Datatilsynet

Fornyings- og administrasjonsdepartementet
v/ Statsråden
Postboks 8004 Dep
0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	07/01251-1 /LTA	31. august 2007

E-forvaltning - Datatilsynets tilrådning til regjeringen

I de seneste år har det vært en rivende utvikling innen e-forvaltning. Denne trenden har vært sterk både i Norge og internasjonalt. De aller fleste, herunder Datatilsynet, synes det er en spennende og positiv utvikling. E-forvaltning bidrar til å gjøre demokratiet mer levende, informasjon bedre tilgjengelig og tilpasser i større grad tjenestetilbudet fra offentlig sektor til brukernes behov. En viktig forutsetning for personvernmyndigheten er imidlertid at samhandlingen skjer på en forsvarlig måte. Det må videre være en forutsetning at både tjeneste og informasjon gjøres tilgjenglig for rette vedkommende.

De offentlige virksomhetene i Norge sitter samlet sett på nærmest ufattelig mengder informasjon om innbyggerne. Omfanget strekker seg primært over tre dimensjoner; bredde, dybde og tid. Individet har i liten grad mulighet til å påvirke hvilke former for opplysninger som samles inn og lagres. Informasjonen er i stor grad samlet inn enten ved at det er stadfestet en plikt for borgeren til å stille informasjonen til rådighet, den offentlige virksomheten har journalplikt, eller har hjemmel til å hente informasjon fra andre kilder.

Når informasjonen først er samlet inn, vil offentlighetsloven i mange tilfeller bestemme spredning. Det innebærer at informasjonen i neste øyeblikk kan stilles til rådighet for allmennheten. Den registrerte innrømmes få eller ingen forebyggende rettigheter, og samtykke forutsettes sjeldent.

Når det gjelder innsyn etter offentlighetsloven har det så langt vært en viss terskel for at retten blir benyttet. Tersklene har gjerne bestått i at det har vært behov for å ta en telefonsamtale, sende et brev, telefaks eller e-post. Det har vært forventning om at forespørselen har vært konkret og knyttet til en spesifikk sak. Mulighetene for masseinnhøsting av opplysninger har vært sterkt begrenset. I all hovedsak, erfarer Datatilsynet, har retten til innsyn fungert i samsvar med intensjonen. Tilsynet legger da til grunn at offentlighetslovens intensjon ikke har vært å tilfredstille allmenn nysgjerrighet, men å innrømme borgeren rett til å føre kontroll med forvaltningen. Kjernen i den liberale rettstatens kontroll-filosofi er borgeres rett til å kontrollere fellesskapets institusjoner, ikke det offentliges adgang til å kontrollere det enkeltes rettssubjekt.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Trenden de siste år har vært å publisere informasjon, slik at de som ønsker det selv kan søke opp aktuelle saker. Begreper som "meroffentlighet" har vært benyttet også i denne sammenheng. Ikke bare gir forvaltningen innsyn på forespørsel, men har aktivt publisert informasjon til allmenn bruk og eventuell bearbeiding. Dette vil kunne gi utilsiktede og endog svært uheldige sideeffekter over tid. Datatilsynet vil spesielt trekke frem følgende bekymringer:

1. At mengden opplysninger som publiseres etter hvert blir så betydelig, og så lett tilgjengelig at utarbeidelse av profiler på enkeltindivider kan ha en kommersiell verdi. Nasjonal lovgivning vil være nytteløst i et slikt perspektiv, siden mediet er Internett.
2. At virksomheter utenfor landets grenser, herunder virksomheter som er hjemmehørende i land utenfor EØS, kan høste store mengder informasjon om nordmenn, mot disses vilje. Verken tilsynet eller andre europeiske myndigheter vil ha anledning til å håndheve rettigheter gitt i personopplysningsloven eller EU-direktivet.
3. At kraftige søkeroboter finner og systematiserer informasjon. Løsninger som benyttes i dag for å hindre slikt, for eksempel piktogram, vil kun ha en tidsavgrenset effekt.
4. At den enkle tilgang til personopplysninger offentlige etater har om nordmenn, kan gjøre Norge til et attraktivt område for kriminelle aktører som ønsker å utnytte svakheter i samfunnet og infrastrukturen. Det mest fremtredende eksempel er identitetstyveri i ulike former, som spenner over et vidt spekter.
5. At den allmenne tilliten til offentlig forvaltning kan bli varig svekket når befolkningen oppdager i hvor stor grad det offentlige gjør "tilgjengelig" informasjon om deres personlige forhold. Allment tilgjengelig informasjon kan systematiseres av uvedkommende, rett og slett fordi det kan eksistere betalingsvillighet for produktet. Det kan i så fall slå hard tilbake på forvaltningen om underlaget er hentet fra lett tilgjengelig materiale på etatenes hjemmesider.
6. At borgernes tillit til behandling av personopplysninger i det offentlige kan bli svekket om de erfarer at det offentlige tilgjengeliggjør opplysninger om dem og at dette er lett tilgjenglig via søkemotorene. Bruk av søkemotorer er allerede i dag benyttet for å danne seg et inntrykk av en person ved ansettelser og kredittgiving.
7. At den svekkede tillitt som kan oppstå, som nevnt i forrige punkt, kan medføre at borgeren vegrer seg fra å forholde seg til de offentlige aktørene og mer eller mindre bevisst kan undra informasjon av betydning for fellesskapet.

I liten grad synes de enkelte aktører i forvaltningen å ta helhetlige hensyn i sine vurderinger. I virksomhetenes betraktninger legges det ofte avgjørende vekt på snevre hensyn som intern effektivisering, hvor menneskene som tidligere vurderte begjæring om innsyn erstattes av servere som automatisk legger ut informasjon som skal være "offentlig". Samtidig forsvinner også tersklene som så langt har gitt et visst vern.

På sensommeren viste den såkalte "Tele 2-saken" problemstillingen i all enkelhet. Noen utvikler et dataprogram som produserte fødselsnummer som var matematisk korrekte. Listen med disse matematisk korrekte passord ble testet mot den offentlige portalen www.altinn.no. Etter vask på denne siden ble det kjørt et script (et lite dataprogram) mot nettsiden (nettbutikken) til Tele 2. Nevnte nettsted returnerte navn og adresse på alle fødselsnummer som er i bruk. Dette var mulig fordi selskapet har online tilgang til

kredittopplysningsbyråenes adresseregister. Et gyldig fødselsnummer var følgelig alt som var nødvendig for å innhøste:

- Tilknytning mellom et fødselsnummer og person
- Adresseinformasjon til vedkommende

Nylig mottok Datatilsynet melding fra nok en virksomhet som var utsatt for tilsvarende angrep som Tele 2 opplevde. I dette siste tilfellet ble det høstet inn tilsvarende data for i overkant av 60.000 mennesker. Til sammen innebære de to hendelsene at inntil 120.000 nordmenn kan være rammet. Datatilsynet har mistanke om at flere andre virksomheter har vært rammet av tilsvarende angrep. Tilsynet vet ikke hvilket motiv gjerningsmennene har hatt. I beste fall har motivet kun vært å påvise svakheter i systemet, i verste fall langsiktige kriminelle motiver.

De nevnte opplysningene er i seg selv ikke kritiske. Det at uvedkommende sitter på en unik, varig og entydig identifikator knyttet til navn, er imidlertid mer bekymringsfullt.

Det reiser seg da to problemstillinger sett fra et personvernperspektiv:

- Fare for illegalt marked for profiler på enkeltmennesker
- Det legges til rette for identitetstyveri

Det faktum at man sitter på en database, med en varig, unik, statsautorisert og entydig identifikator, gjør det lettere å addere tilleggsopplysninger over tid og således følge individet. Nettopp det var en av hovedårsakene til at offentlig forvaltning tok i bruk fødselsnummer. Tilsvarende vil gjelde i forhold til kriminelle aktører som ut fra sine behov ser tilsvarende fordeler.

Identitetstyveri handler fremfor alt om å samle relevant informasjon om offeret. Desto større mengder informasjon, desto større sjanse for å lykkes. Informasjonen brukes i en tidlig fase først og fremst på to måter, enten for å manipulere offeret til å gi ytterlig informasjon eller til å skaffe seg tilgang til ny relevant informasjon virksomheter måtte ha om vedkommende.

En metode som har vært fremholdt som vanlig i forbindelse med identitetstyverier har vært å omadressere post. I Norge har det inntil nylig vært et lavterskeltilbud for å endre postadresse. Kun tilgang til fødselsnummer og eksisterende postnummeradresse var nødvendig for en slik omadressering.

Innhøsting av personopplysninger kan også ha andre, mer marginale sideeffekter. Disse vil imidlertid ikke bli drøftet her.

1.1. Første tilrådning: Hindre bruk av fødselsnummer og andre varige entydige identifikatorer i offentlige portaler

Fødselsnummer har aldri vært ment å benyttes som brukernavn ved samhandling på nettet. Det å utvikle alternative brukernavn som er unike, krever noe innsats, men prioriteres ikke. I stede misbrukes, etter tilsynets vurdering, fødselsnummeret for slike formål.

For det første konstaterer Datatilsynet at fødselsnummer til en viss grad benyttes som erstatning for gyldig legitimasjon. På denne måten sedimenteres inntrykket av at kjennskap til dette nummeret alene har egenverdi for identifisering.

For det annet, problemet med varige, unike identifikatorer er at disse vanskelig lar seg skifte ut. I beste fall er dette særlig byrdefullt for den som ønsker dette, i verste fall lar det seg ikke gjøre. Selv en person som har vært utsatt for identitetstyveri vil neppe få muligheter til bytte sitt fødselsnummer, jf. sommerens Tele 2 sak.

For det tredje konstaterer tilsynet at noen offentlige portaler, som benytter fødselsnummer i sine løsninger, "svarer" på om det er et gyldig fødselsnummer som tastes inn. Dette er svært uheldig og bidrar til at uvedkommende kan vaske lister for å få gyldige numre.

I tilsynets dialog med "Min Side" ble det drøftet andre former for identifikatorer enn fødselsnummer. Interne utredninger i prosjektet konkluderte, i likhet med i mange andre prosjekter, at det ikke var hensiktsmessig. Nevnte prosjekt ente dermed opp med bruk av fødselsnummer som en midlertidig løsning.

Tilrådning 1:
Tilsynet tilrådning er at departementene skjerper kravene ovenfor underliggende etater i forhold til bruk av fødselsnummer på portaler. Tilsvarende bør det tas initiativ ovenfor statsforetakene, kommunal sektor og de kommunale foretak. Det bør også legges strenge føringer mot bruk av varige entydige identifikatorer generelt, herunder bruk av biometriske data.

1.2. Andre tilrådning: Kritisk vurdering av hva som skal publiseres og hvordan

Datatilsynet har merket seg at stadig flere offentlig aktører melder seg i iveren etter å publisere informasjon de måte ha om borgeren, det være seg korrespondanse, registerinformasjon eller saksbehandling om vedkommende. Dette skjer naturligvis kun på de områder hvor informasjonen ikke er beskyttelsesverdig etter annet lovverk og at offentlighetsloven kommer til anvendelse. Likevel er det svært omfattende. I Datatilsynets og Personvernnemndas årsmelding for 2004 (side 28) heter det:

"Det er naturleg, og i dei fleste samanhenger også rett, et ein også i offentlig sektor tek i bruk ny informasjonsteknologi for å effektivisere og rasjonalisere sine samhandlingsprosessar og samhandling med publikum.

Likevel vil Datatilsynet minne om at stat og kommune ikkje einsidig kan leggje vekt på ideal frå privat sektor og etablere løysingar som verkar formålstenlege ut frå reine effektivitetsomsyn. Sjølv om offentlege etatar, på same vis som privat sektor, driv utstrekt tenesteyting, driv det offentlege også ein ikkje uvesentleg grad av makt- og myndigheitsutøving. Det offentlege må derfor, i tillegg til økonomisk rasjonalitet, også leggje vekt på omsyn til rettstryggleik, personvern og medverknad for alle delar av befolkninga. Det er i siste instans opp til dei øvste politiske styresmakter å vege effektivitetsomsyn opp mot slike grunnleggjande rettar."

Datatilsynet har forståelse for ønsket om å gjøre offentlig informasjon tilgjengelig, men er svært kritisk til at dette gjøres på en slik måte at den enten kan innhøstes eller gjøres tilgjengelig åpent via Internett uten begrensninger. I begge tilfeller aktualiseres også problemstillingen som har å gjøre med utlevering til tredjeland. Det kan i så fall være en krenkelse av borgerens rettigheter etter det europeiske personverndirektivet.

Det synes åpenbart at visse former for personopplysninger er mer utsatt enn andre når det gjelder fare for kommersialisering og som underlag for identitetstyveri. Datatilsynet mener således at det kunne være hensiktsmessig å vurdere en gjennomgang og differensiering i forhold til hvor liberale forvaltningen skal være med aktiv publisering av ulik form for informasjon. Artikkel 29 (Data Protection Working Party), som er satt sammen av representanter fra de europeiske personvernmyndighetene, anvender et slikt prinsipp i et arbeidsdokument om differensiering i forhold til helseopplysninger. Tilsvarende tankegang kan trolig anvendes også i denne sammenheng.

I Norge skjer det også annet arbeid som har relevans. Datatilsynet bistår gruppen under departementet som arbeider med tilrettelegging for elektroniske postjournaler. Nevnte gruppe ser imidlertid kun på et mindre aspekt av nevnte problemstilling. Datatilsynet har for eksempel også mottatt henvendelse fra Brønnøysundregistrene hvor det bes om tilsynets syn på å legge ut deler av etatens registre på nettet, søkbart på person/fødselsnummer. Datatilsynet har i tilsvar advart mot dette. Tilsynet mener at en del typer offentlig informasjon ikke bør være tilgjengelig på Internett. Saken illustrerer imidlertid behovet for politiske føringer i saker av denne type.

Tilrådning 2:
Departementet rådes til å trekke opp konsise retningslinjer for ønsket utvikling med hensyn til hvilken form for "offentlig informasjon" det er ønskelig skal aktivt publiseres på nettet, herunder hvordan hensynet til individets personvern kan forenes med ønske om offentlighet.

1.3. Tredje tilrådning: Elektronisk ID

Tjenestespekteret som tilbys fra offentlig og privat sektor innebærer behov for en kontroll av identitet. Dessverre har ikke arbeidet med e-ID gått like raskt som utvikling av tjenestespekteret. I brev av 14. januar 2004 (kopi vedlagt) til daværende justisminister Einar Dørum, med gjenpart til daværende moderniseringsminister Morten Meyer, tar tilsynet opp betydningen av nevnte problemstilling. Man kan langt på vei hevde at det har oppstått et slags

vakuum som fylles med mindre gode løsninger. Formålet med e-ID er å gi en tilstrekklig god garanti for at rette vedkommende gis tilgang til informasjon og tjenester.

Datatilsynet tror de fleste har forståelse for at den som etterspør en tjeneste eller personopplysninger må kunne sannsynliggjøre at han er rette vedkommende. Hvordan dette skal gjøres er imidlertid et åpent spørsmål.

Datatilsynet vil presisere at utgangspunktet må være at identifisering først skjer når det eksisterer et reelt behov. Med det mener tilsynet at individet søker tilgang til informasjon som er beskyttelsesverdig og hvor vedkommende har legitim rett til innsyn eller å foreta en disposisjon. Dersom borgeren kun er ute etter generell informasjon fra forvaltningen bør dette kunne gjøres uten at ovennevnte instrumenter benyttes.

Det som preger mye at bildet i dag er at den enkelte sitter på et brukernavn, et passord og i noen tilfeller engangskoder eller passordgenerator. Slike løsninger kan være tilstrekkelige i forhold til noen kortsiktige formål, men er overhode ikke egnet i et lengre perspektiv. Det er et stort problem at passord gjenbrukes, at de sjeldent byttes ut og at de ikke allment kan trekkes tilbake. Dersom noen skulle få tilgang til en dårlig sikret base over passord er det stor sjanse for at informasjonen kan misbrukes overfor andre virksomheter.

Datatilsynet er naturligvis kjent med departementets arbeid med en revidert utgave av sikkerhetsportal. Tilsynets synspunkter bør være vel kjent for departementet fra forrige runde. Denne sikkerhetsportalen vil imidlertid, etter det tilsynet erfarer, uansett begrense seg til samhandling ovenfor offentlig sektor.

Tilrådning 3:
Departementene og de underliggende etatene bør stille seg i første rekke av aktører som tilstreber bedre og mer moderne løsninger for sikker samhandling på nettet. I praksis innebærer dette at etatene arbeider for aktiv bruk av e-ID og e-signatur. Parallelt bør det trekkes opp retningslinjer som sikrer at identifisering kun skjer når det er reelt behov for sådan. Det anbefales også at det arbeides for en mer allmenn bruk av e-ID. På den måten vil også tjenester med mindre behov for beskyttelse benytte slike instrumenter.

Med hilsen

Georg Apenes
Direktør

Vedlegg: Brev til tidligere justisminister Odd Einar Dørum av 14. januar 2004

Kopi m/ vedlegg: Det kongelige justis- og politidepartement
Personvernkommisjonen