Holdninger til personvern

Rapport fra fokusgrupper om elektroniske spor og personvern

Rapport 1, februar 2004

Holdninger til personvern

Rapport fra fokusgrupper om elektroniske spor og personvern

Utgitt: Oslo, februar, 2004
ISBN: 82-92447-00-8
Opplag: 300
Omslag: Enzo Finger Design AS
Layout: Teknologirådet
Trykk: Allkopi

Elektronisk publisert på: www.teknologiradet.no

INNHOLDSFORTEGNELSE Side

Om Teknologirådet

Teknologirådet er et uavhengig organ som skal vurdere den teknologiske utviklingen på alle samfunnsområder.

Rådet skal følge den teknologiske utviklingen og stimulere til debatt om de muligheter og konsekvenser som ny teknologi skaper for samfunnet og det enkelte individ. Teknologirådet skal formidle resultatet av sitt arbeid til Stortinget, øvrige myndigheter og samfunnet generelt.

Teknologirådet
Prinsensgate 18
Postboks 522 Sentrum
0105 Oslo
Tel: 23 31 83 00
Fax: 23 31 83 01
E-mail: post@teknolgirådet.no
Hjemmeside: www.teknologiradet.no

Forord

Denne rapporten beskriver innsikter fra en fokusgruppeundersøkelse i regi av Teknologirådet. Som del av prosjektet IKT og personvern har vi snakket med 48 vanlige brukere av informasjons- og kommunikasjonsteknologier (IKT) som mobiltelefon og internett. Vi var spesielt interesserte i brukernes tanker omkring elektroniske spor og personvern.

Teknologirådet skal ifølge sitt mandat legge vekt på metoder som involverer lekfolksskjønnet direkte i vurderingene. Vi mener dette kan bidra til en bedre og mer helhetlig teknologivurdering og søker derfor å inkludere andre enn eksperter i de vurderinger som gjøres.

Prosjektet IKT og personvern startet senhøstes 2002 og avsluttes ved utgangen av februar 2004. Prosjektets øvrige arbeid er basert på en gruppe av eksperter på ulike fagområder som kryptografi, elektronikk, informasjonssikkerhet, jus og antropologi. Ekspertgruppen gjør sine egne vurderinger omkring situasjonen for personvernet i lys av dagens IKT, men har også bidratt i kvalitetssikringen av fokusgruppeundersøkelsen og av denne rapporten. Sluttrapporten fra arbeidet i prosjektets ekspertgruppe vil foreligge i begynnelsen av mars 2004 og skal gi en bred situasjonsbeskrivelse for personvernet i lys av ny IKT.

Arbeidet med denne fokusgruppeundersøkelsen ble gjennomført av Teknologirådets prosjektleder Erlend Jakobsen og prosjektmedarbeider Vibeke Almaas. Analysen av datamaterialet og den skriftlige framstilling i denne rapporten er utført av Vibeke Almaas.

Tore Tennøe

Sekretariatsleder

Sammendrag

Med bakgrunn i de senere års kraftige økning i bruken av informasjons- og kommunikasjonsteknologier (IKT) som for eksempel mobiltelefon og Internett, har Teknologirådet som en del av prosjektet *IKT & personvern* gjennomført fokusgrupper for å få et inntrykk av hvordan lekfolk (ikke-eksperter) ser på personvernkonsekvenser knyttet til bruk av slik teknologi. I undersøkelsen har 48 personer fordelt på seks fokusgrupper deltatt i diskusjoner om dette tema.

Deltakerne til fokusgruppene kom fra Oslo og Bodø. Fire grupper bestod av ungdom mellom 17 og 19 år og to grupper var med voksne i alderen 30-40 år. Gruppene var også delt inn etter kjønn. Temaer som ble diskutert var brukervaner knyttet til mobiltelefoni, lokasjonsbaserte tjenester, e-post, internett og e-handel. Holdninger til personvern samt bevissthet omkring elektroniske spor og deres konsekvenser var andre temaer som ble tatt opp i gruppene. Det ble også diskutert avveininger omkring hensynet til personvern i forhold til hensyn som brukervennlighet og kriminalitetsbekjempelse.

Under samtalene kom det fram at flere av deltakerne hadde relativ lite kjennskap til at elektronisk kommunikasjon setter elektroniske spor. De fleste deltakerne var ikke klar over i hvilken grad de etterlater seg spor ved bruk av mobiltelefon eller Internett. Bevisstheten rundt slike spor var likevel merkbart høyere blant de voksne enn blant de unge.

Svært få av deltakerne trodde at personopplysninger om dem noen gang var blitt misbrukt. De unge viste seg å være mindre bekymret i forhold til personvernkonsekvenser ved bruk av IKT, noe som kan skyldes både kunnskapsnivå og en generell ungdommelig ubekymrethet. De voksne var mer kunnskapsrike, mer bevisste og mer reflekterte omkring hvordan bruk av IKT kan påvirke på personvernet. Felles for ungdom og voksne var at svært få var villige til å bruke mye tid for å ivareta eget personvern i bruk av IKT. Deltakerne virket å ha vent seg til tidseffektive og brukervennlige IKT-tjenester slik at ekstra innsats for å sikre egne personopplysninger var vanskelig å motivere.

De unge deltakerne benyttet seg i liten grad av e-handelstjenester. Dette hadde lite å gjøre med engstelse for å handle over nett, men mer å gjøre med at de hadde begrensede midler og hvor flere av de ikke hadde kredittkort. Men de fleste voksne handlet over internett og benyttet seg av nettbank. De voksne deltakerne som ikke benyttet seg av denne type tjenester begrunnet det med sikkerhetshensyn. I disse tilfellene var det ikke primært personvernet de var mest bekymret for, men faren for at kredittkortnummeret skulle kunne komme på avveie eller at fremmede skulle kunne bryte seg inn i nettbanken.

Både menn og kvinner, ungdom og voksne benyttet seg av konstruert brukernavn (nickname) ved bruk av chattekanaler og lignende tjenester. De fleste mannlige deltakerne uttalte at de vanligvis også oppga falske opplysninger om seg selv til tjenester på internett hvis de oppfatter det som unødvendig å oppgi korrekte personopplysninger. Dette ble gjort bevisst for å redusere mengden av spor som kunne knyttes til dem personlig. Flere kvinner, spesielt blant de voksne, påpekte derimot at de unngikk å bruke oppdiktede opplysninger fordi de oppfattet dette som illegitimt og var bekymret for eventuelle konsekvenser. På den annen side opererte omtrent alle deltakerne med flere e-postadresser for å beskytte seg mot søppelpost.

Begreper som cookies (informasjonskapsler) og internettlogg (historiefunksjon) var lite kjent blant deltakerne og bare noen få slettet dette. Anonymiseringsverktøy var i praksis ukjent og ingen oppgav at de benyttet seg av slikt. En mulighet til å kryptere e-post for å

holde innholdet hemmelig for andre enn mottakeren ble av mange voksne vurdert som ønskelig. Forutsetningen var derimot at det måtte være enkelt og brukervennlig. De unge uttrykte mer bekymring for at sidemannen på pc-salen skulle kunne se hva man skrev i en e-post enn for at utenforstående aktører kunne lese mailen deres.

Ingen av deltakerne oppgav å bruke noen form for lokasjonsbaserte tjenester på mobiltelefonen. Videre var deltakerne negative til at kommersielle aktører skulle kunne sende direkte tilbud på SMS ut i fra hvor man befant seg geografisk. Dette ble begrunnet med at det var irriterende med reklame på mobilen, men det ble også forbundet med ubehag at andre skulle kunne ha oversikt over hvor man befant seg til enhver tid.

Stilt overfor dilemmaet om mulig motstridende hensyn mellom personvern og kriminalitetsbekjempelse påpekte de fleste av deltakerne at det var viktigere å hindre kriminalitet enn å beskytte personvernet. En generell holdning som lå til grunn for diskusjonen blant brukerne var at så lenge man ikke gjorde noe kriminelt var det liten grunn til bekymring. Men det ble understreket at kun autoriserte personer skulle ha adgang til slike data. I forhold til ivaretakelse av personvern viste deltakerne stor grad av tillit til både myndigheter og store private selskaper. På den annen side viste de fleste en klar skepsis til aktører på Internett, og de fleste var forsiktige med å oppgi personopplysninger til firmaer som de enten ikke kjente eller som de ikke syntes virket seriøse.

Deltakere påpekte at de selv hadde et ansvar for å beskytte seg ved å ikke legge igjen personopplysninger ukritisk på nettet. Samtidig uttalte de at de ikke visste helt hva de hadde behov for å beskytte seg mot og det ble etterlyst mer informasjon både fra myndighetenes side og fra leverandørenes side.

Inntrykket fra samtalene viste at de av brukerne som hadde best kunnskap om teknologien også var mest bevisst på mulige konsekvenser for personvernet. Selv om de unge deltakerne i stor grad var storforbrukere av kommunikasjonstjenester på mobiltelefon og Internett hadde de mindre kjennskap til hvordan teknologien fungerte på andre områder. Samtidig viste samtalene at flere av de voksne hadde et bredt kunnskapsnivå om teknologi og bevissthet omkring hvilke konsekvenser bruken av disse tjenestene kan ha for deres personvern.

1. Innledning

1.1 Om undersøkelsen

Som del av prosjektet *IKT & personvern* har Teknologirådet høsten 2003 snakket med lekfolk, det vil si vanlige brukere av informasjons- og kommunikasjonsteknologier (IKT) som mobiltelefon og Internett. I den forbindelse har 48 personer fordelt på 6 fokusgrupper i Oslo og Bodø fortalt om sin bruk av IKT og uttalt seg om problemstillinger knyttet til personvern. Vi har snakket med fire grupper av ungdom mellom 17 og 19 år samt to grupper av unge voksne mellom 30 og 40 år. I tillegg til denne inndeling etter alder, var gruppene også delt inn etter kjønn, det vil si tre grupper menn og tre grupper kvinner. Dette for å kunne avdekke mulige forskjeller mellom kjønnene.

Denne delrapporten fra prosjektet IKT & personvern beskriver resultatene fra de samtalene vi hadde i fokusgruppene. Det gjøres oppmerksom på at undersøkelsen ikke representerer noe forskningsprosjekt og heller ikke sikter mot å frambringe statistisk holdbare resultater. Derimot er det en enkel, kvalitativ undersøkelse som gir et innblikk i hvordan vanlige mennesker bruker IKT og hvordan de forholder seg til mulige farer for eget personvern i den sammenheng.

1.2 Bakgrunn

Bruk av nyere IKT-tjenester som Internett, e-post, mobiltelefoni og lokasjonsbaserte tjenester etterlater stadig flere og mer innholdsrike elektroniske spor som i mange tilfeller lagres på ulike steder. Slike spor kan inneholde informasjon som oppfattes som sensitiv av brukeren og som hun derfor ikke ønsker at uvedkommende skal se. Den økte mengden av elektronisk lagret informasjon kan i mange tilfeller lett utnyttes til å få kunnskap om en person og slik kan dette utgjøre en potensiell trussel mot brukerens personvern.
Både kommersielle interesser og myndighetsorganer som politi og rettsvesen har interesse av å få tilgang til slike spor fra elektronisk kommunikasjon. Bedrifter ønsker å kunne tilby skreddersydde tjenester og målrettet markedsføring for bedre å tjene kundene og slik forbedre sin lønnsomhet, mens politiet trenger tilgang til elektroniske spor i etterforskning og for å avverge mulige kriminelle handlinger. Dette er begge legitime interesser og både private og offentlige aktører må naturlig nok ha muligheten til å kunne utnytte de fordelene som elektronisk kommunikasjon medfører. På den annen side gjør hensynet til personvernet det nødvendig å begrense tilgangen til potensielt sensitive personopplysninger som kan trekkes ut av slike data. Det er altså nødvendig å finne en balanse mellom behovene for på den ene side å sikre samfunnet mot kriminalitet samt å gi bedriftene gode konkurransevilkår, og på den andre side å sikre et grunnleggende vern om borgernes personlige integritet og privatsfære. Hvor grensene for personvernet skal gå er derimot intet enkelt spørsmål å finne svar på. Det er et spørsmål det finnes ulike meninger om og hvor brukernes meninger er like interessante som ekspertvurderinger.

Teknologirådets prosjekt IKT & personvern har engasjert et sett av eksperter innen jus, samfunnsvitenskap og teknologi til å se på situasjonen for personvernet i lys av de nye teknologiene som setter mange elektroniske spor. Som et supplement til denne gruppens ekspertvurderinger har prosjektet gjennomført en undersøkelse for å få et innblikk i lekfolks meninger og holdninger knyttet til IKT og personvern. Dette på bakgrunn av at mobiltelefon og Internett er dagligdags teknologi for de fleste. Tall viser at i Norge har 92 prosent av husholdningene mobiltelefon og halvparten av norske husholdninger har tilgang til Internett (SSB, 2003).

2. Elektroniske spor og personvern

Inntrykkene fra fokusgruppene vil her bli presentert ut i fra intervjuguidens struktur, og temaene vil bli fremstilt i følgende rekkefølge; personvern, e-handel, elektroniske spor, mobiltelefon og lokasjonsbaserte tjenester og utvidet lagringstid. Temaene vil inneholde spørsmål som deltakerne har diskutert i gruppene.

2.1.1 Personvern?

Begrepet personvern blir gjerne forbundet med interessen for å kontrollere formidlingen og bruk av opplysninger som angår en selv, det vil si når og til hvem, til hvilket formål og til hvem ved videreformidling (Bing, 1991).

Vi spurte deltakerne om hva de selv mente at begrepet personvern innebar, og om de oppfattet det som en viktig sak for den enkelte.

Internett ble oppfattet som uoversiktlig og ukontrollert med mange aktører og en arena med potensiale for misbruk av personlig opplysninger. De fleste av de unge deltakerne knyttet personvern til noe som hadde med personlige opplysninger å gjøre. De oppfattet personvern som noe viktig, men uten å være helt sikre på hvorfor. Ungdommene påpekte også at dette var noe som de ikke var opptatt av i hverdagen, men konstruerte scenarier om hva som kunne skje hvis deres identitet ble misbrukt eller stjålet.

Blant de voksne deltakerne var det en klar oppfatning hva personvern innebar. De knyttet begrepet til personlige opplysninger og taushetsplikt i ulike sektorer i arbeidslivet, f.eks. helsevesenet, fengsel og politi. De understreket at de var forsiktig med å gi fra seg persondata og vurderte hver forespørsel om personlige opplysninger ut i fra formålet. De voksne deltakerne var mer restriktive til det å utlevere personlige opplysninger om seg selv og var opptatt av hvilke rettigheter man hadde som enkeltindivid. Diskusjonene tydet på at de voksne var mer bevisste enn ungdommene og hadde mer kunnskap om begrepet personvern.

> *"Det er jo blitt lettere å misbruke identiteten til folk på Internett. Du kan gi deg ut for å være hvem som helst, og du kan bruke andres opplysninger. Jeg vet ikke hvor godt det er beskyttet på Internett, jeg vet ikke i hvilken grad de kan kontrollere det, om de i det hele tatt kan det" (Gutt, Oslo)*

> *"Man har jo hørt om identiteten som blir stjålet og blir brukt. Penger og navn blir brukt til ulike ting via kredittkortkort" (Jente, Oslo)*

> *"Det er bare en viss mengde med opplysninger folk rundt deg har behov for å vite om deg. Det er først og fremst navnet ditt, ikke gjeld og sånne ting" (Mann, Oslo)*

2.1.2 Misbruk av personlige opplysninger

Studier viser at økonomisk svindel over nett er et økende problem. En amerikansk undersøkelse indikerer at 27,3 millioneramerikanske personer ble rammet av at uvedkommende misbrukte bankkonto, kredittkort eller offentlige dokumenter i 2002 (Epic, 2002).

Få av deltakerne oppgav selv å ha opplevd misbruk av sine personopplysninger. De som hadde opplevd det mente at det de var utsatt for ikke var av alvorlig karakter, men som de vurderte som relativt uskyldig.

Grunnen for at deres personlige opplysninger i liten grad var utsatt for misbruk mente de kunne skyldes flere ting som tilfeldigheter, at denne type kriminalitet sjeldent skjedde, men først og fremst at deres persondata ikke var interessant nok for andre. Det ble også påpekt at det fantes mye personlige opplysninger om mange slik at sannsynligheten for at dette skulle ramme dem var liten. Derimot var det en oppfatning blant deltakerne om at bedrifter og firmaer i større grad var mer utsatt for misbruk av data fordi dette ble vurdert av deltakerne som mer lønnsomt og lukrativt.

De unge deltakerne var mindre bekymret for eventuelle misbruk av persondata enn det de voksne var. Ungdommene var enig om at man selv kunne redusere faren for misbruk ved å unngå å gi sensitive data som personnummer eller PIN-koden til mobilen. Tenåringene poengterte at dette gjorde man selvfølgelig ikke, og hvis man kom i en slik situasjon ble det understreket at man selv var ansvarlig for å unngå å utlevere denne type data.

De voksne deltakerne uttrykte mer bekymring enn de unge for mulighet for misbruk av personlig opplysninger. De fleste av de voksne benyttet seg av nettbank, men følte seg ikke alltid trygg på at deres opplysninger var sikret for et eventuelt misbruk. Men det ble understreket at de ikke var så engstelig at de unngikk å benytte seg av nettbank.

> *"Jeg tenker ikke over det når jeg gir ifra meg informasjon om meg sjøl, jeg tenker mer at det er ingen som gidder å gjøre noe med det, at det er ingen som kommer til å bruke det. Det er mulig at det er dumt tenkt" (Gutt, Oslo)*

> *"Man tenker jo at det ikke er så mange opplysninger som er så farlig å gi bort. Jeg forstår ikke helt hva som er så farlig med det at noen får tak i navnet mitt og adressen min. Jeg forstår ikke hva de kan gjøre med det" (Jente, Oslo)*

> *"Det er jo dette med økonomisk svindel, kredittkort og regninger. Å få identiteten sin misbrukt" (Mann, Oslo)*

2.1.3 Bilder og MMS

En måte å misbruke personlige opplysninger på kan være gjennom publisering av bilder av en person uten vedkommendes samtykke. Mobilfunksjonen MMS forsterker denne muligheten fordi tjenesten innebærer å sende bilder, lyd og tekst. Stadig flere mobilmodeller har også egne innebygde kameraer. Salget av MMS-telefoner har økt kraftig i løpet av det siste året, og man regner at ca. 40 prosent av alle mobiler som selges i dag er MMS telefoner (Elektro- og Elektronikkbransjen, 2003), samtidig som det har vært gjennomført gratiskampanjer for bruk av MMS hos teleselskapene. I takt med dette har muligheten for å bli fotografert og få bildet publisert uten egen viten og vilje også økt.

På bakgrunn av dette ble deltakerne spurt om de hadde opplevd å bli fotografert og få bildet publisert på nettet eller sendt til andre via MMS uten deres samtykke. Det viste seg at det var kun de unge deltakerne som hadde erfart dette. Det var først og fremst bilder tatt på fest som i etterkant ble lagt ut på spesifikke nettsteder for festbilder. Ungdommene selv mente at årsaken til dette skyldtes bruk av digitale kameraer og at denne type aktivitet ble oppfattet som ganske vanlig i deres miljø. Mange opplevde det som litt ubehagelig, men ubehaget ble redusert ved at de fleste festdeltakerne erfarte det samme. Det ble i samtalene påpekt at hvis man ønsket å unngå dette burde man ta forholdsregler, men det var selvfølgelig ingen garanti mot å bli fotografert.

Til tross for at de voksne selv ikke regnet med å være i faresonen for å bli fotografert i et intetanende øyeblikk utrykte de bekymring for denne type bruk av MMS og Internett. De voksne vurderte det som en mulig trussel mot personvernet, fordi man ikke har kontroll over hvem som kan fotografere en og når det gjøres. De voksne deltakerne påpekte også at ved å bruke Internett som publiseringskanal vil bilder kunne florere og at man ikke har anledning til å fjerne det.

> *"Det har vært tatt bilder fra fester og blitt lagt ut på nettet. Det har stått navnet mitt under og selv så jeg at det var meg. Det synes jeg var litt ubehagelig" (Jente, Oslo)*

> *"Jeg tror ikke at menn over 30 år er en attraksjon for å ta bilder av og legge ut på weben" (Mann, Oslo)*

Inntrykkene fra samtalen viser at MMS og publisering av bilder først og fremst er et fenomen i ungdomskulturen. Samtidig kommer det stadig forbud mot mobilkamera på offentlige steder som skoler, svømmebasseng og treningssentre. Dette har først og fremst skjedd i USA, men også enkelte helsestudioer har tatt i bruk forbudet. Dette kan tyde på at brukere begynner å få en erfaring med uønsket fotografering, og at mange opplever dette som ubehagelig.

2.2.1 E-handel

E-handel innebærer alle former for kommersielle transaksjoner og forretningsvirksomhet over elektroniske nett. I en undersøkelse utført av SSB brukte syv av ti personer Internett som en kanal for å handle eller selge varer og tjenester samt banktjenester (SSB, 2003). Når man handler over nettet vil man etterlate seg identifikasjonsdata, altså opplysninger om navn og adresse, og finansielle data som vil være kredittkortnummer eventuell annen betalingsmåte (Coll, 2000).

En annen type informasjon som blir registrert i forbindelse med en netthandel er bruksmønsterinformasjon som inneholder opplysninger om faktiske forhold som brukerens bevegelser på nettet, hvilke URLs som man har besøkt, cookies og søkeord man har benyttet seg av (Coll, 2000). Det betyr at mengden av personlige opplysninger også har økt. Utfordringen til personvernet her vil være at transaksjonsopplysningene kan kobles til opplysninger som navn og adresse og slik knyttes til en bestemt person. Det blir derfor viktig å vite hvem som har tilgang på hvilken informasjon og hva det brukes til. Til tross for at man regner med at rundt 1.3 millioner nordmenn surfer på nettet er nordmenn fortsatt litt skeptiske til e-handel. En spørreundersøkelse viser at årsaken til at man ennå er litt tilbakeholden skyldes i stor grad sikkerhetssyn (IDC, 2003).

Deltakerne ble spurt om de benyttet seg av nettbaserte tjenester og i så fall hvordan de opplevde å gi fra seg personlige opplysninger over nett. Her varierte oppfatningene ut i fra alder, hvor de unge uttrykte mindre bekymring enn de voksne for å benytte seg av e-handel.

De fleste av de unge deltakerne hadde ikke faste handlevaner på nettet, men kjøpte sporadisk utstyr til fritidsaktiviteter på grunn av gunstig pris eller tilgjengelighet. Mangelen på faste handlevaner hos de unge skyldtes ikke frykt for å måtte gi fra seg personlige opplysninger, men de begrunnet det med at de hadde begrensede ressurser til forbruk. Det var få av de unge som hadde kredittkort så de fleste unge benyttet seg i hovedsak av oppkrav eller faktura som betalingsmåte, det vil si at de bestilte varer over nettet og brukte

Internett som en markedsplass. Ungdommene hadde imidlertid en oppfatning om at det var enkelt og relativt trygt å handle over nett.

Blant de voksne oppsto det et skille under samtalene mellom de som anvendte e-handel og de som ikke gjorde det. Den gruppen av voksne deltakere som benyttet seg av elektronisk handel forklarte det med at de opplevde denne formen å handle på som nyttig og tidsbesparende og brukte det derfor jevnlig. De som ikke handlet over nett begrunnet det med at de ikke følte seg trygge på at deres personlige opplysninger ville bli ivaretatt og håndtert på en forsvarlig måte og unngikk derfor tjenesten.

> *"Det er ikke ofte, men nå og da handler jeg. Det er mest snowboardutstyr og sånn. Det er veldig greit, du trenger ikke å oppgi opplysninger om kontonummeret ditt" (Gutt, Oslo)*

> *"Jeg har ikke handla over nettet. Jeg har hørt så mange historier om det så det har jeg holdt meg unna" (Kvinne, Oslo)*

De voksne som handlet over nett diskuterte også hvilke krav de stilte til en nettside for å benytte seg av den for å handle. De hevdet å være selektive ved valg av nettsider, og de hadde ulike vurderingskriterier. Et moment var nettsidens design som ble tillagt stor betydning fordi den ble oppfattet som en indikator på nettsidens grad av seriøsitet. De foretrakk å handle eller bruke nettsider til kjente eller store firmaer fordi de mente at det var enklere å vurdere dens pålitelighet enn nettsider til mindre og ukjente *dotcom* firmaer. Det ble også nevnt at man kunne undersøke nettselskapene nærmere ved å sjekke deres informasjon i registre, f. eks. Brøynnøysundregistrene. Men dette ble benyttet i liten grad fordi det var for tidkrevende og omfattende i forhold til behovet

> *"Forrige gang jeg brukte nettbank så hadde de endret på hele designen. Da ble jeg skeptisk. Men jeg brukte den etter hvert" (Kvinne, Oslo)*

Blant de voksne deltakerne var skillet mellom de som handlet over nett og de som ikke gjorde det blant annet avhengig av hvor mye Internettkompetanse de hadde. Dette viser også en undersøkelse fra IDC, hvor det blir påpekt at det å bruke Internett som handelskanal var avhengig av brukserfaring og kjennskap til Internett. Sannsynligheten for at folk skal handle over nett er altså større hvis de har brukt Internett over lengre tid (IDC, 2003). Dette harmonerer også med våre antagelser; de som handlet elektronisk påpekte også at de selv mente de hadde en viss kompetanse om teknologi. Ungdommene har ikke e-handel som en sterk digital vane ennå, men er en gruppe som generelt innehar gode basiskompetanse innenfor IKT. Det viser at det er forskjeller mellom digitale vaner og basiskompetanse (Frønes, 2002).

2.2.2 Gratis SMS mot personopplysninger

Mange nettsider tilbyr gaver som f.eks. gratis SMS mot at man oppgir opplysninger om seg selv. Det kan være opplysninger som navn, adresse eller informasjon om sine interesser. En undersøkelse fra SSB (1997) viste at blant personer under 30 var det 48 prosent som var villig til å gi fra seg vane- og interesseinformasjon for å delta i en konkurranse med premie. En amerikansk studie fra 2002 viser at man vurderte opplysninger som kredittkortnummer, personnummer, informasjon om lønn og helse eller telefonnummer som relativt sensitive, mens navn og adresse ble vurdert som det enkleste å gi fra seg (Epic, 2002).

Deltakerne diskuterte om dette var noe som de benyttet seg av, og i så fall hvor grensen gikk for utlevering av personlig opplysninger. Samtalene i gruppene viste at det var en

positiv holdning til å gi fra seg opplysninger mot å motta gaver forutsatt at det dreide seg om enkle opplysninger som navn og adresse.

De unge deltakerne syntes det var uproblematisk å gi bort personopplysninger for å motta gaver og hadde lav terskel for å gi fra seg persondata. Opplysninger som navn og adresse ble oppfattet som ikke-sensitive fordi det var informasjon som ellers var lett tilgjengelig i registre som eksempelvis telefonkatalogen og kunne derfor gis bort over nettet mot gaver. Også de voksne deltakerne hadde en avslappet holdning til dette, og ga gjerne bort opplysninger som navn og adresse for å kunne motta gaver.

> *"Du går jo ikke på sånne sider hvor det står at du er sikret tre millioner hvis du legger igjen de og de opplysningene om deg. Men hvis det er de store mobilselskapene hvor du kan få noen SMS mot å gi par opplysninger om deg sjøl, så er det greit. Det kommer jo litt an på hvor seriøse de er. Du vet stort sett når de er seriøse eller ikke" (Gutt, Bodø)*
>
> *"Det er lett å registrere seg for å få noe gratis, det er jo det. Få såper, diverse dingsedangser" (Kvinne, Oslo)*
>
> *"Jeg har registrert meg på noe for å få gratis SMS'er. Det er jo klart at man må vurdere om det er ok. Jeg er litt skeptisk til det nå. Jeg var ikke det da jeg gjorde det, men har blitt mer skeptisk siden da. Men det er klart, hvis det er noe som virker bra nok ville jeg nok ha registrert meg igjen, så sterk aversjon mot det har jeg ikke. Men bare på nettsteder der jeg får gratis SMS'er" (Mann, Oslo)*

Inntrykkene fra fokusgruppene viser at deltakerne har et bevisst forhold til sine personopplysninger i situasjoner hvor de blir spurt direkte om utlevering av informasjon, og hvor de selv kan vurdere risikoen og gevinsten på å selv bestemme hvilke opplysninger man vil gi for å motta en gave.

2.2.3 Videresalg av personlige opplysninger

Internett gjør det lettere å lage brukerprofiler ved at man kan samle inn informasjon om en persons interesser, forbruk, inntekt, preferanser og vaner. Kartlegging av handlemønster er stor industri, der personlige opplysninger får stor verdi og blir gjenstand for videresalg mellom nettaktører. På den måten kan brukeren få tilbud fra andre nettaktører om tjenester og konsumenter de er interessert i. Dette skjer ofte uten at brukeren har gitt sin tillatelse for det. En amerikansk studie viser at en majoritet ikke stolte på at deres personopplysninger ble forvaltet på en skikkelig måte blant bedrifter og firmaer (Poll, 2002).

Deltakerne diskuterte videresalg av personlig opplysninger, og hadde en klar oppfatning av at dette overhodet ikke var akseptabelt.

Denne type handling så både de unge og voksne deltakerne på som et tillitsbrudd fordi opplysningene i utgangspunket ble gitt til en bestemt aktør fra kunden. Deltakerne påpekte at ved et eventuelt videresalg av persondata hadde man ikke lengre mulighet for kontroll og oversikt over hvem som hadde tilgang til disse. Det ble også uttrykt en viss indignasjon over at andre kunne tjene på opplysninger som de hadde gitt fra seg.

Mange nettaktører opererer med informasjon om personvern (privacy policy*)* på sine nettsider, altså et dokument for hvordan nettaktøren behandler opplysningene som man

gir fra seg ved for eksempel handel. Men det viste seg at det var få av deltakerne som leste den når de skulle benytte seg av nett-tjenester. Både de unge og de voksne mente at denne type dokument var alt for lang og tidkrevende å lese og ble oppfattet som ganske unødvendig.

> *"Når jeg legger igjen sånne opplysninger har jeg en oppfatning at jeg vil bli behandla anonymt. Men når andre får de opplysningene om meg og bruker det videre så liker jeg det ikke noe særlig. Det synes jeg er litt på kanten overfor kundene" (Gutt, Bodø)*

> *"Jeg er skeptisk til det, jeg synes det er en sak mellom meg og der jeg legger igjen opplysninger. Jeg synes ikke at de skal tjene penger på det. Det synes jeg er dårlig, det liker jeg ikke" (Mann, Oslo)*

Deltakerne var interessert i å være orientert om registrering av sine opplysninger og behandling av sin informasjon og indikerer at man har behov for en viss kontroll. Hvis man opplever at tilliten blir brutt kan det påvirke brukerens adferd på nettet. Teknologileverandørene er også avhengig av brukerens tiltro fordi en eventuell mangel på det kan hemme bruken av nye nettbaserte tjenester.

2.2.4 Falske opplysninger

Når operasjoner på nettet krever identifikasjon vil overføringen gi detaljerte spor om brukeren. Disse sporene kan konstruere et bilde av vedkommendes behov, kommersiell adferd, men også ikke-kommersiell virksomhet, eks. tilknytning til politikk eller organisasjonsarbeid. Flere nettsteder krever opplysninger av brukeren for at man skal kunne få adgang til tjenesten deres. Det er ikke alltid det er tydelig hva disse opplysningene skal brukes til, og ofte er disse kravene unødvendige for å kunne benytte seg av den aktuelle tjenesten. Overskuddsinformasjon som man avgir kan brukes til å gi nettselskaper profitt på bekostning av brukerens personvern. Disse opplysningene kan brukes til forskjellige formål, som registrering og statistikk som igjen kan brukes til markedsføring.

En undersøkelse fra Forbrukerombudet i Norden (2003) viser at ut i fra et utvalg av nettsider var det bare en tredjedel av nettstedene som ba om samtykke til direktereklame, mens det kun var halvparten av disse nettsidene som opplyste om hvordan brukeren kunne trekke samtykke tilbake senere. En strategi for å unngå at navn og adresse havnet i register og databaser kan være å oppgi falsk informasjon om seg selv til nettsteder som ikke gir tydelig informasjon hva de skal bruke opplysningene til.

Deltakerne ble spurt om falsk personopplysninger var en framgangsmåte som de benyttet seg av. Det viste seg at noen av deltakerne oppga konstruerte navn, mens andre unnlot det. Her var det merkbar forskjell mellom kjønnene.

I aldersgruppen 17-19 år hadde de fleste av deltakerne opplevd at nettsteder avkrevde de for opplysninger som de selv mente var unødvendig. Jentene var i større grad mer restriktive med å bruke falsk informasjon enn guttene, og valgte heller å oppgi eventuelle mellomnavn eller de brukte kun ett etternavn hvis de hadde flere. Andre valgte å unngå hele tjenesten. Guttene, derimot, hadde et mer avslappet forhold til å benytte seg av konstruerte eller falske opplysninger ved registrering på nettet. Falske navn brukes for å unngå at ens personlig opplysninger havner i databaser. Hvis det ikke oppfattes som nødvendig å oppgi riktig navn, som f. eks hvis man skal få noe tilsendt i posten, fant de ingen grunn til å bruke sitt virkelige navn.

Denne antydningen til kjønnsforskjell gjenspeilte seg også blant de voksne deltakerne. Kvinnene var i større grad skeptisk til å konstruere nye opplysninger om seg selv enn det mennene ga uttrykk for. Vegringen mot å oppgi falske opplysninger ble begrunnet med bekymring for eventuelle konsekvenser fordi de oppfattet handlingen som ikke helt legitim. Men denne aversjonen kom ikke fram blant de mannlige deltakerne. De fremhevet derimot betydningen av å oppgi falsk informasjon for å unngå at deres ekte persondata unødig ble samlet og oppbevart i ulike registre.

Men en strategi som de fleste av deltakerne benyttet seg av, uavhengig av kjønn og alder, var å opprette flere e-postadresser. På den måten kunne deltakerne begrense mengden av spam (uønsket reklame) i sin private e-postboks og redusere faren for virus.

> *"Det er ofte det er noen opplysninger man ikke trenger å gi, så da gjør jeg ikke det. Hvis de skal ha etternavn, har jeg to og bruker bare det ene. Jeg tar bare de navnene jeg må ta" (Jente, Oslo)*

> *"Jeg synes at det er så teit at navnet mitt bare skal stå der når de egentlig ikke trenger det. Jeg føler ikke behov for å gi navnet mitt. Så da bare finner jeg på noe" (Gutt, Oslo)*

> *"Jeg tør ikke, jeg. Jeg er redd for at jeg skal bli straffet hvis jeg skriver noe som ikke er sant" (Kvinne, Oslo)*

Inntrykkene fra samtalene viser at tillit blir sentralt når man skal benytte seg av tjenester på nettet. Når man er usikker på graden av en nettside seriøsitet benyttet man seg av å oppgi begrenset eller feil informasjon for å kunne styre noe av omfanget av personopplysninger.

2.3.1 Elektroniske spor

Når man enten surfer på nettet, bruker mobiltelefonen eller andre elektroniske systemer legger man igjen spor i form av loggdata. Disse sporene kan inneholde opplysninger om hva man har gjort, hvor man har vært og til hvilken tid.

Vi ønsket derfor å vite om dette var noe som deltakerne var klar over og om de i så fall hadde strategier for å begrense mengden av elektroniske spor. En utbredt innstilling i utvalget var at så lenge man ikke begikk kriminelle handlinger hadde man ikke så stor grunn til å bekymre seg for at man la igjen elektroniske spor. Verneverdien av personlige opplysninger blant deltakerne varierte. Blant deltakerne var de voksne mer bekymret for elektroniske spor enn de unge.

De unge deltakerne var avslappet til igjenleggelse av elektroniske spor. Men under diskusjonene ble også noen av de unge deltakerne imidlertid mer bekymret enn det de opprinnelig var i utgangspunktet.

De voksne understreket at det var ubehagelig at man la igjen elektronisk informasjon om seg selv, og at man i liten grad hadde kontroll over det på grunn av teknologiens egenskaper som gjør det vanskelig for brukeren å ha kontroll over hvor ens egne elektroniske spor havner og hvem som har tilgang til dem. Samtidig ble det også påpekt at elektroniske spor kunne innebærer en form for trygghet.

"Men det er ikke alltid man kan gjøre noe, noen ganger så bare setter man spor, særlig med mobilen. Hvis du ringer, du trenger ikke å gjøre det heller, sender mobilen signaler og noen kan da vite hvor du er hen. Det er nok mange ting man må holde seg unna, særlig nå som den teknologiske utviklingen går så sinnssyk fort. Det går jo mer og mer i den retningen" (Gutt, Oslo)

"Jeg føler meg tryggere hvis det skulle skje noe. Da vet noen hvor jeg har vært hen" (Kvinne, Oslo)

"Hvis det er noen som ønsker å finne spesifikk informasjon om deg så kan de det. Det kan jo ligge hvor som helst, man har ikke kontroll over hva som finnes" (Mann, Oslo)

2.3.2 Internett og cookies

Hver gang man surfer på Internett legger man igjen elektroniske spor i form av cookies eller informasjonskapsler som lagres på harddisken. Cookies er små datafiler som lagrer informasjon, og denne lille filen med informasjon gjør at applikasjonene på nettsiden kan skille mellom en selv og andre brukere. Cookies gjør det enklere å surfe på nettet fordi det blir mulig å lagre passord, kjøp og andre preferanser på et nettsted (Coll, 2000).

Cookies kan også gi opplysninger om når man besøkte en nettside, og dermed inneha data om brukerens adferd på nettet. Ut i fra de registrerte preferanser gir cookies anledning til at man kan få skreddersydde tilbud. Skreddersydde og tilrettelagte tjenester og informasjon kan være av interesse for brukeren. Dette krever imidlertid at tilbyderen har korrekte opplysninger om vedkommende som ønsker dette (Coll, 2000) ellers kan det virke mot sin hensikt og skape irritasjon.

Deltakerne ble spurt om de kjente til cookies og om de slettet dem for å skjule spor om sin nettbruk. Det var imidlertid få av deltakerne som kjente til cookies og nesten ingen som slettet dem.

Etter hvert som de fikk en klarere oppfatning hva cookies innebar mente de unge deltakerne at det ville være få som kunne ha interesse av innholdet i deres cookies. Det var også lite kunnskap om dette blant de voksne deltakerne. Det viste seg også at det å ha brukerkunnskap ikke er en forutsetning for å inneha konsekvenskunnskap.

De unge var positive til å motta skreddersydd reklame annonsering om tjenester eller produkter man var interessert i. Hos de voksne var det i større grad delte oppfatninger. Noen opplevde dette som irriterende, og ville selv bestemme når de hadde behov for informasjon om et produkt og oppsøke den aktuelle nettleverandøren på egen hånd.

"Jeg synes at det handler om personvern så fort jeg har vært på en side og bare tittet litt så blir det registrert. Og det er vel noe som man glemmer fort" (Kvinne, Oslo)

"Jeg får sånne mail som tror at jeg liker Justin Timberlake og boyband og sånn, det er jo så feil!" (Jente, Oslo)

Det framgår tydelig i samtalene at det generelt er lite kunnskap om hva slags spor man etterlater seg og hvordan man kan minske mengden av dem. Å oppsøke en nettside oppfattes som uskyldig og de fleste er heller ikke bevisst på at besøket blir registrert.

I utgangspunktet trodde vi at de unge deltakerne skulle inneha mye kunnskap om dette fordi de er vokst opp med denne teknologien og er storforbrukere av Internett. Men denne antagelsen viste seg å ikke stemme med de ungdommene som deltok. Det understreker at det ikke nødvendigvis er så nær sammenheng mellom det å ha brukerkunnskap om IKT og det å ha kunnskap om konsekvenser ved bruk av den.

2.3.3 Internett og logg

En annen måte å redusere synligheten av sin nettaktivitet kan være å slette loggen på harddisken. Slik kan man hindre at andre som har tilgang til samme pc kan se ens bevegelser og adferd på nettet.

En stor andel av deltakerne kjente ikke til nettloggen og slettet den derfor heller ikke. Men ungdommene var ikke så bekymret for at andre kunne se hvilke nettsider de hadde besøkt, og mente at denne type data ville være uinteressant for andre. De unge deltakerne var mer opptatt av å få slettet gamle chattelogger som lå på nettet. De uttrykte at det ville være ubehagelig hvis andre kunne se hva man hadde skrevet i gamle chat-rom selv om det ikke nødvendigvis inneholdt sensitive opplysninger. Ungdommene påpekte at selv om man benyttet seg av nick, altså fiktivt navn, ved chatting, ble det likevel sett på som ekkelt og pinlig hvis andre skulle kunne lese chatteloggen i ettertid.

De fleste av de voksne mente at de ikke hadde noe å skjule når det gjaldt spor etter nettbesøk. Flere av de voksne, uavhengige av kjønn, kjente til nettloggen og slettet den, og noen var også klar over at dette ikke var en endelig fjerning av spor. Likevel ønsket de å fjerne innholdet i nettloggen fordi det ble forbundet med ubehag at andre kunne se hvor de hadde surfet på nettet.

En annen måte å kontrollere hvilke opplysninger man gir fra seg kan være å regulere personverninnstillingen for Internett sonen. Denne strategien var kun få av deltakerne kjent med. Noen av de unge deltakerne hadde prøvd denne den, men sluttet å benytte seg av den fordi den gjorde det vanskelig å besøke enkelte nettsider.

> *"Det som kanskje er mest bekymringsfullt er sånne chattelogger, det har jeg gjort en del av (Chattet,* red.adm*). Der kan folk se utrolig mye rart og personlig" (Gutt, Bodø)*

> *"Jeg tror jeg gjør det (slette spor) fordi jeg sletter loggen på maskinen, men den er jo ikke borte for det, jeg vet såpass. Jeg kan godt slette alt på maskinen og så sende den til en superprogrammerer og han finner alt likevel" (Kvinne, Oslo)*

Det var altså kun få som kjente til nettloggen og enda færre som slettet den. Det faktum at så få regulerer personverninnstillingen i nettleseren gir et signal om betydningen av brukervennlighet framfor ivaretakelse av personvernet. Selv om man er vokst opp med en teknologi er det ingen selvfølge at man har kunnskap om konsekvensene som bruken gir.

2.3.4 Internett og anonymiseringsverktøy

Anonymiseringsverktøy lar brukeren opptre anonymt på Internett slik at spor ikke kan føres tilbake til brukerens reelle identitet. I dag er det flere firmaer som tilbyr anonymitet på nettet. Anonymiseringsverktøy kan gi anledning for kriminelle til å skjule seg og slik gjøre det vanskeligere for politiet til å oppklare kriminalitet. Disse sidene er imidlertid underlagt de samme reglene som resten av Internett, som betyr at de er pålagt å utlevere informasjon til myndighetene ved forbrytelser (Sunde, 2000).

Vi spurte deltakerne om de hadde kjennskap til dette og i så fall om det var noe som de benyttet seg av eller kunne tenke seg å bruke senere. Det var svært få av deltakerne som kjente til anonymiseringsverktøy, men ingen av dem brukte det. Det ble begrunnet med at de oppfattet det som tungvint og at de ikke vurderte det som nødvendig for deres nettbruk.

Noen av de voksne deltakerne reagerte på bruk av verktøy som gir tilgang til avidentifisering;

> *"Når man kan ødelegge så mye man kan i dag på nettet, så bør det ikke være lov, det bør spores tilbake. Jeg synes at det skal forbys. De tilfeller hvor det brukes er jo sikkert for å ødelegge, og da kan det forbys" (Kvinne, Oslo)*

2.4.1 E-post og kryptering

Bruken av elektronisk post har økt de siste årene både i skole- og jobbsammenheng, men også som en privat kommunikasjonskanal. I aldersgruppen 16-24 bruker 89 prosent Internett til å kommunisere og i aldersintervallet 25-44 år bruker 87 prosent Internett som kommunikasjonskanal (SSB, 2003).

Når man sender en e-post er den normalt lite beskyttet. Ved transportering av elektronisk post er innholdet i praksis like lite skjult som når man sender et vanlig postkort. Det vil si at e-posten er åpen for at flere enn kun mottakeren kan lese den.

Vi spurte deltakerne om hva de tenkte om at deres e-post kunne leses av flere enn bare mottakeren. Blant deltakerne var det få som hadde kjennskap til at deres e-post ikke var lukket for andre. Men den generelle oppfatningen var at dette var et lite problem fordi deres e-post i liten grad innehold sensitiv informasjon og at det derfor ikke spilte så stor rolle om andre enn mottakeren kunne lese teksten, selv om det kunne være ubehagelig.

De fleste av de unge mente at det ikke var så risikabelt at flere enn mottakeren kunne lese e-posten deres. De påpekte at det var mer ubehagelig at sidemannen på pc-salen kunne se hva man skrev enn at ukjente kunne lese e-posten deres. Innholdet i e-postene sine vurderte de som lite sensitiv informasjon, og som ikke hadde interesse utover mottakeren. Men noen av de unge deltakerne uttrykte bekymring og påpekte at dette kunne bli et problem på sikt når de gikk ut i arbeidslivet og skal bruke e-post som arbeidsverktøy.

De voksne deltakerne var mer skeptisk enn de unge at deres e-post var åpen for at andre kunne lese den. De oppfattet det som ubehagelig, og påpekte at det egentlig ikke burde være slik.

> *"Jeg synes at det er litt ekkelt, jeg. Jeg visste ikke at det var slik. Men det er ikke fordi jeg har så veldig personlige mail, det er bare ekkelt" (Jente, Oslo)*

> *"Er det sant? Men jeg skriver ikke så hemmelige e-poster" (Kvinne, Oslo)*

Med en stadig mer digitalisert hverdag tas elektronisk kommunikasjon i bruk på nye områder. Et eksempel kan være mailkontakt mellom lege eller psykolog og pasient, som kan inneholde sensitiv informasjon og være sårbare for de som det angår. En slik utvikling understreker betydningen av at e-post blir håndtert på en forsvarlig måte. Selv om elektronisk post ikke inneholder følsomme data kan det oppleves at innholdet i e-post ikke er beskyttet mot lesing fra uvedkommendes side.

For å sikre at innholdet i en e-post kun leses av mottakeren kan kryptering være en løsning. Kryptering innebærer å gjøre noe uleselig i form av å gjøre tekst om til koder og er et verktøy for å sikre hemmelighold av innholdet. Imidlertid krever en kryptert melding at den blir låst opp med samme nøkkel som den ble låst med fordi nøkkelen angir hvordan meldingen skal leses. Det vil normalt si at mottakeren må ha samme krypteringsprogram som avsenderen (Johnsen, 2001).

Deltakerne diskuterte om kryptering av e-post kunne være en fruktbar løsning for å beskytte innholdet for utenforstående. Kryptering var ukjent for de fleste av deltakerne, men mange mente at kryptering ikke var nødvendig fordi de ikke sendte e-post som inneholdt sensitivt informasjon. Det ble også påpekt at kryptering krever ekstra innsats fra brukeren og er ressurskrevende. Behovet for kryptering ble av deltakerne vurdert som mest nødvendig for bedrifter og i næringslivet. Det ble også understreket at hvis man skulle benytte seg av kryptering var man avhengig av at krypteringsløsningen var enkel å bruke og ikke krevde ekstra arbeid.

Men oppfatningene varierte ut i fra alder. De unge deltakerne var mindre interessert i å benytte seg av krypteringsverktøy. Det begrunnet de med at de skrev sjeldent e-post med sensitivt innhold, og at det var få som kunne ha interesse av å lese dem. Selv om ungdommene uttrykte ubehag ved at andre kunne lese e-posten deres mente de at dette var et lite problem og at det ikke veide opp for bryderiet ved å kryptere.

De voksne deltakerne hadde heller ikke vurdert kryptering av e-post som et alternativ, men de var mer positive til det enn det de unge var. I aldersgruppen 30-40 år ble det påpekt at e-post i utgangspunktet burde være lukket, og de var derfor i større grad åpne for kryptering av e-post.

> *"Når man tenker på hvor mange som skriver mail hver dag så tviler jeg på at det er noen som sitter og leser det der. Jeg tror ikke det gjelder for så mange privatpersoner, det er vel mer bedrifter* som *kan ha mye hemmeligheter og informasjon som de ikke vil skal komme ut og som det er mer fare for. Ellers så tror jeg at det ikke er noe problem" (Gutt, Bodø)*

> *"Jeg har ikke sånne hemmeligheter, men det er jo selvfølgelig greit med kryptering, at man får mulighet til det" (Kvinne, Oslo)*

Bruk av kryptering har ikke fått rotfeste blant privatpersoner. Kryptering blir også vanskelig når det er mangel på standardisering og tilretteleggelse av det (Johnsen, 2001). Behovet for krypterte e-post kan øke etter hvert som man benytter seg av flere ulike typer digitale tjenester, som f. eks helserelaterte tjenester som kontakt med lege eller apotek, hvor innholdet vil være av mer sensitiv karakter.

2.5.1 Mobiltelefon og lokasjonsbaserte tilbud

Digitalisering av data har gjort det enklere å samle og oppbevare opplysninger fordi mobiltelefonen avgir posisjonsopplysninger og gir mulighet til å spore bruker geografisk. Økt bruk av GPS-systemet kan gi nøyaktige lokaliseringsmuligheter av brukeren, og dermed gi oversikt over hvor mobilbrukere til enhver tid befinner seg. Kommersielle aktører kan benytte seg av dette ved å sende tilbud via SMS til mobileieren ut i fra hvor vedkommende oppholder seg. Det vil si at hvis man passerer en platebutikk kan man f. eks motta en melding om et tilbud på en bestemt CD.

Vi spurte deltakerne om hva de syntes om å få denne type reklame eller tilbud på mobiltelefonen. Ingen av deltakerne hadde erfart dette, men de var enig om at å bruke mobilen som markedsføringskanal ville først og fremst være irriterende, men også ubehagelig fordi det innebar at noen ville ha en oversikt over hvor de befant seg til enhver tid.

Verken de unge eller de voksne deltakerne var interessert i at kommersielle aktører kunne sende tilbud til dem via SMS ut i fra hvor de oppholdt seg. Å motta reklame på mobilen som er basert på lokasjonsdata ville bli oppfattet som forstyrrende og som en inngripen i ens private sfære fordi man da ville krysse grensen til privatlivet. Selv om man også får reklame i e-postkassen opplevde deltakerne det som mindre invaderende enn når man mottar lokasjonsbasert tilbud på mobiltelefonen.

> *"Jeg synes at det er litt skummelt, at det er noen som vet hvor du er hen og ser deg. Det synes jeg er litt ekkelt" (Jente, Bodø)*

> *"Det skjer jo når du kommer over svenskegrensa, da får du sånne tilbud, så det er jo på tur inn. Det synes jeg ikke om, fordi det grenser opp mot privatlivets fred. Grunnen for at man har mobil er jo for å kunne være for seg selv. Og hvis jeg kommer over grensa så er ikke jeg interessert i hva som er på tilbud og få det på mobilen min" (Mann, Oslo)*

Mobilen oppfattes på mange måter som en del av den private sfære og det kan dermed føles ekstra ubehagelig at andre har oversikt over hvor man befinner seg for å så sende tilbud via SMS.

2.5.2 Mobiltelefon og lokasjonsbaserte tjenester

Det utvikles kontinuerlig tjenester til mobiltelefonen, og en ny type tjenester som nå tilbys er basert å brukerens geografiske lokasjon. En type lokasjonsbasert tjeneste som er lansert kan spore opp ens venner via mobiltelefonen. For å kunne bruke tjenesten må man imidlertid samtykke og bli satt opp på en kontaktliste og for å gi oversikt til ens venner og kontakter hvor man befinner seg. Lokasjonsbaserte tjenester kan etterlate seg svært innholdsrike elektroniske spor, som kan fortelle om tid og lokalisering for hvor en mobiltelefon befinner seg.

Tjenestene som lar brukeren få vite hvor vennene befinner seg er rettet spesielt mot ungdom, men det viste seg at ingen blant våre unge deltakere benyttet seg av denne. De mente at behovet for tjenesten ikke var så stor at de var villig til å betale prisen når man like gjerne kunne spørre på SMS.

Blant de voksne deltakerne var det få som kjente til denne oppsøkningstjenesten, og derfor heller ingen av dem som hadde benyttet seg av den. De voksne var også skeptiske og uttrykte bekymring for denne type tjeneste.

> *"Problemet er at det koster penger, og vi har ikke så mye bruk for det. Hvis det var billig eller gratis så kunne vi kanskje ha brukt det, men nå kan vi heller kontakte andre per SMS. Da slipper vi at mobilen blir invadert og at det koster masse penger" (Jente, Oslo)*

> *"Hvorfor skal folk vite hvor du er hen?" (Jente, Bodø)*

"Det synes jeg virker litt skummelt, jeg har hvert fall aldri brukt det eller skal bruke det" (Gutt, Bodø)

2.6.1 Utvidet lagringstid for trafikkdata

I dag er det blitt nødvendig å utnytte elektroniske spor for å etterforske lovbrudd og forebygge kriminalitet. Dette fordi kriminelle i stor grad benytter seg av kommunikasjonsteknologi, noe som gjør at politi og øvrig myndigheter er avhengig av at data blir lagret for oppklaring og bevisførsel i saker. Flere europeiske land har innført pålegg om lagring mellom ett og to år av trafikkdata for selskaper som tilbyr mobil- og fasttelefon, e-post, SMS, chat-rom, Internett og annet elektronisk kommunikasjonsutstyr. SSB gjennomførte i 1997 en spørreundersøkelse som viste at blant de spurte var det 68 prosent som mente at kriminalitetsbekjempelse og oppklaring av kriminelle handlinger var viktigere enn hensynet til personvern (SSB, 1997).

Trafikkdata er grunnlaget for fakturering av tjenester og inneholder data om brukerens elektroniske kommunikasjon som kan oppfattes som sensitive. Trafikkdata i Norge skal slettes etter 3-5 måneder avhengig av faktureringsperiode. Økokrim ønsker derimot at det skal pålegges utvidet lagringsplikt (Sunde, 2000). Gjennom utvidet lagring av trafikkdata vil politiet få mulighet til å finne beviser og spor bakover i tid og således bedre sin mulighet til finne spor fra planleggingen av en kriminell handling. Etterforskerne har dermed fått et nytt etterforskningsmiddel som ikke har vært tilgjengelig i den fysiske verden. Men når politiet får adgang til å anvende disse opplysningene vil det også omfatte den vanlige bruker og informasjon om brukeren som ikke hadde vært tilgjengelig i den analoge verden, noe som vil utfordre personvernet.

Vi spurte deltakerne om hva de syntes om en eventuell utvidet lagringstid for trafikkdata. De fleste aksepterte en utvidet lagringstid fordi den ble vurdert som nyttig i forbindelse med oppklaring og bevisføring i kriminalsaker. Forutsetningen hos deltakerne for en utvidet lagringstid av data var at kun autoriserte personer skulle ha tilgang til dem, at trafikkdata ble ivaretatt på en forsvarlig måte. Noen nevnte også at politiet måtte ha rettskjennelse ved eventuelle innsyn.

De unge deltakerne var åpne for at trafikkdata for deres mobil- og Internettbruk kunne lagres i ett år. De mente at så lenge det kunne være til nytte for oppklaring eller bevis i kriminalsaker veide dette tyngre enn risikoen ved at deres trafikkdata ble liggende lengre. Flere av deltakerne nevnte Baneheiasaken og Grysaken som et eksempel på en sak hvor det var behov for lagrede trafikkdata.

Også deltakerne mellom 30-40 år mente at utvidet lagringstid var akseptabelt ut ifra hensynet til bistand for politiet. De voksne begrunnet synet sitt ut i fra hensynet til trygghet i samfunnet til tross for at flere av dem understreket at de ikke følte seg helt komfortable med at andre enn politiet kunne ha innsyn i deres trafikkdata, for eksempel utro tjenere i telefonselskapene.

"Jeg synes at det skal være veldig strenge kriterier på bruken av informasjon, det må ikke bli et kontrollsamfunn. Det må være sånn at det er en spesifikk etterforskergruppe som skal bruke den informasjonen. De må være strenge på det" (Gutt, Bodø)

"Nei, ikke at de (politiet) misbruker det, men at andre kan gjøre det. Jeg er ikke så sikker på det" (Kvinne, Oslo)

Deltakernes positive holdning til utvidet lagringstid for trafikkdata tyder på at de har tillit til at myndighetene opptrer korrekt i denne type sammenheng. For å ivareta og opprettholde denne fortroligheten kreves det at det ikke forekommer unødvendig innsyn. En utvidet lagringstid er ikke kun avhengig av tillit til myndighetene og politi, men er også betinget av at teleoperatørene og internettleverandørene selv ivaretar tiltroen.

2.6.2 Uregistrerte kontantkort

I dag er det tillatt å ha mobiltelefoner med uregistrerte kontantkort. Det vil si at kontantkortene ikke er registrert hos forhandler og dermed vil telefonen ikke kunne spores til en person. På den måten har man anledning til å bruke mobiltelefonen anonymt. Det foreligger imidlertid et forslag fra Økokrim om at dette skal forbys for å nettopp unngå at man har anonyme mobilabonnementer som kan være en kanal for kriminelle til å opprettholde og fortsette sin virksomhet (Sunde, 2000).

Deltakerne ble spurt om hva de syntes om dette forslaget til forbud av uregistrerte kontantkort. Det viste seg at blant deltakerne var det fire som hadde uregistrert mobiltelefon, hvor tre av dem var ungdommer. Den generelle holdningen blant deltakerne var at så lenge man førte et normalt liv så hadde man ikke behov for uregistrert kontantkort. Men samtidig ble det også uttrykt at det nødvendigvis ikke var akseptabelt å gå så langt som å forby det.

De unge deltakerne mente at det burde være lov til å ha uregistrerte kontantkort selv om man ikke hadde et prekært behov for å være anonym. De påpekte at ved en gjennomføring av en lovregulering kunne det oppleves som overformynderi.

Blant de voksne deltakerne var det ulike oppfatninger om uregistrerte mobiltelefoner. Noen av dem mente at så lenge man ikke hadde noe å skjule så hadde man heller ikke behov for mobiltelefon med uregistrert kontantkort. Men noen av de andre voksne deltakerne mente at det fremdeles burde være lov til å ha uregistrert kontantkort ut fra hensynet til den enkeltes rett til å selv bestemme om man vil være anonym. Det ble også argumentert for at dette kunne berøre enkeltindividets ytringsfrihet i sårbare grupper. Et eksempel som ble trukket fram var anonyme presseinformanter.

> *"Jeg synes at det skal være mulig å være anonym, også på Internett. Jeg synes at det skal være lov til å ha uregistrerte telefoner" (Gutt, Bodø)*
>
> *"Det er jo en av tingene som forsterker muligheten for kontrollsamfunnet, selv om Norge i dag er bygd på sikkerhet og trygghet så kan det jo være at det går i feil retning" (Gutt, Bodø)*
>
> *"Hvorfor skal man være så anonym? Hvis man ikke har noe å skjule, er det er jo kriminelle som benytter seg av sånt" (Kvinne, Oslo)*

Under diskusjonene blant de unge deltakerne ble det etterlyst mer informasjon om elektroniske spor. Ungdommene understreket også at som bruker av teknologi var man selv ansvarlig når man etterlot spor, men de etterlyste også informasjon fra myndigheter og leverandører av kommunikasjonsteknologi. Det ble også diskutert hvem som har ansvaret for å ivareta personvernet. Her var det en klar oppfatning blant deltakerne om at det først og fremst var brukeren selv som hadde ansvar for hvor man la igjen informasjon. Men det ble også påpekt at staten i større grad burde gi informasjon til brukerne om hva som kunne true personvernet og ha klare retningslinjer for hvordan man kunne kreve innsyn i trafikkdata. Deltakerne etterlyste også informasjon fra leverandørene om hvordan

teknologien fungerte og hvordan man i større grad kunne beskytte seg selv, eksempelvis informasjon om hvordan man kan slette cookies.

> *"Etter den samtalen som vi har hatt her i dag ser man at det er mye vi ikke har vært så bevisste på, men som kan misbrukes, selv om vi er personer som ikke er så interessante for samfunnet. Men det er jo informasjon som handler om oss" (Gutt, Bodø)*

> *"Jeg tenker mest på at det burde være mer informasjon om dette her, hva som kan skje når man bruker denne teknologien. Jeg har en følelse at ikke alle vet noe eller nok om dette" (Jente, Bodø)*

Mangelen på og behovet for generell informasjon om elektroniske spor ble også etterlyst i lekfolkenes dokument da det danske Teknologirådet gjennomførte en konsensuskonferanse om elektronisk overvåking i 2000. I sitt sluttdokument anbefalte lekfolkspanelet at det skulle gis mer informasjon til brukerne om problemet med sikkerhet i forbindelse med Internett, e-post og mobiltelefon. Gjennom deltakelsen i fokusgruppene ble deltakerne mer bevisst på personvernmessige utfordringer ved bruk av IKT.

Men en av de unge utrykte seg imidlertid slik til slutt;

> *"Jeg er kanskje blitt mer bekymra nå, men om ei uke har det nok gått over" (Jente, Oslo)*

3. Avslutning

Denne rapporten er basert på samtaler i seks fokusgrupper med til sammen 48 tilfeldig utvalgte deltakere, hvor det ble diskutert bruk av mobiltelefon og Internett og de konsekvenser dette kan ha for personvern. Det sier seg selv at et slikt datagrunnlag ikke gir et statistisk grunnlag til å hevde at dette er representativt for befolkningen. Men de seks gruppesamtalene gav likevel et interessant innblikk i hvordan lekfolk tenker omkring personvern og bruk av IKT.

Resultatene fra fokusgruppene bygger opp under den oppfatning at de fleste unge i stor grad har høy brukerkompetanse av mobiltelefon og Internett. Litt overraskende var det derfor å registrere at kunnskapen om elektroniske spor var ganske lav blant de unge. Man kunne vente at tastegenerasjonens brukerferdigheter også innebar kunnskap om hvilke spor teknologibruken setter og hvordan man kan bruke teknologien til å minske mengden av dette. Hos de voksne deltakerne var inntrykket at kunnskapsnivået var mer varierende.

Årsakene til at ungdommene hadde såpass lite kunnskap omkring elektroniske spor kan være flere, men en mulig sammenheng kan være deres lave bevisstheten omkring personvern. Ingen av dem hadde opplevd noe alvorlig misbruk av sine personopplysninger, og det kan derfor være grunn til at man vurderer elektroniske spor som en mer abstrakt fare. Bekymringsløshet kan også være en annen mulig årsak som på mange måter er det utvilsomt en god ting, men som kan også gjøre de unge ekstra sårbare. Likefullt var det mange av deltakerne i vår undersøkelse som understreket behovet for mer informasjon fra myndighetenes side og leverandørene om elektroniske spor og hvordan man best mulig kan ivareta personvernet. Det er interessant å merke seg at verken blant ungdommen eller de voksne avdekket vi noen systematiske kjønnsforskjeller i forhold til kunnskap om bruk av teknologien eller om konsekvensene for personvernet.

Tradisjonelt har man vært vant til å tenke på myndighetene som den største potensielle trusselen mot personvernet og med private selskaper som håndterer store mengder personopplysninger på en god nummer to. Deltakerne hadde derimot stor tillit til myndighetene og til store, seriøse selskaper, men var på den annen side mer opptatt av faren for det vi kan kalle sivilt misbruk av personopplysninger, altså forårsaket av privatpersoner. Et generelt inntrykk fra samtalene var at det er i de nære ting at folk oppfatter reelle trusler mot personvernet.

En av de største utfordringene i forhold til personvernet i IKT-alderen er å tilpasse graden av identifikasjon til den aktuelle situasjonen. I forhold til mange tjenester på nettet er en korrekt og sterk identifikasjon av brukeren avgjørende. Men tjenester som f. eks å lese en artikkel på nettet er det derimot ikke rimelig å kreve en mengde personopplysninger av brukeren. I slike tilfeller er det en effektiv personvernstrategi å holde tilbake personlige opplysninger man ikke føler at leverandøren av den aktuelle tjenesten har saklig grunn til å be om.

Litteratur

Bing, Jon (1991):"*Handbook of legal information retrieval*" Norwegian Research Center for Computers and Law, Oslo, Norway

Bjørn Remseth og Thomas Gramstad: "*Kryptografi, kriminalitet og personvern*" Elektronisk Forpost Norge, notat nr. 1. http://www.efn.no/krypto-notat.html

Cranor, Lorrie Faith, Reagle, Joseph, and Ackerman, Mark S. (1999):" *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy"* AT&T survey: http://www.research.att.com/projects/privacystudy/

Coll, Line (2000): "*Innsyn i personopplysninger i elektroniske markedsplasser*" Institutt for rettsinformatikk. CompLex nr. 3/2000

Det danske Teknologirådet (2000): "*Sluttdokument for konsensuskonferansen om elektronisk overvåking, 01.12.2000*" http//:www.tekno.dk

Det danske Teknologirådet (2000): "*Overvåking på glidebane. Elektronisk overvågning uden grænser kan true brukernes retssikkerhed*" Nyhetsbrev fra det danske Teknologirådet. Nr. 150, desember 2000

Det danske Teknologirådet (2001): "*Total kontrol på Internettet. Terror er løftestang for at give politiet vide muligheder for at overvåge brukerne*". Nyhetsbrev fra det danske Teknologirådet. Nr. 166, januar 2001

Electronic Privacy Information Center (2002): "*Public Opinion on Privacy*" http://www.epic.org/privacy/survey/

Forbrukerombudet (2003): "*Nordisk undersøkelse av internettsider for barn og ungdom 2003*". Rapport fra de nordiske forbrukerombudenes undersøkelse av internettsider for barn vedrørende registrering av personopplysninger og skjult reklame

Forskningsmininsteriet. IT-sikkerhedsrådet (1998): "*Privatliv på Internett*" http://www.fsk.dk/fsk/publ/1998/privatliv/inde0005.htm

Frønes, Ivar (2002): "*Digitale skiller. Utfordringer og strategier*" Fagbokforlaget, Bergen

Hellevik, Ottar (1995): "*Sosiologiske metoder*". Universitetsforlaget. Metodebiblioteket

IDC (2003): http://www.idc.com/nordic/products/default.htm

Johnsen, Ben (2001): *"Kryptografi den hemmelige skriften; kryptografiens kulturhistorie fra år 0 til 2001"* Tapir Akademiske Forlag, Trondheim

Krueger, Richard A. (1998): "*Developing Questions for Focus Groups. Focus Group 3*" Sage Publications, International Educational and Professional Publisher

Krueger, Richard A. (1998): "*Moderating Focus Group. Focus Group 4*" Sage Publications, International Educational and Professional Publisher

Krueger, Richard A. (1998): "*Analyzing & Reporting Focus Group Results. Focus Group Kit 6*" Sage Publications, International Educational and Professional Publisher

Krueger, Richard A. & King, Jean A. (1997): "*Involving Community Members in FocusGroups. Fokus Group Kit 5*" Sage Publications, International Educational and Professional Publisher

Krueger, Richard A. & Casey, Mary Anne (2000): "*A practical guide for applied research*" Sage Publications. International Educational and Professional Publisher

Mey, Inger Lise (1996):"*Personregisterlovens anvendelse i et elektronisk betalingssystem*" http://www.jus.uio.no/iri/forskning/lib/rapporter/elektronisk_marked/personvern02.htm

SSB (1997): "*Holdninger til personvern. Elektroniske spor*" http://www.ssb.no/vis/emner/00/01/30/persvhold/main.html

SSB (2003):"*IKT i den norske husholdningen, andre kvartal, 2003"* http://www.ssb.no/emner/10/03/ikthus/. Publisert på nettet 06.11.03

Sunde, Inger Marie (2000): "*IKT-kriminalitet: Etterforskningsmetoder og personvern*" http://www.okokrim.no/aktuelt_arkiv/artikler/Etterforskniongmetoder_og_personvern.html

Tjøstheim, Ingvar & Solheim, Ivar, (2001): "*Nordmenns Internettbruk og e-handel*" Norwegian Computing Center. Rapport nr. 971, Oslo 2001 http://odin.dep.no/odinarkiv/norsk/dep/nhd/2001/annet/024101-990052/index-dok000-b-n-a.html

Wibeck, Victoria (2000):"*Om fokuserade gruppeintervjuer som undersökningsmetod"* Studentlitteratur, Lund, Sverige

Wollan, Camilla Julie (1999): *"Betaling via Internett. Et utvalg av juridiske problemstillinger"* CompLex 2/99. Tano, Aschehoug

Appendiks:

Metode

For å få fruktbare innspill og deltakelse fra den vanlige bruker valgte Teknologirådet å benytte seg av metoden fokusgruppe.

Om fokusgruppe

En fokusgruppe innebærer å samle en gruppe mennesker til å diskutere et spesifikt tema. Deltakerne i en fokusgruppe vil være en avgrenset gruppe med representanter for en bestemt målgruppe og som har ganske lik bakgrunn. Metoden gir dermed mulighet til å fange opp meninger fra flere målgrupper hvis man bruker flere fokusgrupper. I en fokusgruppe vil deltakerne få anledning til å diskutere seg imellom, og dermed utnytte dynamikken og interaksjonen i gruppen for å kartlegge bevissthetsgraden (Krueger & King, 1997, Krueger & Casey, 2000).

Det er ulike måter å avvikle fokusgrupper på. En måte kan være at man gjennomfører en samtale med flere forskjellige grupper. Den andre framgangsmåten innebærer at man møter den samme gruppen gjentatte ganger over en viss tid. Valg av prosess er avhenging av tema og formålet med prosjektet. Teknologirådet benyttet seg av den første framgangsmåten, altså flere ulike grupper. Bakgrunnen for dette var ønsket om å fange opp meninger og holdninger om personvern og elektroniske spor ut fra kjønn og ulike aldersgrupper.

Hvorfor fokusgruppe?

Fordelen ved å bruke fokusgruppemetoden er at denne type kvalitativ metode gir rom for refleksjon og diskusjon mellom deltakerne. Hensikten er å få frem holdninger og meninger hos individene. Styrken ved fokusgruppe er dens kompleksitet og uforutsigbarhet, og kan være et nyttig verktøy når man ønsker å få forklart bevissthetsgraden av et tema. Lik andre typer kvalitative metodebruk har også denne metoden ulemper. En av de er at fokusgruppemetoden har et begrenset antall deltakere og man må derfor være forsiktig med å generalisere ut i fra utvalget (Hellevik, 1995).

Fokusgrupper kan være en nyttig metode for å få anledning til å undersøke nærmere hva som ligger til grunn for deltakernes synspunkter og få svar på ”hvorfor” spørsmålene. Videre gir fokusgruppe mulighet til å se hvilke spørsmål deltakerne mener er relevante i forhold til temaet. I en fokusgruppe tvinges deltakerne til å tenke og formulere seg, og kan gi dybde og kontekst til meninger, tanker og erfaring (Krueger & King, 1997, Wibeck, 2000). På den måten kan fokusgrupper gi rom for tolkning og forståelse for hvorfor ting er som de er. Fokusgruppe blir en prosessbasert metode hvor deltakerne kan endre eller utdype sine holdninger og synspunkter underveis på grunn av diskusjon med de andre deltakerne eller på grunn av informasjon.

Under fokusgruppene benyttet vi som moderatorer oss av en intervjuguide hvor vi diskuterte de samme temaene for hver gruppe. Dette var en forutsetning for å kunne sammenlikne gruppene i analysen.

I en kvalitativ metode med et lite utvalg har man begrenset mulighet til å generalisere, men det er heller ikke mål i denne sammenheng. Vi ønsket å få tak hva den vanlige bruker mente om elektroniske spor ved bruk av informasjons- og kommunikasjonsteknologi.

Deltakerne/utvalg
Høsten 2003 gjennomførte Teknologirådet seks fokusgrupper med åtte deltakere i hver gruppe. Å ha åtte deltakerne i en fokusgruppe er hensiktsmessig for å ikke miste oversikten og gir mulighet for at alle deltakerne skal kunne komme til orde (Krueger & King, 1997, Krueger, 1998). For å få homogene grupper ble deltakerne inndelt etter alder og kjønn. Dette for å ha mulighet til å avdekke eventuelle forskjeller i holdninger ut i fra alder og kjønn. Det betyr at deltakerne er fordelt i to ulike aldersintervaller, hvor deltakerne i fire av gruppene er mellom 17 til 19 år (De unge) og deltakerne i de to andre gruppene er mellom 30 til 40 år (De voksne).

Grunnen for å dele gruppene etter kjønn var at det tradisjonelt sett har vært og er forskjeller mellom kjønn og teknologi. Det gjelder både bruken og det å forholde seg og tilnærme seg teknologi (Frønes, 2002). Selv om det i dag er jevnere forhold mellom kjønn ved bruk av mobiltelefon og Internett ønsket Teknologirådet likevel å benytte seg av disse variablene for eventuelt å kunne avdekke likheter eller ulikheter om temaet.

Deltakerne er fra to ulike plasser i Norge, Oslo og Bodø. To av de fire ungdomsgruppene ble gjennomført i Bodø, mens de resterende fokusgruppene ble foretatt i Oslo.

Temaet personvern og elektroniske spor forutsatte at de som ønsket å delta anvendte mobiltelefon og Internett aktivt. Det bør også understrekes at utvalget er tilfeldig, men ikke nødvendigvis representativt.

Ungdom og IKT
Teknologirådet valgte å gjennomføre fire av de seks fokusgrupper med ungdom i aldersgruppen 17-19 år. Grunnen for at hovedfokuset ble rettet mot denne aldersgruppen var at denne aldersgruppen er vokst opp med kommunikasjonsteknologi, og er den største gruppen av mobileiere i Norge. Blant gruppen 16-24 år ligger antallet mobilbrukere på 99 prosent (SSB, 2003).

Internett er også blitt viktig for denne aldersgruppen, hvor 79 prosent av ungdommene har Internett hjemme (SSB, 2003). Ungdom adopterer rask ny teknologi og nye trender og tilegner seg den tekniske kunnskapen kjappere enn andre aldersgrupper (Frønes 2002). Vårt utgangspunkt var at vi trodde ungdommene ville inneha stor brukerkunnskap om teknologi. Det kan det derfor være interessant å se nærmere på deres holdninger og bevissthet til elektroniske spor og personvern.

Voksne og IKT
Deltakerne i to av fokusgruppene var i alderen 30-40 år og bosatt i Oslo. Årsaken var at denne aldersgruppen *ikke* er vokst opp med egne mobiltelefoner eller Internett. Denne aldersgruppen har likevel blitt store forbrukere av IKT (Informasjons- og kommunikasjonsteknologi) både i jobbsammenheng og privat, og har gradvis utviklet sin digitale kompetanse. I aldersgruppen mellom 25 til 44 år har 98-99 prosent mobiltelefon (SSB, 2003). Sammen med ungdomsgruppen utgjør de største gruppene av mobilbrukere i Norge. Tall om Internettbruk viser at i aldersgruppen 25 til 44 år ligger prosenten mellom 72-76 av de som har adgang til Internett. Vi hadde en antagelse om at aldersgruppen 30-40 år i større grad skulle være opptatt av personvern enn de yngre deltakerne. Dette var basert på tanken om at økt livserfaring gir evne til å vurdere risiko på en annen måte enn det ungdom gjør. Det kan derfor være interessant å se nærmere på disse to gruppene i forhold til hverandre. Det kan være rimelig å anta at de voksne hadde mindre nærhet til teknologi og mindre tillit til teknologi enn det ungdom har.

Analyse

Det er ingen fasit for hvordan man skal analysere et kvalitativt utvalg, selv om det fins noen retningslinjer. Analysen innebærer en presentasjon gjennom en oppsummering av data, som ikke er en nøytral gjengivelse, men en fremstilling av materialet slik vi oppfatter det (Krueger & King, 1997, Krueger, 1998). Samtalene er skrevet ut fra opptak og er sammen med notater grunnlaget for analysen. Intervjuguiden som ble brukt under diskusjonene er selvfølgelig lik for alle gruppene og ble et viktig element for etterstrebelse av validitet.

En analyse av data basert på fokusgruppe handler om å kode materialet, se etter mønstre og sammenhenger og dele dataen opp i enheter. Analysen kan derfor inneholde både det typiske og det avvikende hos deltakerne, og kan presentere flere forklaringer hvis det er ulike oppfatninger rundt temaet. De forskjellige fokusgruppene blir sammenliknet i analysen, men også deltakerne innad i en gruppe (Krueger & King, 1997). Analysen vil av den grunn inneholde hovedfunn, deretter spesifiserte funn ut i fra alder og kjønn. Vi har også valgt å bruke sitater som belyser meningene som kom fram under samtalene.