

- Abelia
- Elektronisk Forpost Norge
- Forbrukerombudet
- IBM
- Hans Rustad, journalist i Mandag Morgen
- Norsk Regnesentral
- NTNU - Q2S
- Steria
- Tele2
- Thales
- Universitetet i Oslo, Avdeling for forvaltningsinformatikk
- Statens vegvesen

Innleggene kan leses på Teknologirådets nettsider: http://www.teknologiradet.no