Teknologirådets høring om IKT & personvern

Bakgrunn

Norsk Regnesentral har et strategisk instituttprogram finansiert av forskningsrådet hvor vi jobber med løsninger på ulike problemstillinger innen personvern. Vår hovedtese er at det er mulig å designe tekniske løsninger, og prosesser og rutiner som ivaretar personvernet for den enkelte på en tilfredsstillende måte, samtidig som man kan utnytte personinformasjon til å lage nyttige, personaliserte tjenester. Vårt utgangspunkt er at vi har et lovverk som skal håndheves, samt at det i størst mulig grad skal gis anledning for den enkelte til å kontrollere sitt eget personvern. Dvs. at man i stor grad skal ha mulighet til selv å velge hvilke personopplysninger man vil gi fra seg til hvem, og hva disse opplysningene senere kan brukes til. Dette er bakgrunnen for våre svar på de spørsmålene Teknologirådet stiller i sin høringsinvitasjon.

Svar på Teknologirådets spørsmål

1) *Nyter norske borgere i sin nye IKT-hverdag tilstrekkelig personvern, eller har teknologien løpt fra personvernet slik at noe må gjøres for å styrke det?*

Definisjonen av ”tilstrekkelig personvern” vil sannsynligvis variere fra person til person, og fra situasjon til situasjon. I Norge synes folk generelt å være skeptiske til hva private bedrifter kan foreta seg med informasjonen de samler inn, mens man f. eks. i USA er mye mer bekymret for hva myndighetene kan finne på. Vi tror ikke det umiddelbart er noen stor trussel mot personvernet for folk flest, men det er en gradvis økning i presset mot personvernet som må bremses før det går for langt.

Spør du folk om de er bekymret for personvernet, eller om de ønsker et sterkt personvern, vil de aller fleste svare ja. Men ser man på hva folk faktisk gjør i ulike situasjoner, så får man et annet inntrykk. Hvis man må velge mellom beskyttelse av personinformasjon, eller å få en vare eller tjeneste man ønsker eller trenger, vil svært mange velge det siste. I mange tilfeller har man ikke egentlig noe reelt valg. Det gjelder kanskje særlig i forhold til offentlige tjenester, eller tjenester man er avhengige av for å få gjort jobben sin.

Hvis vi skal legge personopplysningslovens intensjoner til grunn for definisjonen av et tilstrekkelig personvern, så kan man i mange tilfeller hevde at spørsmålsstillingen er feil: Det er faktisk personvernet som har løpt fra teknologien, og ikke omvendt. Lovverket gir en rimelig sterk beskyttelse av personvernet, men dagens IKT-systemer gir dårlig støtte for etterlevelse av dette lovverket. For eksempel er det et problem for mange organisasjoner å håndtere en økende strøm av innsynsbegjæringer. Resultatet av dette er at det er mange tjenester som ikke er mulig å tilby fordi man ikke har IKT-systemer som muliggjør etterlevelse av lovverket.

2) *Hvilke er de alvorligste IKT-relaterte truslene mot folks personvern i dag?*

Det er etter vårt syn to hovedproblemer. Det første er at det samles inn og produseres stadig større mengder informasjon som kan knyttes til individer. Mye av denne informasjonen er samlet inn unødvendig, men eksistensen av den gjør det meget fristende å utnytte den til ulike andre formål.

Det andre hovedproblemet er at det er altfor vanskelig for individer å utøve den kontrollen over sitt eget personvern som personopplysningsloven legger opp til. Dette skyldes at det er

svært vanskelig å få oversikt over hvilke systemer som faktisk lagrer personinformasjon og hvilken type informasjon de lagrer, samt at systemene stort sett er meget dårlig tilrettelagt for at individer skal kunne utøve noen form for kontroll.

Som nevnt ser vi et stadig økende press mot personvernet. Vi vil her peke på noen eksempler på dette:

- Skattelistene og andre offentlige registre lagt tilgjengelig på Internett muliggjør meget effektive søk og aggregering av informasjon om enkeltindivider. Identitetstyverier for svindelformål er et konkret eksempel på misbruk av informasjon samlet inn på denne måten. Dette er et stort problem i USA og Storbritannia, og det er rapportert om flere tilfeller i Norge også.
- Outsourcing av tjenester (f.eks. CRM- eller økonomisystemer) blir stadig vanligere. Den som leverer slike tjenester til flere kunder har en unik mulighet til å samle personinformasjon fra mange ulike kilder. Konkrete eksempler her er "web bug"-problematikken fra blant annet DoubleClick-saken i USA for en tid tilbake, og som også ble oppdaget hos SAS og deres leverandør SCD nylig. Hvis slik outsourcing skjer over landegrenser og kanskje i flere ledd, kan ansvarsforholdene fort bli uklare.
- I de fleste bransjer er det en utvikling mot stadig færre, men større, selskaper, noe som gjerne innebærer sammenkobling av datasystemer og databaser. Dette skjer også på tvers av tidligere separate bransjer, som f.eks. bank og forsikring. Dermed samles mye makt og mye informasjon hos noen få aktører.
- Lokasjonsbaserte tjenester antas å bli svært utbredt, og åpner helt nye muligheter for å spore individer og bygge opp profiler av hva de gjør. Lokasjonsinformasjon for svært mange individer finnes allerede i dag i mobilnettene, men vil få et langt større omfang og nøyaktighet når andre teknologier for trådløs kommunikasjon tas i bruk i større grad enn i dag.
- Det er et uttalt ønske om å få integrert flere av de offentlige etatene slik at man får færre kontorer å forholde seg til. Dette vil utvilsomt være nyttig for brukerne, men kan også føre med seg nye trusler mot personvernet. Mer om dette under punkt 5).
- Det er velkjent at angrep fra "insidere" ofte utgjør den største trusselen. Selv om organisasjonen som har ansvaret for et lager med persondata ikke har uærlige hensikter, så kan man ikke forvente at alle dennes ansatte er like mye til å stole på. Mangelen på beskyttelsestiltak mot utro ansatte er en av de alvorligste truslene når stadig mer informasjon lagres.
- Mengden av overvåkingskameraer er sterkt økende. Det gjelder både de "offisielle" kameraene hvor det er satt opp skilt om kameraovervåking, men også personlige web-kameraer og etter hvert også kameraer på mobiltelefoner. Ikke minst det siste gjør kontroll med videoovervåkingen svært vanskelig.

3) *Hva er viktigst for å sikre personvernet mot potensielle trusler fra ny IKT?*

   - *Tiltak på lov- og regelsiden?*
   - *Aktiv bruk av teknologier som kan styrke personvernet?*
   - *Tiltak for å bidra til personvernfremmende atferd fra brukernes side?*
   - *Andre ting?*

Lover og regler er et meget viktig fundament for å sikre personvernet. Vi mener at dagens lovverk er et godt utgangspunkt, men det må selvsagt holdes oppdatert i takt med teknologiutviklingen. Det kan også være en mulighet å bruke lover og regler til å fremtvinge forbedringer i teknologien, slik at man kan styre utviklingen i riktig retning. Lovverket

fastslår hvilke rettigheter hver enkelt har i forhold til personvern. Det er imidlertid viktig at kontrollen av hvorvidt lovverket etterleves blir styrket. Det er sannsynligvis mulig å få til mer automatisering av denne typen overvåking og kontroll, slik at f.eks. Datatilsynets aktivitetsnivå kan økes.

Vi har stor tro på at teknologiske løsninger kan styrke personvernet, men en kritisk suksessfaktor her vil være slike systemers brukervennlighet. Det må ikke være vanskeligere å bruke personvernfremmende teknologi enn å bruke tilsvarende, mer personvernfiendtlige, løsninger. Det beste, og sannsynligvis eneste virkelig effektive, tiltaket for å bidra til personvernfremmende adferd, er å sørge for at "default" alltid er personvernvennlig, dvs. at man må gjøre noe aktivt for å svekke personvernet i en gitt sammenheng. Prinsippet om "opt-in" i stedet for "opt-out" ligger allerede til grunn i lovverket, men det finnes mange unntak. Prinsippet etterleves heller ikke i noen større utstrekning, noe som muligens mest skyldes manglende teknologistøtte.

Det er viktig at både privat og offentlig sektor tar ansvar i forhold til personvern. Når et nytt system eller en ny prosess planlegges, eller gamle endres, bør virkningen på personvernet analyseres. Det er et viktig prinsipp i lovverket at man skal minimere mengden persondata som samles inn, og det er et forbud mot lagring av persondata som ikke er nødvendig for formålet. I Canada, hvor man har kommet meget langt på mange IKT-områder i det offentlige, er det et krav for alle offentlige systemer, og en betingelse for finansiering, at det først gjennomføres en slik analyse av virkningen på personvernet.

Økonomiske incentiver har som regel stor effekt ovenfor både private og offentlige aktører. Vi tror at aktiv beskyttelse av personvernet kan være et konkurransefortrinn. Det vi trenger, er noen som kommer på banen og tilbyr kundene virkelig gode innsynsmuligheter og beskyttelse av personvernet. En suksesshistorie på dette området vil lokke – eller tvinge – resten av privat sektor til å følge etter.

I de tilfellene hvor innsamling og lagring av persondata er nødvendig, finnes det mange typer mekanismer som kan redusere trusselen mot personvernet, f.eks. bruk av såkalte pseudonyme identifikatorer, eller mekanismer for automatisk håndheving av personvern policy. Systemer for enkeltpersoners innsyn i informasjon om en selv er viktige å få på plass, både for brukernes del og for å redusere ressursbruken ved håndtering av innsynsbegjæringer.

4) *Hvor viktig er det å ta vare på personvernet? I en situasjon med terrorfare og hvor elektroniske spor står sentralt i politiets etterforskning av de fleste former for kriminalitet – må vi gi avkall på noe av personvernet for å øke trygghetsnivået i samfunnet?*

Det å gi avkall på personvernet fører med seg andre alvorlige trusler, slik at det samlet sett ikke er sikkert at trygghetsnivået vil øke med slike tiltak som det her siktes til. Som nevnt er insidere ofte de vanligste og farligste angriperne. Kan vi si med noen som helst sikkerhet at trusselen fra utsiden (terroristene) er større enn trusselen fra innsiden (de ansatte, "systemet")? Kan vi sikre oss mot at terroristene samarbeider med folk på innsiden? Den økte informasjonsmengden som blir tilgjengelig hvis man lemper på personvernet kan også tenkes å gjøre angrep fra terrorister enklere, eller mer målrettede og effektive, hvis terroristene får tilgang til informasjonen. Det er mange vanskelige avveininger på dette området, men vi kan faktisk risikere at et dårlig personvern øker terrortrusselen, både mot enkeltindivider og mot samfunnet som helhet.

Når det er sagt, så bør man også se på muligheten for tekniske løsninger som tar hensyn både til personvernet og til behovet for overvåking. Overvåkingskameraer som automatisk skjuler ansikter, eller bruk av pseudonyme identifikatorer i logger, er eksempler på dette.

5) *Vil den digitale forvaltning stille spesielle krav til personvern for å kunne bli en suksess blant brukerne?*

Dette spørsmålet må vi svare et ubetinget ja på. Separering av data samlet inn for ulike formål er et fundamentalt prinsipp for personvern. Informasjon som alene ikke betraktes som særlig sensitiv, vil kunne bli sensitiv hvis den sammenstilles med annen informasjon. En hovedtanke bak den digitale forvaltning er jo nettopp at informasjon skal være tilgjengelig på tvers av (det som i dag er) ulike etater, for å oppnå effektivisering både for brukeren og etatene.

Særlig utenfor de store byene, hvor samfunnet er mer gjennomsiktig og folk i stor grad kjenner (til) hverandre, tror vi at folk generelt vil være skeptiske til at kommunalt ansatte kan innhente informasjon fra mange ulike registre.

Det er dessuten betenkelig at det i personopplysningsloven finnes så mange unntak fra de generelle prinsippene som kan gjøres gjeldende for offentlig forvaltning. Det er derfor essensielt at man tenker grundig gjennom både organisasjon, prosesser, rutiner og ikke minst de teknologiske systemene med tanke på beskyttelse av personvernet og bevaring av ”need-to-know”-prinsippet i forhold til de ansatte i forvaltningen.

Norsk Regnesentral

Ragni Ryvold Arnesen
Seniorforsker

Jerker Danielsson
Forsker