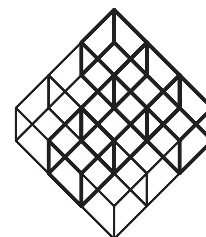


Fornyings- og
administrasjonsdepartementet
postmottak@fad.dep.no

Kopi: postmottak@nhd.dep.no



Teknologirådet

Vår ref.: 30.06/CH
Deres Ref.: 200600326-/EDK
Dato: 23. februar 2006

IKT og personvern

Teknologirådet er et uavhengig, rådgivende organ som skal vurdere den teknologiske utviklingen på alle samfunnsområder og stimulere til debatt om de muligheter og konsekvenser som ny teknologi skaper for samfunnet og det enkelte individ.

Teknologirådet har de siste årene engasjert seg i flere prosjekter som omfatter personvern i ulike sammenhenger. I 2005 publiserte vi rapporten *Elektroniske spor og personvern*, som gir en omfattende oversikt over teknologier som skaper elektroniske spor og tiltak man kan iverksette for å sikre personvernet, både for individer, bedrifter og offentlige myndigheter. For tiden er vi slutfasen av prosjektet *Offentlige tjenester på nett*, hvor personvern er et av de aspektene vi vurderer. Rapporten fra dette prosjektet vil bli publisert i mars 2006.

Teknologirådet er også engasjert i to europeiske personvernprosjekter. Det ene, EPTA Privacy, er et prosjekt som søker å sammenstille resultatene fra en rekke personvernrelaterte prosjekter hos 7 medlemsland i EPTA (European Parliamentary Technology Assessment). Dette arbeidet ferdigstilles første halvdel av 2006. Det andre prosjektet, PRISE, er finansiert av EU-kommisjonen gjennom PASR (Preparatory Action in the field of Security Research), og skal se på kriterier for å designe sikkerhetsteknologi på en personvernvennlig måte. Dette prosjektet startet i februar 2006 og skal løpe i 28 måneder. Innspillene i dette dokumentet er basert på resultater og erfaringer fra de nevnte prosjektene.

Offentlige IT-systemer og samordning av data

I arbeidet med å fornye offentlig sektor har det vært mye fokus på å øke den digitale utvekslingen av informasjon mellom etater og departementer – å "rive siloene" mellom de ulike IT-systemene i forvaltningen. En slik nedbygging av grensene mellom

Pb 522 Sentrum
0105 Oslo

Prinsensgate 18
Norway

T: +47 23 31 83 00
F: +47 23 31 83 01

www.teknologiradet.no
post@teknologiradet.no

systemene vil medføre en økt samordning av persondata, og en større mulighet for at saksbehandlere i ulike etater får tilgang på mer personlig informasjon enn det som er nødvendig. Sammenkobling av kunnskap medfører at man reelt får vite mer om en person, og kan være en trussel mot personvernet.

I dagens informasjonssystemer er det vanlig med en relativt grovkornet behandling av tilgangsrettigheter. 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.

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 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.

En av hovedanbefalingene fra det felleseuropeiske prosjektet EPTA privacy er at man alltid bør gjøre en analyse av personvernkonsekvensene, en såkalt Privacy Impact Assessment (PIA), når et nytt system skal utvikles eller et eksisterende redesignes. I det offentlige bør PIA være en forutsetning i alle anskaffelsesprosesser hvor systemene inneholder persondata.

Hva mener brukerne?

Samordning av data kan være en personverntrusel, men det kan ses på som et gode for brukeren. Rent praktisk kan det bety at man slipper å taste inn den samme informasjonen i mange ulike sammenhenger, og at man får mer korrekte data.

I forbindelse med prosjektet *Offentlige tjenester på nett* gjennomførte Teknologirådet en prosess hvor 3 ulike borgerpaneler møttes over tre kvelder for å diskutere konsekvenser ved offentlige tjenester på nett og e-forvaltning. Vi spurte borgerpanelene hvilken informasjon de synes det vil være greit at ulike offentlige kontorer og etater har felles. Det var bred enighet om at grunnleggende personinformasjon, som navn, adresse, sivilstatus og lignende, gjerne kunne være delt. I forhold til sensitiv informasjon, som helseopplysninger, ønsket de en svært restriktiv politikk i forhold til deling og samtykke.

Personvernet stiller også krav til at kvaliteten på de opplysninger om enkeltpersoner som legges til grunn for beslutningsprosesser, for eksempel i offentlig saksbehandling, er god. Det å kunne fremstå som et helt menneske foran forvaltningen (ikke bare som trygdemottaker, sosialklient el.l.) kan slik også betraktes som en del av personvernet. Dersom man har dette som utgangspunkt, kan det være ønskelig at ulike etater får utveksle informasjon. Et sentralt punkt blir da spørsmålet om samtykke. Teknologirådets borgerpaneler syntes det var viktig at de ble bedt om samtykke når en

etat ønsket data fra andre etater. Som et minstekrav mente de at man burde motta en melding når data ble utvekslet, på samme måte som man i dag gjør dersom noen har foretatt en kredittsjekk.

Gjennomsiktighet

Med gjennomsiktighet, eller transparens, mener vi innsyn i egne data og i hvordan saksgang og automatiserte beslutningsprosesser fungerer. En av hensiktene med MinSide, slik den presenteres i eNorge 2009, er at brukerne skal få tilgang til all den informasjonen det offentlig har samlet om dem. Denne formen for sammenstilling av informasjon er uproblematisk, og faktisk positiv fra et personvernperspektiv. Så lenge informasjonen hentes fra ulike, isolerte systemer, og kun sammenstilles for brukeren, i hans eller hennes nettleser, er det ingen andre enn brukeren selv som får oversikt over all den ulike informasjonen som finnes.

I Danmark har man gått langt i å gi kommunale virksomheter rett til å utveksle data uten å innhente spesifikt samtykke fra brukerne. Det danske Teknologirådet publiserte høsten 2005 sin rapport *Rettsikkerhed og aktivt medborgerskab i digital forvaltning*. I rapporten peker de på at det bør være en balanse mellom myndighetene og den enkelte borger når det gjelder å utnytte den digitale teknologien. Dersom myndighetene skal få utvidet tilgang til informasjon, gjennom samordning av data, må dette balanseres ved at borgeren også får utvidet innsynsrett: Den enkelte bør ikke bare få se sine egne data, men også få innsyn i hvem som har innhentet hvilken informasjon, hele saksgangen for sin egen sak – også internt i det aktuelle forvaltningsorganet, samt tilgang til logger over hvem som har opprettet, endret og aksessert hans eller hennes data.

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.

Identifikasjon og autentisering

I dagens samfunn blir det stadig vanskeligere å være anonym. Når man innfører en type sterk identifikasjon, slik som elektronisk ID, blir det i praksis ofte slik at man ber brukerne logge seg på (autentisere seg) på et mye tidligere tidspunkt enn det som i praksis er nødvendig. Det er et viktig personvernprinsipp å ikke kreve autentisering på et tidligere tidspunkt enn nødvendig.

Det er mulig å utvikle systemer som ikke krever autentisering på individnivå når dette ikke er påkrevd:

- 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.

Ta gjerne kontakt med undertegnede eller prosjektleder Christine Hafskjold dersom dere har spørsmål, eller ønsker mer informasjon om noen av de prosjektene vi har referert til.

Med vennlig hilsen

Tore Tennøe
Sekretariatsleder, Teknologirådet