

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 OSLO

Høringsuttalelse: NOU 2009:1, Individ og integritet

Viser til departementets høringsbrev av 17.februar d.å. vedrørende NOU 2009:1.

Fakultetet for informasjonsteknologi, matematikk og elektroteknikk ved NTNU nedsatte et utvalg 17.mars for å utarbeide en høringsuttalelse, men uttalelsene ble dessverre ikke sendt videre av fakultetet og jeg legger derfor frem høringsuttalelsene i dette brevet.

Merknader til rapporten

Kapittel 4 "Utgangspunkt og avgrensninger" er et verdifullt bidrag i rapporten. Her forsøkes å sette de grunnleggende problemstillinger og begrepsdannelse inn i et oppklarende filosofisk, juridisk og historisk perspektiv. Kapitlet dokumenterer også bakgrunnen for "terminologisk uklarhet, forvirring og strid" med Seip-utvalgets 1975-innstilling som sa at presise og meningsfylte definisjoner vil være relativt nytteløst og føre til feil fokus. Det er rosverdig at kommisjonen med denne rapporten forsøker å bryte med slike holdninger.

Derimot er Kap. 11 "Forslag til tiltak" under Del III "Det teknologiske landskapet" et sørgelig kort kapittel på 7 setninger, og viser hvordan rapporten feiler fullstendig mandatpunktet om å "Fremje forslag til nye prinsipper og verkemidler." Det er svært sannsynlig at en dialog med universitetenes fagmiljøer innen informasjonssikkerhet ville ha sørget for et betydelig mer fyldig "Forslag til tiltak" kapittel. Dette må det arbeides videre med.

Syvende og siste setning i dette kap. 11 sier "Videre bør det pågående arbeidet med infrastruktur for distribusjon av offentlige kryptografiske nøkler (PKI) intensiveres." Også flere andre steder i rapporten nevnes PKI og personvern som samme sak. Så enkelt er det ikke. Etablering og bruk av PKI vil ikke *nødvendigvis* medvirke til vern av personopplysninger. For eksempel har det vært foreslått en nasjonal PKI-løsning der personlige brukere skal ha nøkkelsertifikater med fødselsnummer til å bruke i både offentlige og kommersielle transaksjoner. PKI i denne formen forverrer selvfølgelig persondatavernet.

I Norge kan vi ennå gå, sykle, ta tog, båt og buss uten identitetspapirer. Vi bruker fortsatt ofte låsnøkler og papirbilletter som navnløse adgangsinstrument. Dette kan være en målsetting for elektronisk kommunikasjon også. Dersom personidentifiseringen fjernes i dataregistre og -

Postadresse	Org.nr. 974 767 880	Besøksadresse	Telefon	Professor
Sem Sælandsvei 5 7491 Trondheim	E-post: postmottak@item.ntnu.no http://www.item.ntnu.no	Rom B-211 O.S. Bragstads plass 2B Gløshaugen	+ 47 73 59 43 24 Telefaks + 47 73 59 69 73	Stig Frode Mjøltnes Tlf: + 47 73550459

kommunikasjon vil data bli mindre sensitive med hensyn til personvern. Dette reduserer konfidensialitetskravet og dermed kompleksiteten, for mange anvendelser uten å redusere informasjonens nytteverdi. Rapporten nevner avgiftsregulering av video-overvåkning som en mulighet. Mitt forslag i denne retning er at borgerne skal kunne kreve et vederlag for hver elektroniske personidentifisering som forlanges i kommersielle transaksjoner. Da ville vi kanskje ha satt pris på det.

Datalagringsdirektivet fra EU 2006 pålegger registrering og lagring i 6 til 24 måneder av trafikkinformasjon fra e-post, alle typer telefoni, og internett aksess i allment tilgjengelige tjenester. Dette er en konkret politisk utfordring til spørsmålet "Individ og integritet" i 2009, og kommisjonen har gitt en innsiktsfull og skeptisk uttalelse i vedlegg 1 av sin rapport. Dersom det politisk likevel ender med aksept av direktivet er mitt råd å legge opp til å realisere dette som et interesserbalansert flerparts-system som forsøker å ivareta de hensyn til individ og integritet som kommisjonen fremmer.

Angående pseudonyme helseregistre og innsynsrett.

Vårsemesteret 2007 initierte og veiledet jeg to masteroppgaver

(NTNU Master i kommunikasjonsteknologi med fordypning i informasjonssikkerhet) som skulle vurdere eksisterende realiserte pseudonyme helseregistre i Norge, fra teknisk og organisatorisk synsvinkel. Jeg foreslo og utformet det tekniske grunnlaget for pseudonym registerform som Boe-kommisjonen beskrev og bygget på i NOU 1993:22.

Begge masterkandidatene fant at teknisk og konseptuell forståelse av kryptografiske pseudonymer er for svak hos de ansvarlige myndigheter og også hos registeransvarlige. Alt tyder på at mangel på erfaring med nye teknologiske muligheter resulterer i forsvar for dagens etablerte praksis hos offentlige helseorganisasjoner, med anbefaling om personidentifiserende registerorganisering, og til dels med bruk av vikarierende argumenter mot pseudonyme løsninger.

En masterkandidat (Tine Gevelt) testet ut sin egen innsynsrett til Reseptregisteret. Hun fant at organiseringen av denne innsynsretten ble svært tåpelig gjennomført, slik at innsynsproseduren brøt ned hele hensikten med pseudonymer, og var sannsynligvis langt utenfor det loven forutsetter. Mer detaljer om dette lenger nede. Jeg sendte en orienterende e-post til helsedepartementet den 30. sept 2007 om forholdene vi hadde funnet, men fikk aldri noe tilsvarende.

Masteroppgaven til Refsdal "Bruk av pseudonymiseringsteknologi i nasjonale registre" tok utgangspunkt i en ideell løsning for nasjonale helseregistre sett i lys av både sikkerhetskrav og krav til personvern og pasientrettigheter. Den kartla og vurderte eksisterende løsningsforslag og mekanismer for denne type registre. Videre ble den ideelle situasjonen vurdert opp mot operativ praksis og erfaring for slike registre både i Norge og i utlandet, og han forsøkte å finne fram til en begrunnet teknisk løsning som vil lette realisering og etablering av nasjonale pseudonyme helseregistre.

Pseudonym registerform ble i 2001 tatt inn i Helseregisterloven som en av fire mulige registerformer for nasjonale helseregistre. Siden den gang er det etablert tre nasjonale, pseudonyme helseregistre – Reseptregisteret, Abortregisteret og IPLOS-registeret, men da Norsk pasientregister (NPR) skulle etableres som et personentydig register endte man opp med å velge personidentifiserbar registerform i stedet.

Kandidatens arbeid ble derfor konsentrert om å identifisere tekniske problemer som er til hinder for etablering av nasjonale, pseudonyme helseregistre. Han valgte å studere prosessen rundt etablering av Norsk pasientregister som et personentydig helseregister. Dette er det hittil siste ferdigbehandlede tilfellet hvor både Helse- og omsorgsdepartementet – og et bredt utvalg av høringsinstanser – har gjort en vurdering og sammenlikning av personidentifiserbar og pseudonym registerform.

Kandidaten fant at høringsuttalelsene i forbindelse med etableringen av Norsk pasientregister synes fra mange høringsinstanser å være en repetisjon av innvendingene fra faglig brukerhold ved Folkehelseinstituttet. Denne samklagen kan kanskje skyldes mangel på interesse, tid, og indikerer mangel på selvstendig teknisk vurderingskompetanse. For eksempel NTNU. Institutt for samfunnsmedisin ved NTNU valgte en "konform" høringsuttalelse uten referanse til NTNUs teknologiske ekspertise på pseudonym registerform og informasjonssikkerhet. Denne høringsuttalelsen gjentar Folkehelseinstituttets argumenter som sier at pseudonyme registre ikke gir den samme anledning til å kvalitetssikre data, og videre at det ikke er mulig å finne tilbake til pasientens identitet. Denne innvendingen ble gjennomdrøftet og løst i Boe-utvalgets rapport i 1993, men likevel ser det ut til at denne type innvendinger stadig gjentas.

Refsdal går i sin rapport "Bruk av pseudonymiseringsteknologi i nasjonale registre" igjennom alle uttalte innvendinger i høringen omkring Norsk pasientregister, og konkluderer med at bare fire av høringsargumentene mot pseudonyme registre er reelle problemer. For disse presenterer han forslag til hvordan de kan løses, basert på den eksisterende og etablerte infrastrukturen som finnes for pseudonyme registre. De fire foreslåtte løsningene vil kreve noe mer ressurser i forhold til tilsvarende prosesser for et personidentifiserbart register, men vil gi sterkere vern for persondata.

I Gevelts masteroppgave "Pseudonymiseringsteknologi i nasjonale helseregistre" var det overordnede spørsmålet om dagens løsninger til sentrale helseregistre er optimale i forhold til tekniske og organisatoriske løsningsrom og brukerkrav. Kandidaten kartla hvordan slike helseregistre brukes i dag, og gjorde en stor spørreundersøkelse på hvordan involverte parter tenker omkring optimal løsning av et nasjonalt register basert på pseudonymer. Basert på disse resultatene utarbeidet hun ett konkret forslag til teknisk og organisatorisk forbedring i forhold til dagens situasjon, samt fremtidige muligheter for mer utstrakt bruk av registeret.

Hennes konklusjon er at ingen av dagens to registre (IPLOS-registeret og Reseptregisteret) er optimale. Det mest oppsiktsvekkende funnet ble gjort hos Reseptregisteret, som innledningsvis

nevnt. Her viste det seg at Registeret ikke overholder bestemmelsene for hvordan innsyn i registeret skal håndteres.

Gjennom et enkelt eksperiment med å gjøre en innsynsforespørsel for seg selv, avdekket hun at Reseptregisteret brukte Statistisk Sentralbyrå (SSB) som "orakel" for kobling fra fødselsnummer til pseudonym! Reseptregisteret spurte Gevelt om fødselsnummeret, fikk dette, og sendte det videre til SSB med forespørsel om å få pseudonymet hennes. SSB svarte med riktig pseudonym, og deretter kunne de slå opp i registeret og sende data tilbake til Gevelt. Man trenger ikke være Master i Teknologi for å forstå at denne organiseringen av innsynsretten knekker intensjonen med pseudonymiseringen helt og fullstendig!

Innsynsretten er et viktig personvernprinsipp, og en tilfredsstillende realisering av innsynstjenesten er påkrevd. Derfor ble det i Gevelts oppgave i stor grad lagt vekt på å presentere løsninger som håndterer innsyn etter bestemmelsene, med case study av Reseptregisteret. Kandidaten foreslår to måter for hvordan innsyn bedre kan håndteres her. Den ene baserte seg på at en forespørsel om innsyn ble rettet gjennom en nettbasert løsning, mens den andre brukte apotekene som en slags inngangsportal for å rette en forespørsel om innsyn mot Reseptregisteret.

Informasjonsplikten til apotekene for Reseptregisteret ble også undersøkt. Hvordan status er for IPLOS-registeret burde vært undersøkt, men ble det ikke. Det viste seg at apotekenes informasjonsformidling til de som henter ut resepter ikke er tilfredsstillende. Dette til tross for at apotekene selv mener at informasjonen er tilstrekkelig. For personvernet er informasjonsformidling til de som blir registrert i registeret viktig. Og at dette heller ikke håndteres tilfredsstillende er ikke bra med hensyn på personvernet. Det er svekkende for personvernet at de som blir registrert i Reseptregisteret faktisk ikke er klar over det.

Med hilsen

Professor Stig F. Mjølhus

NTNU