



DET KONGELEGE
MODERNISERINGSDEPARTEMENT

St.meld. nr. 40

(2004–2005)

Datatilsynets og Personvernneemndas årsmeldingar for 2004



Innhald

1	Innleiing	5	4	Administrasjon og ressursar	12
2	Moderniseringsdepartementets merknader til Datatilsynets årsmelding for 2004	8	Vedlegg		
			1	Datatilsynets årsmelding 2004.....	13
3	Moderniseringsdepartementets merknader til Personvernemndas årsmelding for 2004	11	2	Personvernemndas årsmelding 2004	53



DET KONGELEGE
MODERNISERINGSDEPARTEMENT

St.meld. nr. 40

(2004–2005)

Datatilsynets og Personvernemndas årsmeldingar for 2004

*Tilråding frå Moderniseringsdepartementet av 10. juni 2005,
godkjend i statsråd same dagen.
(Regjeringa Bondevik II)*

1 Innleiing

Er individuelle personvernrettar i ferd med å måtte vike for samfunnets behov for vern, kontroll og effektivitet? Ein kan seie at grensene for den personlege sfæren til kvar enkelt blir trekte stadig snevrare. Rørslene våre blir kartlagde i større og større grad – det vere seg *kva* vi har gjort, *kvar*, og til *kva* tidspunkt. George Orwell skildra i "1984" eit samfunn der styresmaktene eller "Storebror" overvaka kvar minste rørslle menneska gjorde. Eit slikt samfunn er vi heldigvis langt unna. Den teknologiske utviklinga har likevel ført til at vi har ei rekkje "veslebror" som følgjer oss til alle tider – bl.a. representert ved ei rekkje overvakingkamera og elektroniske spor vi let etter oss. Så – kvar bør grensa for privatsfæren gå?

Personvern blir ofte karakterisert som vern av kvar enkelt sin personlege integritet og ivaretakinga av privatlivets fred. Men kva som blir sett på som viktig å verne for somme, vil vere mindre viktig for andre. Korleis kvar enkelt vurderer dette vil blant anna avhenge av eigne erfaringar og opplevingar, saker omtalte i ulike medium, kor komplisert det er å ta vare på personvernet i kvart enkelt tilfelle, kva ein kan oppnå ved å fire på personvernet i ei enkelt sak, og ikkje minst av kvar enkelt sine kunnskapar og medvit om personvernutfordringar. Vidare er det ofte mangel på kunnskap om

omfang av tilgjengelege personopplysningar, og korleis desse kan koplast. Helseopplysningar blir ofte oppfatta som svært kjenslege. Dei fleste av oss vil nok vere einige i at helseopplysningar krev spesielt vern slik at dei ikkje kjem uvedkommande i hende.

Det siste året har det vore ein debatt i media om overvaking av offentlege kommunikasjonsmiddel. Mange har uttalt seg om behovet for å overvake bl.a. bussar for å gjere det trygt for tilsette og passasjerar. Eit anna aktuelt tema har vore overvaking av tilsette på arbeidsplassen. Ein argumentasjon som går att er: Når det først er mogleg - kvifor skal ein ikkje då kunne gjere det? I ei klagesak omtalt bakarst i denne meldinga kom Personvernemnda fram til at det må finnast ei grense for kor intensiv overvaking som kan tillatast på ein arbeidsplass. Moderniseringsdepartementet ser det som nødvendig med debatt rundt omsynet til kvar enkelt integritet kontra omsynet til det moderne samfunnets behov for å kunne behandle og utveksle personopplysningar.

I meldinga i fjor lanserte regjeringa 2005 som *Personvernåret*. Det er fleire grunnar til at 2005 er viktig i personvernsamheng. Både personvernlovgivinga i Noreg og Datatilsynet fyller 25 år i år. Etter ønske frå Stortinget startar arbeidet med

revisjon av personopplysningsloven og –forskriftene i år. I år gjennomfører Moderniseringsdepartementet i samarbeid med Datatilsynet ei befolkningsundersøking og ei bedriftsundersøking om bl.a. haldningar til personvern generelt og personopplysningsloven spesielt. Grensa for den private sfæren vil stå sentralt i dette arbeidet.

Det er fleire instansar som er direkte involverte i personvernarbeidet. Datatilsynet er som fagleg uavhengig forvaltningsorgan administrativt underlagt Moderniseringsdepartementet. Klagesaker over Datatilsynets avgjerder blir behandla av Personvernemnda. Ansvar for personopplysningsloven ligg i Justisdepartementet. Moderniseringsdepartementet har ansvar for personopplysningsforskrifta, enkeltsaker etter loven, etatsstyringa av Datatilsynet og det administrative ansvaret for Personvernemnda.

Personvernet gjennom 25 år

Noreg var eit av dei første landa i Europa med eit eige lovverk om personvern. Personregisterloven trådde i kraft 1. januar 1980. Datatilsynet blei etablert samtidig. Når ein ser tilbake på den tida Datatilsynet har verka, ser vi at ulike personvernspørsmål i eit kvart hundreår har skapt engasjement blant store delar av befolkninga. Innhaldet i personverndebatten har endra seg i takt med samfunnsutviklinga – ikkje minst den teknologiske utviklinga. Jamvel om relativt nye undersøkingar viser at svært mange framleis ikkje har noko forhold til personvernspørsmål, er det likevel grunn for å tru at fleire har kunnskap om ulike personvernema no enn for 25 år sidan.

Frå personregisterlov til personopplysningslov

Fokus i den tidlegare personregisterloven var retta mot systematiske lister og oppteikningar og liknande som kunne karakteriserast som register. Det var først og fremst her lovgivarane såg behov for regelverk for å verne enkeltindividet sine interesser. I åra som følgde etter at loven trådde i kraft blei fokuset breiare, og det klassiske registeromgrepet var ikkje lenger like viktig som utgangspunkt for personvernet. Personopplysningar blei etter kvart behandla i elektronisk form i stort omfang i både offentleg og privat sektor. Personregisteromgrepet blei derfor etter kvart for snevert. Det blei behov for ei meir tidsriktig lovgiving for behandling av personopplysningar.

I 2001 blei personregisterloven erstatta av personopplysningsloven. Personopplysningsloven representerer delvis ei vidareføring, oppdatering og vidareutvikling av personregisterloven, men

inneheld også ei rekkje nye reglar bl.a. som følgje av at loven også implementerte EUs personverndirektiv 95/46 EF. I 2003 fekk vi vidare ein eigen personvernlov for helsesektoren – helseregisterloven.

Det nye personvernregelverket inneber eit større ansvar for bedrifter og verksemdar i og med at konsesjonsinstituttet er bygd ned samstundes som det er innført meldeplikt til Datatilsynet for behandling av personopplysningar. Vidare styrkjer loven rettane til den som personopplysningane gjeld, bl.a. får den som er registrert utvida rett til innsyn. Særleg overfor private behandlingsansvarlege inneber dette utvida rettar. Som ei viktig nyskaping blir den som behandlar personopplysningar pålagt av sitt eige tiltak å varsle den registrerte når opplysningar om vedkommande blir samla inn. Loven har dessutan fleire og meir utførlege reglar om når personopplysningar kan overførast til utlandet, og regelverket for fjernsynsovervaking er skjerpa. Det er innført eit generelt erstatningsansvar for lovbrøt. Klagar over avgjerdene til Datatilsynet blir ikkje lenger behandla av departementet, men av ei uavhengig klagenemnd – Personvernemnda.

Internasjonalisering av personvernlovgivinga

I løpet av Datatilsynets verketid har personverndiskusjonen dreidd frå stort sett å handle om interne norske spørsmål til i stor grad også å handle om internasjonale forhold. Dette kjem av at utfordringane stort sett er like frå land til land – og at det derfor er formålstenleg å samarbeide om løysingar. Vidare har overføring av personopplysningar over landegrensene blitt enklare og meir omfattande enn tidlegare. Internett har dessutan medført at opplysningar som blir publiserte på dette mediet i eitt land, blir publiserte internasjonalt på same tid.

Personopplysningsloven og helseregisterloven er som nemnt sterkt påverka av EUs personverndirektiv. Implementering av direktivet inneber at landegrensene innanfor EU/EØS ikkje inneber noka avgrensing på flyten av personopplysningar. Men implementeringa har også medført at spørsmål om personvern er sett på saklista i ei rekkje land som ikkje har særlege tradisjonar på området.

Det er vidare avsagt viktige dommar på personvernområdet i Den europeiske menneskerettsdomstolen (EMD). Den europeiske menneskerettskonvensjonen, artikkel 8 slår fast retten til eit privatliv: *"Kvar og ein har rett til respekt for sitt privatliv og familieliv, sin heim og sin korrespondanse."* EMD har i fleire sentrale dommar teke stilling til ytringsfridomen halde opp mot vernet av privatli-

vets fred. Mykje kan tyde på at personvernet i enkelte samanhengar er i ferd med å få ei styrkt stilling. Moderniseringsdepartementet viser bl.a. til den mykje omtalte saka *Von Hannover vs. Tyskland* frå 2004. EMD kom her til at Prinsesse Caroline av Monaco hadde rett til å sleppe å få søkjelyset på seg i private samanhengar.

Datatilsynet deltek i ulike nordiske, europeiske og internasjonale fora for fremjing av personvern. Her diskuterer og utvekslar ein utfordringar og erfaringar på personvernområdet slik at landa står betre rusta til å møte eigne utfordringar.

Personvernundersøkinga 2005

Utviklinga mot ein stadig meir omfattande bruk av personopplysningar gjer det nødvendig å vege omsynet til privatlivets fred opp mot andre sentrale samfunnsomsyn – slik som tiltak mot kriminalitet og ei meir effektiv forvaltning. Ei utfordring i forhold til denne avveginga er at personvern i utgangspunktet er eit immaterielt gode som lett tapar i forhold til meir målbare storleikar. Vidare vil ulike personar leggje ulik vekt på desse omsyna, jf. ovanfor. Ei kartlegging av kunnskapar og haldningar til personvern er nødvendig for å sørge for at reguleringa av bruken av personopplysningar samsvarer med samfunnsutviklinga.

Den siste personvernundersøkinga blei utført i 1997 på oppdrag frå Datatilsynet. Moderniseringsdepartementet meiner det er grunn til å tru at folks kunnskapar og haldningar er endra bl.a. som følgje

av den teknologiske utviklinga. Mobiltelefonar med kamera var for eksempel ukjent i 1997. Ein kan også gå ut frå at merksemda dei siste åra kring terror og annan kriminalitet har påverka folks aksept for ulike kontroll- og overvakingstiltak. Moderniseringsdepartementet meiner at det er nødvendig med regelmessige undersøkingar for å sørge for at reguleringa av personvernsspørsmål samsvarer med samfunnsutviklinga.

Revisjon av personopplysningsloven

Justiskomiteen uttalte ved behandling av personopplysningsloven i Innst. O. nr. 51 (1999-2000) at det kunne vere fornuftig å ha ein etterkontroll av loven etter fire år. Etterkontrollen startar opp i 2005. Endring i teknologisk utvikling, i samfunnsforhold og av trusselbilete har gjort det ønskjeleg å sjå på enkelte av føresegnene i loven i lys av utviklinga etter at loven blei vedteken. I etterkontrollen vil regjeringa bl.a. sjå på om føresetnader som blei lagde til grunn for loven framleis er haldbare. To sentrale tema her er ein gjennomgang av konsekvensinstituttet og ei vurdering av rettane som blei gitt til enkeltpersonar i forhold til å vareta eige personvern. Andre viktige tema blir vurdering av ei eventuell regulering av elektroniske spor og kontroll og overvaking av arbeidslivet. Resultata frå personvernundersøkinga vil stå sentralt i revisjonen av loven som faktagrunnlag for eventuelle endringar.

2 Moderniseringsdepartementets merknader til Datatilsynets årsmelding for 2004

Datatilsynets arbeidsområde

Datatilsynets hovudoppgåver er å verne kvar enkelt mot at personvernet blir krenkt gjennom behandling av personopplysningar. Datatilsynet er tilsynsmyndigheit etter personopplysningsloven og helseregisterloven. Sjølv om lovene stort sett er uendra sidan dei blei vedtekne, har Datatilsynet sitt arbeidsfelt auka bl.a. som følgje av at informasjonsgrunnlaget og informasjonsbehovet i samfunnet stadig aukar i volum. Fordi personvernspørsmål vedgår oss alle på stadig fleire område er det viktig med eit synleg Datatilsyn.

Datatilsynets arbeid

Datatilsynet behandla eit stort tal saker i 2004. Gjennom aktivt tilsyn og saksbehandling kontrollerer Datatilsynet at lover og forskrifter for behandling av personopplysningar blir følgde, og at feil og manglar blir retta. Datatilsynet kombinerer aktivt tilsyn med informasjon og rettleiing – og oppnår etter Moderniseringsdepartementets syn mykje "personvern" for ressursane. Kombinasjonen av tilsyn og andre verkemiddel har vist seg vellykka for både Datatilsynet og den verksemda som er gjenstand for tilsyn.

Svært mange saker som det offentlege har med å gjere har sideomsyn til personvern. Datatilsynet gav 104 svar på saker som var på høring i 2004. Fleire av sakene var forslag til omfattande reformer på ulike område – slik som for eksempel NOU 2004: 5 Arbeidslivslovutvalget. Departementa som utgreier saker pliktar å greie ut kva konsekvensar forslaga deira har for personvernet. Ei sentral rolle for Datatilsynet er å fange opp og kommentere eventuelle manglande og mangelfulle personvern-utgreiingar. Høringssvar inneber derfor ofte ein første kontakt med forslagstillaren. Ofte blir høringssvara følgde opp med ein dialog om løysingar. Dialogen blir ofte betre jo tidlegare Datatilsynet blir involvert i prosessen. Datatilsynet deltek derfor også i ulike offentlege råd og utval.

Ei anna sentralt verkemiddel er utarbeiding av relevant personverndokumentasjon. I personvernrapporten i fjor presenterte Datatilsynet 10 viktige

Boks 2.1 10 viktige prinsipp for behandling av personopplysningar

1. Det skal gode grunnar til å behandle personopplysningar.
2. Du skal informerast før du blir registrert.
3. Registrering skal i størst mogleg grad baserast på samtykke.
4. Overskottsinformasjon skal ikkje lagrast.
5. Du har rett til innsyn i kva slags behandling av personopplysningar som blir føreteke av ei verksemd – og i eigne opplysningar.
6. Unødvendige opplysningar skal slettast.
7. Feilaktige eller mangelfulle opplysningar skal rettast.
8. Det skal vere gratis å vareta sine rettar til innsyn, retting og sletting.
9. Personopplysningar skal sikrast og rutinar og tiltak som sikrar personopplysningar skal dokumenterast.
10. Opplysningar som er samla inn til eitt formål skal ikkje brukast til noko anna utan samtykke eller lovheimel.

prinsipp for behandling av personopplysningar. Moderniseringsdepartementet strekar under at det er viktig å innrette seg etter desse.

Særleg om Datatilsynets tilsynsarbeid

Datatilsynet gjennomførte 161 tilsyn i 2004. Datatilsynets årsmelding inneheld ei fullstendig liste over tilsynsobjekta. Hovudinntrykket er at det framleis er manglande kunnskap om pliktene i personvernregelverket. Det gir grunn til uro når dei aller fleste av tilsynsobjekta får merknad frå Datatilsynet om manglande internkontroll. Tilsyna viser at det i manglande grad er teke initiativ frå leiinga om å setje i gang nødvendige aktivitetar og å klargjere ansvar. Datatilsynet avdekte gjennom tilsynsverksemda at enkelte medisinske forskarar valde å

ikkje ta omsyn til konsesjonsvilkåra frå Datatilsynet fordi desse blei oppfatta som kompliserande i forskinga. Dette er alvorleg. Regelverket på personvernområdet og konsesjonsvilkår frå Datatilsynet skal sikre at dei som av ulike grunnar har gitt frå seg medisinsk informasjon skal ha krav på at opplysningane blir behandla med den respekt som regelverket skal sikre. Moderniseringsdepartementet viser til at regelverket for medisinsk forskning nyleg er vurdert av eit utval (Nylennautvalet) jf. NOU 2005:1 God forskning - bedre helse.

Moderniseringsdepartementet vonar at det ekstra fokuset på personvern i år kan føre til at verksemdar får på plass ein personvernpolicy og får rydda opp i ansvarsforholda i forhold til informasjonstryggleiken slik personvernregelverket krev.

Datatilsynets overordna prioriteringar i 2004

Datatilsynet hadde fokus på fleire område i 2004: Direkte marknadsføring, offentlig forvaltning, helse og forskning, Internett, samferdselssektoren, kameraovervaking, justissektoren og arbeidsliv. Både arbeidsliv og helse er ei vidareføring av satsingsområde frå 2003. Moderniseringsdepartementet ønskjer særleg å kommentere tre tema:

Kameraovervaking

Eitt av dei tema som har skapt debatt i media det siste året er spørsmål om kameraovervaking. Oslo er ved sida av London ein av dei mest kameraovervakte byar i verda. Overvakingskamera blir stadig meir avanserte og rimelege i innkjøp, og dei blir tekne i bruk stadig oftare. Kameraovervaking er i stor grad blitt ein akseptert metode i forsøk på å løyse ulike problem – ofte utan at alternative tiltak blir diskuterte. Kamera overtek i mange tilfelle for, eller supplerer fysisk vakthald og personleg nærvær. Saker omtalte i media tyder på at det rår ein kombinasjon av ukunne kring regelverket for kameraovervaking, og manglande dømmekraft med omsyn til kva overvakingstiltak det er akseptabelt å setje i verk. Og gir verkeleg overvaking auka tryggleik?

Det er delte meiningar om kriminaliteten går ned ved overvaking. Somme hevdar at kriminaliteten flyttar seg til område utan overvaking. Fjernsynsovervaking kan likevel medverke til betre og raskare oppklaring av kriminalitet – føresett at dei kamera som er sette opp verkeleg fungerer. Datatilsynet har avdekt at mange kamera som er sette opp ikkje er i funksjon. Faren for at kamera berre viser ein del av sanninga, slik at uskyldige personar blir mistenkeleggjorde, er alltid til stades. Vidare

finst det ingen garanti for at informasjonen ikkje blir misbrukt av folk som ikkje har reint mjøl i posen, eller at informasjon kjem på avvegar som følgje av at opptaka ikkje er tilstrekkeleg sikra.

Datatilsynet har laga ein rettleiar for bedrifter og enkeltpersonar som vurderer å setje opp overvakingskamera. Rettleiaren finst bl.a. på Datatilsynets heimesider <http://www.datatilsynet.no>. Vidare har Datatilsynet gått inn i eit samarbeid med NELFO, bransjeorganisasjonen for bedrifter som arbeider med installasjon innan elektrofaga i Noreg. Moderniseringsdepartementet ser på dette samarbeidet som svært positivt, og gir honnør til Datatilsynet og NELFO for å ha teke dette initiativet for å heve kompetansen om plikter ved kameraovervaking i bransjen.

Direkte marknadsføring

Personvern inneber også retten til å kunne unngå å bli kontakta i marknadsføringsformål pr telefon eller post. Ved utgangen av 2004 hadde litt over ein million personar registrert seg i reservasjonsregisteret i Brønnøysund. Det har vist seg at reservasjonsregisteret ikkje nødvendigvis blir teke alvorleg frå marknadsførarar, eller at systemet ikkje fungerer heilt etter intensjonen – noko som skaper irritasjon blant dei som har reservert seg. Dette tener neppe verken marknadsførar eller enkeltpersonar. Datatilsynet vil av denne grunn sjå nærmare på reservasjonsordninga. Blant ideane som har vore diskuterte er at den direkte marknadsføringa skal baserast på førehandssamtykke og ikkje reservasjon slik som i dag.

Offentleg forvaltning

I regjeringas moderniseringsprogram er eit sentralt mål å utnytte fellesskapets ressursar betre for å sikre tenester med høg kvalitet og tilstrekkeleg omfang, tilpassa individet, pluss å skape ein enklare kvardag for borgarar og næringsliv. Ny informasjonsteknologi skal takast i bruk for å effektivisere saksbehandlinga og samhandlinga med publikum. Tilgang til personopplysningar om kvar enkelt er nødvendig for at forvaltninga skal kunne vareta sine oppgåver på ein fagleg forsvarleg måte. Det er likevel viktig at ein held dei faglege omsyna opp mot personvernomsyn. Forvaltninga er avhengig av at kvar enkelt har tillit til at opplysningane blir behandla på ein forsvarleg måte og ikkje kjem uvedkommande i hende. I motsett fall vil borgarane kunne la vere å ta kontakt, halde tilbake eller gi feilaktig informasjon av frykt for at opplysningar skal komme på avvegar. Ei oppfatning i befolkninga om at forvaltninga ikkje vare-

tek pliktene sine her, vil følgeleg setje regjeringas effektiviseringsprosjekt kraftig tilbake. Ein grunnleggjande føresetnad for regjeringas effektiviseringsarbeid er derfor at tilsette i forvaltninga berre skal ha tilgang til opplysningar som er nødvendige for at dei skal kunne utføre sine arbeidsoppgåver.

Sentrale prosjekt er etableringa av ein felles it-arkitektur og felles grunndata. Desse prosjekta står sentralt i arbeidet med "Min side". Min side vil vere borgaranes felles inngangsdør til offentlege tenester på Internett og vil gi tilgang til digitale tenester uavhengig av kva sektor eller kva forvaltningsnivå som tilbyr tenestene. Moderniseringsdepartementet vil sørge for at personvern står sentralt i arbeidet med effektiviseringa av offentleg

forvaltning. Blant anna vil Moderniseringsdepartementet vurdere korleis Min side kan brukast til å styrkje den enkeltes rettar etter personopplysningsloven.

Moderniseringsdepartementet viser til kronikken i Datatilsynets årsmelding av Anders Ryssdal, leiar av advokatforeininga. Ryssdal viser til at teknologisamfunnet opnar for nye og uoverskodelege høve til innsamling, lagring og bruk av informasjon – både for forvaltning og næringsliv. Potensialet for effektivisering er stort, men slik bruk opnar også for misbruk av den informasjon som blir samla inn. Det må derfor vere klare grenser for bruk, gjenbruk og samankopling av informasjon.

3 Moderniseringsdepartementets merknader til Personvernemndas årsmelding for 2004

Behandling av klagesaker

Personvernemnda avgjer klagar over Datatilsynets avgjerder. Tidlegare behandla Moderniseringsdepartementet saker som fall utanfor bruksområdet for personopplysningsloven. I 2004 kom Justisdepartementets Lovavdeling til at Personvernemnda er rette instans til å behandle alle klagar over Datatilsynets avgjerder, med unntak av reint administrative avgjerder. Dette vil truleg føre til at Personvernemnda vil få nokre fleire saker enn tidlegare.

Talet på klagesaker som kom inn til nemnda i 2004 var på omlag same nivå som tidlegare år. Erfaring viser likevel at sakene blir meir komplekse og at fleire saker er av prinsipiell karakter. Særleg spørsmål vedrørande forskning og personvern – og forholdet til samtykke – har vist seg vanskelege. Ein stor del av klagesakene gjeld tvil om tolkinga av føresegnene i personvernlovgivinga. Vedtaka blir lagde ut på Personvernemndas heimeside, <http://www.personvernemnda.no>. Sakene blir presenterte på ein slik måte at dei i tillegg til å avgjere den konkrete saka også kan medverke til avklaring av gjeldande rett.

Ny Personvernemnd frå 2005

I samsvar med personopplysningsloven er medlemmene i Personvernemnda oppnemnde for fire år av gongen med høve til å bli oppattnemnde for ytterlegare fire år. Medlemmene er utpeikte i kraft av sine kunnskapar innanfor bestemte saksområde, og ikkje som representantar for bestemte interesseorganisasjonar eller liknande. Målet er at nemnda skal ha ein samansett kompetanse innanfor personvernspørsmål og til å avvege personvernspørsmål mot andre samfunns mål. For å unngå at alle medlemmene må skiftast ut frå 2009, blei enkelte av medlemmene skifta ut trass i at dei har gjort ein god jobb i nemnda.

Stortinget nemnde hausten 2004 oppatt professor Jon Bing og juridisk rådgivar Gro Hillestad Thune som høvesvis leiar og nestleiar av nemnda for perioden 2005 til 2008. Dei andre medlemmene av nemnda blei høvesvis oppattnemnde og oppnemnde av regjeringa. Advokat Siv Pedersen, seniorrådgivar Hanne Bjurstrøm, adm. dir. Tom Bolstad, førsteamanuensis Jostein Halgunset og førsteamanuensis Leikny Øgrim utgjer dei andre medlemmene av nemnda for noverande periode. I tillegg blei det oppnemnd personleg vara for kvart av medlemmene.

4 Administrasjon og ressursar

Datatilsynet som ein brukarvennleg etat

Mange enkeltpersonar har ein høg terskel for å ta kontakt med statlege organ. I Datatilsynet har dei freista gjere kontakten med etaten enklare. Datatilsynet har i 2004 – etter litt prøvetid – fått etablert ei såkalla ”førstelinjeteneste”. Tenesta svarer på innkomne telefonar og e-post – i tillegg til å yte hjelp i saksbehandlinga. Dette har medført at alle relativt enkle spørsmål får raskare svar. Tilbakemelding frå publikum har vore positiv. Moderniseringsdepartementet meiner førstelinjetenesta er eit føredøme for andre verksemdar.

Klagesaker

Talet på klagesaker til Personvernemnda var i 2004 på om lag same nivå som tidlegare år. Personvernemnda har likevel varsla om at det dei første månadene i 2005 har komme inn ei rekkje nye klagesaker. Auken i talet på klagesaker kjem bl.a. av auka aktivitet i Datatilsynet. Fleire av klagesakene oppstår i etterkant av Datatilsynets tilsynsverksemd – særleg tilsyn i samband med forskingsprosjekt. Her har Datatilsynet avdekt ei rekkje tilfelle

der forskarar ikkje følgjer dei fastsette konsesjonsvilkåra. Vidare oppstår ein del klagar som følgje av usemje om konsesjonsvilkår. Andre saker gjeld privatpersonar som meiner deira personvern er krenkt på ulike måtar, og som søker hjelp frå Datatilsynet for å rette opp i dette. I tillegg til at talet på klagesaker har auka, har sakene blitt meir komplekse. Ein stor del av sakene har handla om å vege viktige samfunnsomsyn mot kvarandre – slik som ytringsfridom og personvern.

Moderniseringsdepartementet vil følgje med i utviklinga og vurdere om både Datatilsynet og Personvernemnda har tilstrekkelege ressursar i forhold til arbeidsoppgåvene dei er pålagde.

Moderniseringsdepartementet

t i l r å r :

Tilråding frå Moderniseringsdepartementet av 10. juni 2005 om Datatilsynets og Personvernemndas årsmeldingar blir send Stortinget.

Vedlegg 1**Datatilsynets årsmelding 2004****Innhald**

1	Datatilsynet 25 år i 2005.....	13
2	Organisasjon og administrasjon	14
3	Saksbehandling	14
4	Deltaking i offentlege råd og utval	16
5	Internasjonalt samarbeid	18
6	Informasjon som verkemiddel	19
7	Tilsyns- og tryggingssarbeid	21
7.1	Hovedinntrykk	22
7.2	Større tilsynsprosjekt.....	24
7.3	Kort om andre tilsyn	25
7.4	Styringssvikt i organisasjonen?.....	26
8	Tema 2004	26
8.1	Direkte marknadsføring	26
8.2	Offentleg forvaltning	28
8.3	Helse og forskning	31
8.4	Internett.....	33
8.5	Samferdselssektoren	34
8.6	Kameraovervaking.....	38
8.7	Justissektoren	40
8.8	Arbeidsliv	45

Gjestekommentar: Rettssikkerhet på vikende front av Anders Ryssdal, leiar Advokatforeningen.....	47
---	-----------

Oversikt over gjennomførte tilsyn 2004.....	49
--	-----------

1 Datatilsynet 25 år i 2005

Datatilsynet blei etablert 1. januar 1980 i samsvar med den dåverande personregisterloven vedteken i 1978. Datatilsynet markerer derfor sitt 25-årsjubileum i 2005.

Datatilsynet har til oppgåve å verne kvar enkelt mot at personverninteressene blir krenkte gjennom behandling av personopplysningar. Personopplysningar skal behandlast i samsvar med grunnleggjande personvernomsyn som behovet for vern av personleg integritet og privatlivets fred. Det juridiske grunnlaget for verksemda til Datatilsynet er regulert i Lov om behandling av person-

opplysningar av 14. april 2000 (personopplysningsloven) og Lov om helseregistre og behandling av helseopplysningar (helseregisterloven) av 18. mai 2001.

Datatilsynet er eit uavhengig forvaltningsorgan, administrativt underordna Kongen ved Moderniseringsdepartementet. Det at Datatilsynet er uavhengig inneber at departementet ikkje kan gi instruks om, eller gjere om dei avgjerder Datatilsynet tek ut frå personopplysnings- eller helseregisterloven. Som klageinstans i forhold til Datatilsynets vedtak er det oppretta ei Personvernemnd. Nemnda gir ut si eiga årsmelding.

Datatilsynets oppgaver

Datatilsynet skal halde seg orientert og informere om den nasjonale og internasjonale utviklinga i behandlinga av personopplysningar, og om dei problema som knytter seg til slik behandling. Datatilsynet skal identifisere truslar mot personvernet og gi råd om korleis ein kan unngå eller avgrense dei. Å delta i råd og utval er derfor ein viktig del av arbeidet til Datatilsynet. Også som høringsinstans i saker som kan ha konsekvensar for personvernet, har Datatilsynet innverknad på samfunnsutviklinga.

Datatilsynet fører eit offentleg oversyn over alle behandlingar av personopplysningar som er melde inn. Vidare behandlar Datatilsynet søknader om konsesjon, der det er krav om dette etter loven.

Gjennom aktivt tilsyn og saksbehandling kontrollerer Datatilsynet at lovar og forskrifter for behandling av personopplysningar blir følgde, og at feil og manglar blir retta. Datatilsynet hjelper bransjeorganisasjonar med å utarbeide bransjevise åtferdsnormer, og gir bransjar og enkeltverksemdar råd om sikring av personopplysningar. Datatilsynet motiverer også til, og støt verksemdar som på frivillig basis har oppnemnt eit eige personvernombod.

Sist, men ikkje minst, har Datatilsynet også ei viktig ombudsrolle. I samband med dette gir ein råd og informasjon til enkeltpersonar som tek kontakt med tilsynet. Publikum generelt blir i første rekkje nådd gjennom aktiv mediekontakt og publi-

sering på ein eigen nettstad. For å skape merksemd og interesse kring personvernspørsmål deltek Datatilsynet aktivt i den offentlege debatten og legg stor vekt på å praktisere meirinnsyn.

2 Organisasjon og administrasjon

Budsjett

Budsjettramma for Datatilsynet blei auka for 2004 i forhold til året før. Datatilsynet styrkte som følgje av dette innsatsen på dei områda som var føresetnaden for budsjettauken. Det vil seie gjennomføring av tilsyn/kontrollar innan prioriterte satsingsområde, reduksjon av saksbehandlingstida, etablering av ei Frontserviceeining, samt førebunde arbeid til ei større personvernundersøking.

Den økonomiske ramma for Datatilsynet for 2004 var på i overkant av 21 millionar kroner. Dei reine lønnskostnadene utgjer ca 70 prosent av driftsbudsjettet. Ut over dette har løyvinga dekt faste driftsutgifter og utgifter til operativ tilsynsverksemd, informasjonsarbeid og representasjon i internasjonale organ. I 2004 har det også vore ekstra kostnader i samband med avlevering av arkiv og etablering av ny heimeside på Internett.

Organisasjon

Datatilsynet blir leidd av direktør Georg Apenes og er organisert i fire avdelingar; juridisk, tilsyn og tryggleik, informasjon og administrasjon. Juridisk avdeling utgjer med sine 15 medarbeidarar den største organisatoriske eininga.

Det var i verksemdsåret 27 fast tilsette, 17 kvinner og 10 menn. Gjennomsnittsalderen er 44 år for menn og 36 år for kvinner.

Det har vore tilsett ekstrahjelp og vikarar for å bøte på arbeidssituasjonen. To engasjementsstillingar er vidareførte i juridisk avdeling i samband med at det er etablert ei førstelinjeteneste (Frontservice). Denne består av tre juridiske saksbehandlarar som svarer på innkomne telefonar og e-post, i tillegg til å medverke i saksbehandlinga. Det er vidare blitt oppretta ei ny stilling i tilsyns- og tryggleiksavdelinga. Denne har som hovudoppgåve å styrkje tilsynsarbeidet og hjelpe til med IT-driftsoppgåver. Det er også blitt oppretta ei ny rådgivarstilling i informasjonsavdelinga.

I løpet av året har éin medarbeidar slutta i Datatilsynet. Men fleire engasjement og vikariat har gått til opphør og fast tilsette er tilbake i arbeid etter svangerskapspermisjonar.

Avtale om inkluderande arbeidsliv

Datatilsynet blei med verknad frå september 2003 knytt til avtalen om eit inkluderande arbeidsliv. Avtalen tydeleggjer samarbeidet mellom arbeidsgivar og arbeidstakar med det mål å skape eit meir inkluderande og utviklande arbeidsmiljø. Datatilsynet såg behov for støtte til HMS-arbeidet for å leggje forholda best mogleg til rette for sunn, trygg og effektiv drift. Datatilsynet inngjekk derfor i 2004 avtale med Norsk Bedriftshelseteneste AS og har hatt tilbod til dei tilsette om ei arbeidshelseundersøking. Det blir utarbeidd ein oppsummeringsrapport etter at arbeidshelseundersøkingane er utførte. Denne vil kunne gi innspel til prioritering av aktivitetar for 2005.

Grøn stat

Alle statlege etatar og verksemdar skal innan 2005 innføre miljøleiving som ein integrert del av styringssystema i organisasjonen. Datatilsynet slutførte dette arbeidet i 2004.

Resultatindikatorar

Det er i 2004 etablert rutinar for rapportering på relevante resultatindikatorar for Datatilsynet. Desse skal gjelde ved rapportering til departement og Storting i 2005.

Arkiv

Etter ei tilbodsinnbyding inngjekk Datatilsynet ein avtale med Stiftelsen ASTA om ordning av arkivmateriale frå perioden 1979-2000. Kassasjonsplan er utarbeidd og godkjend av Riksarkivet. Materialet som er ordna utgjer i alt ca 160 hyllemeter. I tillegg kjem ca 25 hyllemeter med kopibøker som Datatilsynet har bunde inn sjølv. Arbeidet blei avslutta i november 2004.

Revisjon av økonomiregelverket

Nytt reglement for økonomistyring i staten med føresegner trådde i kraft frå 1. januar 2004. Datatilsynet har i samband med dette oppdatert økonomiinstruksar og tilhørande retningslinjer.

3 Saksbehandling

Ordinær saksbehandling

Det blei i meldingsåret journalført 7 725 dokument, av desse var 4 129 innkomne og 3 596 utgåande brev frå Datatilsynet. Dette er ein liten auke frå året før. Helserelaterte saker utgjer den største delen, med sine til saman 1 552 dokument.

150 av sakene handla om problemstillingar av i all hovudsak teknisk karakter. Dette kjem i tillegg til at ein kjem borti tekniske problemstillingar også ved behandling av konsesjonssøknader og ved gjennomføring av tilsyn.

Konsesjonssaker

Plikta til å søkje konsesjon gjeld i all hovudsak ved behandling av sensitive personopplysningar, blant anna opplysningar om helse, rase, tru, politisk tilknytning, straffbare handlingar og seksuelle forhold. Datatilsynet kan likevel avgjere at også andre behandlingar av personopplysningar skal vere konsesjonspliktige. Det føreset at behandlinga openbert vil krenkje tungtvegande personverninteresser. Ved vurderinga av personopplysningar skal Datatilsynet ta omsyn til art, mengd og formålet med behandlinga.

Det blei i 2004 gitt 817 konsesjonar, mot 470 året før. Auken kjem av at det er gitt likelydande konsesjonar til blant andre bankar (195) og pensjonskassar (94). Det blei gitt konsesjon til 280 forskingsprosjekt.

Meldingar

Meldeplikta inneber at den som ønskjer å setje i gang behandling av personopplysningar skal orientere Datatilsynet seinast 30 dagar før behandlinga tek til. Det er likevel ein del unntak frå meldeplikta.

I 2004 kom det inn 2 777 meldingar om behandling av personopplysningar som ikkje er konsesjonspliktige. Totalt er det no 14 394 aktivt gjeldande meldingar i meldingsdatabasen. Ca fire tusen meldingar blei sletta frå databasen i 2004, fordi dei er "gått ut på dato".

Klagesaker

I meldingsåret oversende Datatilsynet ni saker til Personvernemnda for vidare klagesaksbehandling:

Statens arbeidsmiljøinstitutt

Klage på konsesjonsvedtak. Saka galdt ein oppfølgingsstudie om kreft og lungesjukdommar blant tilsette i norsk silisiumkarbidindustri. Hovudspørsmålet var om ein skulle krevje informert samtykke for å tillate oppfølgingsstudien, eller om denne kunne baserast på eit av dei andre grunnlaga som personopplysningsloven gir for å kunne behandle personopplysningar.

Personvernemnda omgjorde Datatilsynets vedtak, slik at oppfølgingsstudien kan gjennomførast utan informert samtykke.

Noregs teknisk-naturvitskapelege universitet (NTNU)

Klage frå NTNU om krav om samtykke for framleis å kunne lagre opplysningar frå prosjektet "Helse- og stressreaksjoner hos oljearbeidere i Nordsjøen". Saka galdt om forskaren måtte ha samtykke for framleis å lagre opplysningar (som skulle ha vore sletta i 2002), eller om det var tilstrekkeleg at slikt samtykke blir henta inn når oppfølgingsstudien blir sett i gang.

Klagaren fekk medhald i Personvernemnda. Forskaren fekk dermed løyve til å oppbevare personopplysningane inntil oppfølgingsstudien blir sett i gang, men maksimalt inntil seks månader.

Posten Noreg AS

Saka galdt om Postens utleige av adresselister kunne forankrast i personopplysningsloven § 8 f. Datatilsynet sa nei. Klagar fekk ikkje medhald i Personvernemnda. Saka er elles omtalt ein annan stad i årsmeldinga.

NKS Olavviken Behandlingssenter

Saka gjeld Datatilsynets avslag på å gi konsesjon til prosjektet "Suicidal atferd i Bergensområdet". Datatilsynet avsto søknaden av di dette omfatta opplysningar frå eit prosjekt som skulle vore anonymisert i samsvar med konsesjonsvilkår fastsette i den opphavlege konsesjonen. Saka var i meldingsåret ikkje behandla i Personvernemnda.

Norske Kredittopplysningsbyråers forening

Klage på konsesjonsvilkår. Klagesaka er omfattande, men gjeld i korte trekk tidspunkt for registrering av betalingsmerknader om enkeltpersonar, slettefrist for fordringar som er gjorde opp og behandling av personopplysningar ved berekning av såkalla "rating" for nyetablerte føretak. Saka var i meldingsåret ikkje behandla i Personvernemnda.

Ullevål Universitetssjukehus

Saka gjeld kven som kan sitje med koplingsnøgelen til identifikasjon av prosjektdata. Saka var i meldingsåret ikkje behandla i Personvernemnda.

Telenor

Saka gjeld Datatilsynets pålegg til Telenor om å slette tidlegare kundar. Saka var i meldingsåret ikkje behandla i Personvernemnda.

Finansnæringens Hovudorganisasjon - FNH

Gjeld Datatilsynets vedtak om at helseopplysningar berre kan behandlast av forsikringsselskapa

etter skriftleg samtykke. Saka var i meldingsåret ikkje behandla i Personvernemnda.

Bakehuset Kafe AS

Gjeld kameraovervaking på arbeidsplass. Saka var i meldingsåret ikkje behandla i Personvernemnda.

I tillegg behandla Personvernemnda to saker som var sende inn i 2003. Dette galdt:

Gjensidige Nor Sparebank ASA

Saka galdt spørsmålet om det i Datatilsynets konsesjon til klagaren skal kunne stillast vilkår om at det ikkje utan samtykke frå kunden skal tillatast at eit konsernkunderegister inneheld opplysningar om kva type tenester og produkt kunden har avtale om hos dei ulike selskapa i konsernet. Datatilsynet meinte dette berre kunne skje etter samtykke.

Personvernemnda omgjorde Datatilsynet si avgjerd og gav klagaren medhald i at dette kan skje utan samtykke.

Nasjonalt Folkehelseinstitutt

Klagen galdt nekting av konsesjon for regelmessig overføring av data frå Utlendingsdirektorat til Tuberkuloseregisteret. Vedtaket blei ikkje endra som følge av klagen.

Klagar over enkeltvedtak

Tidlegare skulle Personvernemnda berre behandle enkeltvedtak som Datatilsynet gjer med heimel i personopplysningsloven. Andre enkeltvedtak skulle behandlast av Moderniseringsdepartementet. I ei fråsegn på slutten av meldingsåret har likevel Lovavdelinga i Justisdepartementet komme til at Personvernemnda er rette instans til å behandle klagar over alle avgjerder i Datatilsynet, med unntak av reint administrative avgjerder, som for eksempel tilsynets eigne tilsetjingssaker. For tida har Personvernemnda eitt avvisingsvedtak til behandling.

Lov- og forskriftsarbeid

I 2004 utarbeidde Datatilsynet forslag til endringar i personopplysningsforskrifta. Forslaget går ut på å lette i konsesjonsplikta for forskingsprosjekt som blir tilrådde av ei etisk nemnd. Forslaget er sendt på høring.

Høringssaker

I 2004 kom det inn totalt 124 høringssaker. Datatilsynet gav tilsvaret i 104 av sakene. I dei andre 20

hadde ikkje Datatilsynet merknader, då desse ikkje reiste personvernspørsmål av større interesse. Av høringssaker der det blei gitt viktige innspel kan nemnast:

- ny handlingsplan for elektronisk samarbeid i helse- og sosialsektoren,
- forslag til nye reglar for rapportering og undersøkingar av ulykker og hendingar i luftfarts- og jernbanesektoren,
- utkast til IKT-strategi for justissektoren 2004 – 2007,
- ”Draft guiding principles for the protection of personal data with regard to smart cards”,
- straffegjennomføringsloven,
- individuell plan for einslege mindreårige asylsøkjjarar og flyktningar,
- utkast til ny lov om utdanningsstøtte,
- utkast til lov om supplerande stønad for personar med kort butid i Noreg,
- reglar om buretsregister,
- forslag frå arbeidsgruppe om endringar i tryggleiksloven og forskrift om personelltryggleik,
- NOU 2004:5 Arbeidslivslovutvalget,
- etablering av eit personeintydig helseregister,
- NOU 2004:6 Mellom effektivitet og personvern,
- forslag om å innføre rapporteringsplikt for revisorar,
- lovheimling og etikkomitear og ”Nasjonalt utvalg for uredelighet i forskning”,
- persondatautveksling i Noreg,
- forprosjektrapport om arkitektur for elektronisk samhandling i offentleg sektor,
- ei ny arbeids- og velferdsforvaltning – om samordning av Aetat, trygdestaten og sosialtenesta sine oppgåver,
- IKT-strategi for kriminalomsorga 2005 – 2008,
- ”Fra bruk til gjenbruk”,
- forslag om utprøving av dommarleidd narkotikaprogram i Noreg,
- forslag om endringar i barnevernloven, sosialtenesteloven og smittevernloven,
- blodforskrifta
- utgreiing nr. 12 frå banklovkommisjonen.

4 Deltaking i offentlege råd og utval

Datatilsynet prøver, så langt ein avgrensa kapasitet rekk, å delta i ulike råd og utval, for å sikre at personverninteressene blir varetekne tidleg i planleggingsprosessen. Tilsynet var i meldingsåret representert i desse råda og utvala:

Utval for politimetodar med førebyggjande siktemål

Politimetodeutvalets rapport Mellom effektivitet og personvern (NOU 2004:6) blei lagd fram våren 2004. Sjå nærmare omtale seinare i årsmeldinga.

DNA-utval

Direktøren i Datatilsynet er oppnemnd i eit utval som skal vurdere om høvet til å ta DNA-prøver skal utvidast, for eksempel slik at høvet blir det same som for fingeravtrykk. I tillegg skal utvalet vurdere om det skal opnast for å registrere DNA-profilar i fleire typar av saker og om sikting skal vere eit tilstrekkeleg vilkår for å registrere DNA-profilen til vedkommande. Utvalet skal også vurdere eventuelle endringar i saksbehandlingsreglane for registrering og søk i DNA-registeret. Utvalet skal slutføre arbeidet innan utgangen av 2005.

Vurdering av utval for behandling av uheiderleg framferd i forskning

Datatilsynet er representert i ei arbeidsgruppe nedsett av Undervisnings- og forskingsdepartementet. Arbeidsgruppa skal jobbe med ei mogleg lovfesting av eit utval for uheiderleg framferd i forskning, samt dei forskningsetiske komiteane.

Sertifiseringsordning for informasjonstryggleik

Nasjonal tryggleiksmyndigheit er ansvarleg for sertifiseringsordninga for informasjonstryggleik for IT-utstyr og system (SERTIT). Datatilsynet deltek i styringsgruppa for dette arbeidet. Formålet med deltakinga er å fremje sertifiseringsordninga, slik at ho kan få praktisk nytte for dei som er underlagde tryggingsføresegnene i personopplysningsloven. Det har vore to møte i 2004.

Samarbeidsråd for helsesektoren

Rådet er oppretta av Sosial- og helsedirektoratet med sikte på å koordinere arbeid med informasjonsteknologi i helsesektoren. Arbeidet i gruppa tek utgangspunkt i direktoratet sin strategiplan "E-2007" som handlar om strategi og planar for å fremje bruk av informasjonsteknologi. Formål med samarbeidsrådet er å styrkje samarbeidet aktørane i mellom og med dei sentrale styresmaktene. Datatilsynet deltek som observatør og ser på deltaking i rådet som eit viktig ledd i å kommunisere tilsynet sine standpunkt. Datatilsynet deltok på tre av dei fire møta i rådet.

Bransjenorm for helsesektoren

Sosial- og helsedirektoratet var initiativtakar til eit større prosjekt der formålet er å utvikle ei felles

bransjenorm for helsesektoren. Norma skal medverke til å harmonisere nivået på informasjonstryggleik. Dei kontrollar som Datatilsynet har gjennomført innan sektoren har avdekt eit stort behov for eit slikt felles løft. Ikkje minst gjeld dette tilknyttinga dei ulike aktørane har til det nasjonale helsenettet. Datatilsynet har derfor delteke i styringsgruppa for arbeidet med bransjenorma, og har hjelpt til med råd og rettleiing.

Koordineringsutvalet for informasjonstryggleik - KIS

Utvalet består av representantar for sju departement, Statsministerens kontor og ni direktorat. Koordineringsutvalet blei oppretta som ledd i gjennomføring av ein nasjonal strategi for informasjonstryggleik. Arbeidet omfattar alminneleg IT-tryggleik og spørsmål knytte til rikets tryggleik, vitale nasjonale tryggingsinteresser og kritiske samfunnsfunksjonar. Utvalet skal samordne vida-reutviklinga av regelverket for IT-trygging, få fram felles standardar, normer, metodar og verktøy for IT-tryggleik. Utvalet skal også drøfte aktuelle spørsmål som vedrører risiko og fare for datamisbruk og medverke til koordinering av informasjonstiltak og beredskapsplanlegging. Koordineringsutvalet hadde fire møte i 2004.

Referansegruppe for kravspesifikasjon for digitale signaturar

Datatilsynet deltok som observatør i ei referansegruppe oppretta av Moderniseringsdepartementet i samband med utvikling av ny kravspesifikasjon for digitale signaturar i det offentlege. Formålet med deltaking har vore å fremje tilsynet sine standpunkt i forhold til dette prosjektet. Utgangspunktet for Datatilsynet har heile tida vore at kravspesifikasjonen burde ha som føresetnad kvalifiserte digitale signaturar. Innstillinga frå prosjektet har blitt ein tonivåmodell for digitale signaturar, noko som ikkje er i samsvar med tilrådinga frå Datatilsynet. Datatilsynet si tilråding var elles i samsvar med standpunktet til ei rekkje andre aktørar i referansegruppa.

Internett og misbruk

Ei internettgruppe er etablert av Post- og teletilsynet som eit frivillig ope forum, i hovudsak samansett av internett-aksesstilbydarar og andre som direkte handterer internettrelaterte oppgåver. I 2004 har Datatilsynet særleg teke opp private heimesiders forhold til personopplysningsloven.

Datatilsynet har i tillegg delteke i ei undergruppe som konsentrerer seg om misbruksrelaterte spørsmål knytte til Internett. Datatilsynet har

delteke som observatør i dei to møta som gruppa har hatt i meldingsåret.

5 Internasjonalt samarbeid

Personopplysningar blir i stadig større grad utveksla over landegrensene. For Datatilsynet er det derfor viktig å samarbeide med tilsvarende organ i andre land. Internasjonale samarbeidsforum er dessutan viktige arenaer for erfaringsutveksling. Som det går fram av oversikta nedanfor deltek Datatilsynet i mange ulike samanhengar. Men dessverre er Noreg ikkje trekt inn i det personvernarbeidet som går føre seg innan ramma av Europarådet sine organ.

Artikkel 29-gruppa

Artikkel 29-gruppa har som oppgåve å drive fram koordinering og synkronisering av EU/EØS-landas nasjonale personvernarbeid med utgangspunkt i personverndirektivet frå 1995. Gruppa har ingen avgjerdsrett, men ein rådgivande funksjon overfor Kommisjonen. Det norske Datatilsynet har observatørstatus.

Gruppa tek av eige tiltak opp ei rekkje saker, men blir også bede av Kommisjonen om råd og kommentarar. Sakslista er stor både i breidde og omfang. Og veksande. Dette er ei hovudårsak til at ein har valt å saksførebu gjennom arbeidet i undergrupper som møtest forholdsvis uformelt. Noreg har for tida slutta seg til ei undergruppe som tek føre seg ulike sider ved politiet si verksemd nasjonalt og internasjonalt.

Av aktuelle saker under behandling kan ein elles nemne:

- Haldning til og mogleg regulering av høvet til å programmere PC-ar for automatiske tilbake meldingar.
- Vilkår for utlevering av flypassasjerlister til styresmakter i land utanfor EU til andre formål enn flyselskapas egne.
- Bruk av biometriske data for pass og andre id-dokument.
- Kommersiell utnytting av persondata som stat og kommune hentar inn for sine forvaltningsformål.
- Bruk og bruksvilkår for bruk av den nye RFID-teknologien (dvs. sporing av gjenstandar og personar ved hjelp av radiobølgjer)

Utviklinga av Internett og dei indirekte personvernetruslane som knyter seg til monopol tendensar innan software-sektoren går att i gruppas behandling av fleire saker og tema.

Internasjonalt datatilsynsmøte

Kvart år blir det halde ein internasjonal konferanse for datatilsynssjefar med deltakarar frå heile verda. Polen var vertskap for 2004-konferansen. Konferansen inneheld ein open del som også andre enn datatilsynssjefane kan delta på. Men vel så viktig er den delen av konferansen der møtet berre er ope for datatilsynssjefane. Eit interessant tema i år var spørsmålet om tilgang til arkiva etter dei gamle regima i Polen, DDR og Argentina.

Berlingruppa

Den internasjonale arbeidsgruppa for personvern innan telekommunikasjon (Berlin-gruppa) er primært etablert for å arbeide med tekniske problemstillingar knytte til telekommunikasjon, men behandlar også andre tekniske problemstillingar. Arbeidet i gruppa gir Datatilsynet viktige bidrag i arbeidet med tekniske problemstillingar. Datatilsynet deltok derfor på begge møta som blei haldne i 2004. Sentrale saker i meldingsåret var å utvikle felles innstillingar når det gjeld:

- kommersialisering av lokaliseringsdata frå GSM mobiltelefonnett
- å oppnå tilfredstillande sikring av trådlause nettverk
- føretrekte metodar for å kjempe mot elektronisk kriminalitet med personvernvennlege metodar
- personvern innan medias handtering av personopplysningar. Dette var elles eit spørsmål der dei nordiske landa hadde dissens på grunn av våre føresegner om ytringsfridom.

RIPE (Réseaux IP Européens)

Datatilsynet deltok med ein person på to møte i RIPE i 2004. Møta er eit felles forum for alle som er interesserte i IP-nettverk i Europa. Formålet med forumet er å sikre nødvendig administrativ og teknisk koordinasjon for å etablere eit pan-europeisk IP-nettverk. Diskusjonen i møta er til stor nytte for Datatilsynets arbeid og gjer det mogleg å vere oppdatert på nytt innan IP-teknologi.

Europeisk ekspertgruppe innan teknologi

Etter invitasjon frå det franske datatilsynet deltok Datatilsynet med ein representant på skipingsmøtet for ei ekspertgruppe innan teknologiske spørsmål. Gruppa skal primært tene som nettverk for teknologisk ekspertise i dei europeiske landa. Vidare framdrift for gruppa er ikkje avklart.

OECD

OECD har ei undergruppe som arbeider med informasjonstryggleik og personvern. Datatilsynet

deltok som observatør på eit møte i 2004. Det er Nærings- og handelsdepartementet som utgjer den offisielle norske representasjonen. Sentrale tema i det aktuelle møtet var knytte til digitale signaturar og PKI.

Nordisk teknologimøte

Nordisk teknologimøte er oppretta for å skape god kontakt mellom dei teknologiske miljøa hos personvernstyresmaktene i dei nordiske land. Aktuelle tekniske problemstillingar blir diskuterte med sikte på å komme fram til ei mest mogleg felles handheving av regelverket i dei nordiske landa. Møtet blir halde kvart år, denne gong i Finland. Sentrale problemstillingar på møtet var:

- Digitale signaturar
- Strategi og metodikk ved gjennomføring av operative tilsyn
- Heilautomatiske bomstasjonar. Utveksling av synspunkt på teknologi og løysingar
- Lokaliseringsteknologi ved bruk av GSM-nett.

Nordisk datatilsynsmøte

Danmark var vertskap for møtet. Av sentrale saker som blei tekne opp var blant anna retten til anonym ferdsel i samferdselssektoren og resultatane frå eit felles nordisk tilsynsprosjekt om behandling av personopplysningar ved tilsetjingsprosessar.

Saksbehandlarmøte innan EU/EØS

To saksbehandlarar deltok i 2004 på to møte i regi av det internasjonale samarbeidsforumet for saksbehandlarar ("complaint workshop"). Møta blei haldne i Stockholm og Praha. Saker som blei drøfta var blant anna politimetodar og bruk av politiregister og overvaking i arbeidslivet.

Nordisk saksbehandlarmøte

Møtet blei i år halde på Island og omfatta tema som anonymitet innan samferdsel, elektroniske postjournalar, samordning av offentlege etatar og samtykkeproblematikken innan forskning.

Joint Supervisory Authority (JSA)

JSA er det felles tilsynsorganet for Schengen informasjonssystem (SIS). Informasjonssystemet inneheld opplysningar om personar som er ettersøkte, sakna, nekta innreise til Schengen-området, eller er straffedømde i eit av medlemslanda. Datatilsynet møter med ein fast observatør. Det har i meldingsåret vore eit ekstra høgt aktivitetsnivå. Dette har generelt si årsak i stor aktivitet i Schengensamarbeidet. JSA har i tillegg hatt fellesmøte med

tilsynsorganet for Europol, og tilsvarande når det gjeld tollsamarbeidet.

Sjå eigen omtale av internasjonalt politisamarbeid seinare i årsmeldinga.

6 Informasjon som verkemiddel

Personvernlovgivinga legg i stor grad ansvaret på kvar enkelt når det gjeld å ta vare på sitt eige personvern. Samtidig er alle som behandlar personopplysningar, anten det er offentlege etatar eller næringsdrivande, pålagde vesentlege plikter med omsyn til å etterleve lovgivinga på området. Datatilsynet er derfor avhengig av å bli synleg i samfunnet og å skape ein aktiv debatt, refleksjon og medvit kring sentrale personvernspørsmål. Aktiv kommunikasjonsverksemd er dermed eit verkemiddel det blir lagt sterk vekt på. Dette skjer i første rekkje gjennom mediekontakt, Datatilsynets heimeside og ei svarteneste for publikum ("Frontservice").

Rådgiving om informasjonstryggleik

Datatilsynet har lagt vekt på gi råd og rettleiing til verksemdar som arbeider med å sikre personopplysningar i samsvar med regelverket. I ein del saker krev dette rettleiing i møte, mens mindre kompliserte spørsmål kan takast via telefon eller e-post.

Datatilsynet gjennomførte 70 rettleiingsmøte. I tillegg blei det svart på om lag 700 spørsmål over telefon og 450 e-postbrev om temaet. Desse kjem i tillegg til det som Frontservice har svart på.

Hovudvekta av spørsmåla er knytt til behov for avklaring og fortolking av kravet til forholdsmessig tryggleik, pluss råd om korleis dette kan gjennomførast i praksis. Ein del konsultentselskap, produsentar og leverandørar tek også kontakt for å få ei betre forståing av regelverket.

Tilsvarande blir det halde ei rekkje møte for reine juridiske avklaringar.

Sentralisert betening av svar på spørsmål på telefon- og e-post

Datatilsynet bruker ein vesentleg del av ressursane til å svare på spørsmål som kjem inn via brev, e-post og telefonar. Dei aller fleste av desse blir kanaliserte til ei profesjonalisert førstelinjeteneste, "Frontservice" - tre juristar som også trekkjer på teknologisk kompetanse når dei ser behov for det. Dette sikrar at publikum raskt og enkelt får den faglege rådgivinga som er nødvendig. Etter eitt års erfaring er det tydeleg at publikum set pris på denne løysinga.

2004 var det første heile året med ei systematisk registrering av talet på telefon- og e-postspørsmål til Frontservice. I løpet av året er det blitt registrert at ein har svart på i overkant av 9 000 spørsmål over telefon og 2 258 pr. e-post. Dei reelle tala er likevel høgare, idet ein del telefonoppringingar går direkte til andre saksbehandlarar. Reservasjon/DM, arbeidsliv og fjernsynsovervaking utgjorde nær halvparten av alle brev og telefonar.

Stor mediemerksemd

I forhold til storleik og administrative ressursar var Datatilsynet også i 2004 ein svært synleg aktør i samfunnsdebatten og i mediebildet. Mange ulike saksområde har aktualisert interessa for, og spørsmål om, personvern frå journalistar. Det kan verke som om spørsmål som rører ved personvern er komne meir på dagsorden. Personvern er ei ideell interesse som det er vanskeleg å kommunisere verdien av, når ein skal ta stilling til saker der personverninteressene skal vegast opp mot omsyn som i større grad kan visualiserast og vekke kjensler og engasjement hos folk flest. Dette stiller store krav til måten Datatilsynet kommuniserer på.

Den auka merksemda kring personvernspørsmål ser ein tydeleg i talet på medieoppslag der Datatilsynet er nemnd. Det blei i løpet av 2004 registrert 2 189 nyheitsinnslag på internettsidene til norske medium, mot 1 500 året før. Det reelle talet på nyheitsoppslag er likevel truleg endå høgare enn dette, då mange nyheiter kjem på trykk (eksempelvis i lokal presse) eller på radio/tv utan at desse samtidig blir lagde ut på Internett.

Populær personvernrapport

I tillegg til å utarbeide den tradisjonelle årsmeldinga som blir lagd fram for Stortinget, blei det i 2004 også utarbeidd ei popularisert trykksak, "Personvernrapporten 2004". Denne fekk vesentleg større merksemd enn ved tidlegare tradisjonelle årsmeldingar. Personvernrapporten blei trykt og distribuert i seks tusen eksemplar. Det kom likevel etterpå inn etterbestillingar av eit heilt anna omfang enn tidlegare, deriblant fleire bestillingar av klassesett til vidaregåande skolar og høghøgskolar.

Fokus på kameraovervaking

Det er eit stadig større problem at ulike aktørar som har teke i bruk kameraovervaking ikkje kjener til regelverket på området. Det er eit stort behov for å nå fram med betre kunnskap om regelverket til brukarane av utstyret, då det er desse som også sit med ansvaret.

Datatilsynet utarbeidde derfor ein rettleiar om kameraovervaking. Denne er skriven slik at han skal vere lett forståeleg. Etter at rettleiaren blei distribuert også til ulike regionale og lokale medium kom det mange presseoppslag som fokuserte på problemstillinga. Den auka merksemda førte til så mange tingingar av rettleiaren at ekstra opplag ganske raskt måtte trykkjast opp.

Seminar

Det blei også innleidd eit samarbeid med bransjeforeninga for elektrofag, NELFO. Brosjyren blei som del av dette samarbeidet distribuert til alle medlemmer og ei rekkje andre lesarar av organisasjonen sitt fagblad. Datatilsynet samarbeider også med NELFO om ein større dagskonferanse om kameraovervaking i februar 2005.

Datatilsynets heimeside

Arbeidet med å oppgradere rettleiingar for publikum og behandlingsansvarlege verksemdar har hatt høg prioritet. Det er derfor blitt publisert nye rettleiingar om:

- Publisering av bilete og andre personopplysningar om mindreårige på Internett
- Detaljregistreringar i arbeidslivet
- Personvern knytt til arbeidsliv, medrekna arbeidsgivar sitt innsyn i e-post mv.
- Bruk av fødselsnummer i skole/barnehage
- Internkontroll - spørsmål og svar
- Kameraovervaking
- Overføring av personopplysningar til utlandet
- Meldeskjema er gjorde tilgjengelege også på nynorsk og engelsk

Det blei i meldingsåret publisert 74 eigenproduserte nyheitsartiklar og notisar.

Nær 2 000 personar står på ei abonnentliste for melding om nyheitsoppdateringar på nettstaden. Estimert tal dagleg besøkjande på heimesida er framleis ca 700.

Arbeidet med å etablere ei ny og meir funksjonell heimeside blei sett i gang i 2004. Denne blir lansert i mars 2005.

Seminar og foredragsverksemd

I staden for å bruke ressursar på å administrere eigne kurs- og konferansar satsar Datatilsynet heller på å stille opp med foredragshaldarar på arrangement i regi av andre. Dette ser ut til å ha vore ein vellykka strategi. I 2004 stilte Datatilsynet opp med foredragshaldar på i overkant av 70 ulike seminar og konferansar. Dette er om lag same omfang som året før.

Datatilsynet var initiativtakar til og ein sentral bidragsytar ved ein to dagars konferanse om personvern i kommunesektoren som blei arrangert i regi av Kommunanes sentralforbund.

Personvernombod

Mange bedrifter og organisasjonar behandlar dagleg store mengder personopplysningar.

Er dei usikre på kva som er lovleg eller ikkje kontaktar mange av desse Datatilsynet for å få råd. Fleire verksemdar har likevel sett at det kan vere ei betre ordning på frivillig basis å opprette sitt eige personvernombod.

Personvernombodet er ein ressursperson som kjenner verksemda, kva formål som ligg til grunn for behandlinga av personopplysningar, kva for framgangsmetodar som blir nytta og kva for behandlingssystem som er innførte. Ombodet vil raskt og presist kunne handtere problemstillingar som måtte oppstå. Ikkje minst vil personvernombodet både innetter i verksemda og utetter framstå som ein fagperson med spesialkompetanse, som kan hjelpe til i for eksempel opplæring og klagesaksbehandling. I tillegg opnar oppnemning av personvernombod for lempingar i forhold til den lovpålagde meldeplikta.

Norsk samfunnsvitskapleg datateneste, NSD er personvernombod for alle universitet i landet og dei vitskaplege og statlege høyskolorane. I tillegg har fleire institutt, private høyskolar, helseføretak og sjukehus valt NSD som sitt personvernombod. Til saman er NSD personvernombod for 115 ulike verksemdar.

I tillegg til at ytterlegare 15 verksemdar har oppnemnt NSD som personvernombod, er det i løpet av 2004 komme til følgjande nye verksemdar med personvernombod:

- Kommunane Ballangen, Grane, Hamarøy, Nesna, Steigen og Øksnes har alle oppnemnt Alf Leinan, It-Con A/S som sitt personvernombod.
- Universitetssjukehuset Nord-Noreg HF: Personvernombod Per Bruvold
- Wyeth Lederle Noreg: Personvernombod Reidar Lewis

Status ved årsskiftet er dermed at 8 personvernombod representerer til saman 130 ulike verksemdar.

Seminar for omboda

Datatilsynet arrangerte, som året før, eit seminar over to dagar for nye og allereie etablerte personvernombod. Formålet med seminaret er å gi grunnleggjande opplæring i personopplysningslo-

ven og helseregisterloven, i tillegg til å skape nettverk mellom personvernomboda.

Datatilsynet samarbeidde også med Ullevål Universitetssjukehus om eit seminar som fokuserte på ivaretaking av personvernet ved medisinsk forskning. Bakgrunnen for dette var at sjukehuset har etablert ein organisasjon som medverkar til at verksemda varetek lover og forskrifter innan medisinsk forskning. Etablering av personvernombod internt i verksemda var viktig i dette arbeidet. På seminaret orienterte sjukehuset om korleis arbeidet med ivaretaking av personvernomsyn i forskninga er blitt organisert reint praktisk.

Politiet og kommunesektoren neste?

Datatilsynet har i fleire samanhengar foreslått at det også innan politiet blir utnemnd personvernombod. Ein er derfor nøgd med å kunne konstatere at det i forslag til politiregisterlov (NOU 2003:21) er foreslått at det blir oppretta personvernombod innan politiet. Også i kommunesektoren behandlar ein ei så stor mengd personopplysningar, mange av dei sensitive, at oppretting av personvernombod burde vere naturleg å vurdere for mange kommunar. Større kommunar som allereie har oppnemnt byombod, bør vurdere å leggje også personvern inn i ombodsfunksjonen.

Bransjevisse åtferdsnormer

I personopplysningsloven blir det lagt det opp til at Datatilsynet skal hjelpe til med å utarbeide bransjevisse åtferdsnormer. I meldingsåret slutførte Noregs Idrettsforbund arbeidet med bransjereglar for idrett. Formelt er reglane ennå ikkje vedtekne, men dette vil skje på vårparten 2005. I dette arbeidet har Datatilsynet arbeidd tett saman med Idrettens hovudorganisasjon.

Datatilsynet tek sikte på å arbeide vidare med andre bransjar i kommande år.

7 Tilsyns- og tryggleiksarbeid

Tilsynsverksemda er eit viktig verkemiddel i Datatilsynets arbeid med å fremje eit godt personvern i samfunnet. I tillegg til å kontrollere at regelverket blir etterlevd, er tilsyna også ein viktig kanal for dialog og kunnskapsoverføring, til nytte for både tilsynsobjekta og Datatilsynet.

Datatilsynet har i rapporteringsåret innført såkalla "brevlege tilsyn" som eit supplement til "stadlege tilsyn", eller tilsyn på staden, det vil seie besøk hos tilsynsobjekta. Denne framgangsmåten blir i hovudsak vald ved systemrevisjonar og

ved verifisering av konkret dokumentasjonsplikt. Der behovet for direkte dialog er klårare, er besøk hos tilsynsobjekta framleis mest formålstenleg.

Tilsynsaktiviteten er basert på eit internt utarbeidd kvalitetssystem for tilsyn. Året blir delt inn i to tilsynsperiodar. For kvar periode blir det utarbeidd ein tilsynsplan. Denne omtaler i hovudsak organiseringa av tilsynsaktiviteten og dei tema som danner grunnlag for val av tilsynsobjekt.

Datatilsynet gjennomførte til saman 161 brevlege og stadlege tilsyn i 2004. Oversikta nedanfor viser tilsynsaktiviteten innan forskjellige område:

7.1 Hovudinstrykk

Mange aktørar har framleis manglande kunnskap om regelverket. Dette ser ein i første rekkje gjennom at verksemdene ikkje har etablert ei oversikt over kva for personopplysningar dei faktisk behandlar. Dei har heller ikkje sett i gang nødvendige aktivitetar for å møte dei pliktene dei har etter regelverket. Dei aller fleste tilsynsobjekta får derfor merknad frå Datatilsynet om manglande internkontroll. Dette er alvorleg fordi internkontrollsystemet, og føresegnene om informasjonstryggleik som hører med, skal danne fundamentet i at personvernlovgivinga blir etterlevd.

Tabell 1.1

<i>Bransje / Sektor</i>	<i>Tal</i>
Arbeidsliv	8
Detaljhandel	2
Fjernsynsovervaking	24
Forsking	76 *
Internettrelaterte verksemder	9
Kommune	1
Marknadsførarar	2
Primærhelsetenesta	10
Helseføretak	1
Private / ideelle organisasjonar	7
Telekommunikasjon	5
Samferdsel	7
Trygd	5
Krisesenter	5
Sum	161

*Det blei kontrollert 76 konsesjonar innan forsking. Talet på tilsynsbesøk på staden var 29. Ei fullstendig liste over tilsynsobjekta ligg som eige vedlegg bak i årsmeldinga.

Leiinga sviktar

Rapportane frå tilsynsverksemda viser at eit fleirtal av verksemdene har etablert visse rutinar når det gjeld behandling av personopplysningar. Men desse rutinane er i liten grad sette inn i eit heilskapleg system, tufta på ei vurdering av pliktene i regelverket. Eit viktig element i internkontrollsystemet er å fastsetje ansvar og styringsrett i verksemda. Det er i for liten grad teke initiativ frå leiinga når det gjeld å setje i gang nødvendige aktivitetar og å klargjere ansvar. I den grad det er teke formelle initiativ er desse i liten grad følgde opp av organisasjonen i praksis. Oppbygging, implementering og vedlikehald av eit vel fungerande internkontrollsystem tek nødvendigvis ein del tid og ressursar første gong ein gjer dette.

Store og ressurssterke verksemder burde ha både føresetnadar og tradisjon for systemretta tenking. Erfaringane frå tilsynsverksemda tyder likevel ikkje på nokon samanheng mellom kor stor verksemda er og om ein har etablert eit internkontrollsystem. Det avgjerande er kva for kunnskapar og haldningar leiinga i verksemdene faktisk har i forhold til dette arbeidet.

Datatilsynet minner om at etablering av eit internkontrollsystem er eit lovpålagt krav, som verksemdene ikkje lenger kan nedprioritere eller setje heilt til side.

Manglande systematikk

Når det gjeld informasjonstryggleik, har dei fleste verksemder etablert tryggingstiltak, men det viser seg å mangle systematikk også i dette arbeidet. God tryggleik føreset ein systematisk prosess. Kva verksemda meiner er ein tilfredsstillande informasjonstryggleik skal fastleggjast, risiko skal kartleggjast og nødvendige tiltak skal gjennomførast. Mangel i forhold til å etablere struktur og innhald i denne delen av internkontrollsystemet er framleis framståande.

Dårleg tryggleik ved elektronisk samhandling

Samhandlinga mellom publikum/kundar og offentlege og private verksemder skjer naturleg nok i aukande grad ved hjelp av elektroniske hjelpemiddel. Publikum ventar at det skal vere mogleg å kommunisere via Internett og e-post, om ein ønskjer det. Verksemdene på si side ser på dette som ein sjanse til både å gi betre service og å effektivisere kundedialogen. Datatilsynet erfarer likevel at den infrastrukturen som blir bygd opp for den elektroniske samhandlinga ofte ikkje er god nok. Mange verksemder nyttar dårleg sikra e-postløyseringar og tilbyr løysingar på Internett med ein utilstrekkeleg grad av tryggleik.

Publikum har stort sett tillit til at verksemder dei oppfattar som seriøse og skikkelege, også tek vare på tryggleiken i dei elektroniske løysingane dei oppfordrar publikum til å nytte seg av. Brukarane vil derfor ikkje reservere seg mot å kommunisere også sensitive personopplysningar, dersom dei ikkje tydeleg blir åtvare mot det. I den grad elles ansvarlege verksemder tilbyr løysingar som reelt sett er lite sikre, medverkar dette til at publikum heller ikkje i andre samanhengar stiller spørsmål ved tryggleiken i løysingane.

Bildet er likevel ikkje eintydig negativt. Datatilsynet har gjennom si tilsynsverksemd også sett løysingar der informasjonstryggleiken verkeleg er teken på alvor, samtidig som det er teke omsyn til kostnader, effektivitet og at systemet er brukarvennleg.

Nasjonal satsing nødvendig

Erfaringane Datatilsynet har hausta dei siste åra understrekar behovet for ei nasjonal satsing for å etablere ein tilfredstillande infrastruktur for trygg samhandling via elektroniske medium. Moderniseringsministeren har i den samanhengen teke viktige initiativ for å fremje elektroniske signalurar.

Brot på sletteplikta

Personopplysningar som ikkje lenger er nødvendige for formålet med registreringa skal slettast. Dei tilsyn som er gjennomførte viser likevel at brot på sletteplikta går att. Problemet ser ikkje ut til å vere knytt til nokon spesiell sektor, men er gjennomgåande.

Verksemdene har i liten grad fastsett retningslinjer og tilhørande rutinar for sletting av overskottsinformasjon. Inntrykket er at mange vel å framleis lagre personopplysningar sjølv om ein er klar over desse eigentleg skulle vore sletta. Det kan ikkje utelukkast at verksemdene rett og slett vurderer det slik at kostnadene ved framleis å oppbevare personopplysningar er lågare enn kostnadene ved å ha rutinar for gjennomgang og sletting. Ein lagrar også for det tilfelle at ein, av årsaker ein ikkje har oversikt over i dag, kanskje likevel ein gong i framtida kan dra nytte av personopplysningane.

Publikums rett til innsyn

I følgje personopplysningsloven skal den behandlingsansvarlege hjelpe den registrerte med å gi innsyn i kva for personopplysningar som er lagra, kva dei skal brukast til, og kvar dei er henta frå.

Verksemdene fortel at dei registrerte i liten grad krev innsyn ved å vise til personopplysningsloven. Innan offentleg forvaltning er innsynsretten i praksis langt på veg også ivareteke av offentleglov, forvaltningslov og særlovgivinga. I privat sektor blir det å gi innsyn i registrerte opplysningar oppfatta av mange verksemder som ein naturleg del av kundeservice og dialog. Datatilsynet vil likevel minne om at den behandlingsansvarlege må sørge for å ha retningslinjer for korleis ein tek seg av den registrerte sin innsynsrett etter personopplysningsloven. Ikkje minst er det også viktig at reglane blir gjorde kjende for dei av organisasjonen sine medarbeidarar som møter publikum.

Personvern - hemske for utvikling?

Personvern ser ut til å komme under stadig sterkare press når det blir vege mot andre omsyn. Krav til rasjonalitet og effektivitet er stikkord i denne samanhengen. Verksemder, i aukande grad også innan offentleg sektor, tek ikkje tilstrekkeleg omsyn til personvernet. Somme let også heilt vere å vurdere konsekvensane for personvernet når nye løysingar og tiltak blir etablerte. Fleire aktørar gir også direkte uttrykk for at dei opplever omsynet til personvern som ein hemske i utviklinga. Gjennom tilsynsverksemda blei det for eksempel avdekt at somme medisinske forskarar rett og slett hadde valt å ikkje ta omsyn til konsesjonsvilkåra frå Datatilsynet. Dette kan vere signal om ei svekt forståing og respekt for intensjonane bak personvernlovgivinga.

Datatilsynet erfarer også i aukande grad at tilsynsobjekta markerer usemje i forhold til dei vedtak som tilsynet gjer i samband med tilsynsverksemda. Vedtaka blir påklaga til Personvernemnda. Årsaka til dette kan dels liggje i at det er blitt gjennomført langt fleire tilsyn enn tidlegare, samtidig som Datatilsynet er tydelegare i si fortolking av regelverket enn når personopplysningsloven var heilt ny. Problemstillingar som har komme opp i samband med tilsynsaktivitetane, kan derfor ha lege latent i lang tid.

Behandlinga av klagane i Personvernemnda medverkar i alle tilfelle til klargjering og presedens for tilsvarande saker som dukkar opp seinare.

Internasjonaliseringa gir utfordringar

Datatilsynet får stadig større utfordringar når det gjeld det å føre tilsyn med selskap som har aktivitet i fleire land og der den behandlingsansvarlege har hovudsete utanfor våre landegrenser. Dette gjeld endå om selskapa er etablerte innanfor EØS-området, der EUs personverndirektiv gjeld. I prinsippet

skal slike tilsyn varetakast ved ei koordinering mellom tilsynsstyresmaktene i respektive land. Men ei slik koordinering fører til ein god del meirarbeid og byr ofte på praktiske problem. Blant anna er det store variasjonar landa i mellom når det gjeld omfang og organisering av den operative tilsynsverksemda. Datatilsynet er i dialog kring dette med andre land, særleg dei nordiske.

7.2 Større tilsynsprosjekt

Datatilsynet valde i 2004 å organisere noko av tilsynsaktiviteten som større prosjekt. Denne organiseringa blei vald for sektorar der det blei vurdert som viktig å setje inn ressursar for ei ekstra grundig, og dermed ressurskrevjande, kartlegging. Det blei gjennomført prosjektbaserte tilsyn innan følgjande område:

- Kriesesenter
- Elektronisk kommunikasjon innan helsesektoren
- Trygdeetaten
- Medisinsk forskning

Tilsynsprosjektet om medisinsk forskning blir omtalt under temadelen seinare i årsmeldinga. Det blei også gjennomført eit forprosjekt når det gjeld behandling av personopplysningar innan idretten. Dette prosjektet vil bli følgd vidare opp i 2005.

Kriesesentera

Kriesesentera var opphavleg etablerte med lokal frivillig arbeidsinnsats og verksemda har aldri vore lovregulert. Dette har gitt utfordringar, blant anna i forhold til teieplikta. Forhold av svært personleg art kan lett eksponerast i lokalsamfunnet. Konseksjonane, som i si tid blei utferd med heimel i den tidlegare personregisterloven, følgde derfor ein svært restriktiv praksis. Kriesesentera fekk berre registrere namn og adresse på brukarane, og då i første rekkje for omadressering av post.

Mykje har endra seg sidan dei første kriesesentera dukka opp på første halvdel av 1980-tallet. Personopplysningsloven har erstatta den tidlegare personregisterloven. Samtidig har mange kriesesenter utvikla seg til å yte fleire tenester enn berre å fungere som ein tilfluktsstad for mishandla kvinner.

Datatilsynet organiserte derfor i 2004 eit tilsynsprosjekt overfor kriesesentera. Først blei det sendt ut eit kartleggingsskjema til i alt 50 kriesesenter. Etter å ha motteke tilbagemeldingar frå 39 senter, blei fem valde ut for tilsynsbesøk.

Det er særleg tre spørsmål Datatilsynet har vore oppteke av i prosjektet:

- retten til anonymt opphald

- teieplikt/utlevering av opplysningar
- registrering av opplysningar om tredjeperson

Retten til anonymt opphald

Retten til å opphalde seg anonymt på kriesesenteret har lenge vore eit viktig prinsipp for Datatilsynet. Eit fleirtal av kriesesentera svarte i kartlegginga at kvinnene blir gitt høve til å opphalde seg anonymt. Tilsynsbesøka avdekte likevel at det berre var eitt av fem kriesesenter som gjorde det reelt mogleg å ha anonymt opphald. Det blei likevel ikkje gjort identitetssjekk ved nokon av sentera. Etter dialog med kriesesentera ser Datatilsynet at det kan vere gode grunnar for at kvinna skal opplyse om namnet sitt under opphaldet. Primært er dette knytt til å ta vare på kvinna sine eigen tryggleik, for eksempel ved akutte sjukdomssituasjonar, evakuering og liknande. Dette behovet er likevel mindre for dagbrukarar enn for dei som bur der.

Utlevering av opplysningar

Fordi kriesesentera ikkje er regulerte av særlover, er samtykke til behandling av personopplysningar heilt grunnleggjande. Samtykkekravet vil som hovudregel gjelde også ved utlevering av opplysningar til barnevernet.

Dei aller fleste kriesesentera opplyser at dei har som hovudregel at kvinna skal gi sitt samtykke før barnevernet eventuelt blir kontakta. Hovudregelen blir broten dersom situasjonen blir vurdert til å vere svært alvorleg med omsyn til liv og helse for barnet. Datatilsynet er tilfreds med at leiarane ved kriesesentera ser ut til å ha eit svært bevisst forhold til denne problemstillinga.

Ved utveksling av opplysningar til andre institusjonar og etatar ser kriesesentera gjennomgåande ut til å vere påpasselege med å innhente samtykke til utvekslinga. For lagring av opplysningar til bruk for eventuell seinare rettssak, og til bruk under opphaldet, ser det likevel ikkje ut til å liggje føre tilfredsstillande samtykkeerklæringer.

Registrering av opplysningar om tredjepersonar

I tillegg til opplysningar om kvinna registrerer ein også opplysningar om andre familiemedlemmer, i første rekkje barn. Barne- og familiedepartementet har dessutan utarbeidd relativt detaljerte skjema som i utgangspunktet ikkje skal vere knytte til kvinna, eller tredjeperson, sin identitet. Datatilsynet ser det likevel som urovekjande at skjema for bebuarar og dagbrukarar gir informasjon også om overgriparen, og at desse

opplysningane blir oppbevarte saman med opplysningar om kvinna.

Vidare oppfølging

Med bakgrunn i kartlegginga, og tilsyna på staden, har Datatilsynet utarbeidd eit utkast til retningslinjer for krisesentera. Dei tek utgangspunkt i korleis Datatilsynet meiner at personopplysningsloven bør tolkast og nyttast i forhold til krisesentera. Retningslinjene er sende til dei instansar dei vedgår for uttale. Dei vil deretter bli formidla i ei endeleg form til alle krisesenter.

Elektronisk kommunikasjon i primærhelsetenesta

Hausten 2004 gjennomførte Datatilsynet eit tilsynsprosjekt som sette fokus på elektronisk kommunikasjon i primærhelsetenesta. Prosjektet var ei direkte vidareføring av den jamlege tilsynsaktiviteten som Datatilsynet har hatt mot helsesektoren sidan 2002. Målet med prosjektet var å kartlegge nokre av dei utfordringane som primærhelsetenesta møter ved å ta i bruk elektronisk kommunikasjon mot helseføretaka og dei andre instansane innan helsesektoren, og i dialog med pasientane deira. Korleis regelverket blir etterlevd meir generelt med omsyn til internkontroll og informasjonstryggleik blei også kontrollert.

Det blei gjennomført ti tilsyn som ledd i prosjektet. Fem tilsyn på staden og fire per brev var retta mot legekontor, og eitt tilsyn på staden mot helseføretak. Det blei også halde møte med to leverandørar av programvare for elektronisk kommunikasjon.

Tilsyna viste at ansvarsforholda var rimeleg avklarte når det gjeld legekontoras oppkopling mot dei regionale helsenetta. I forhold til leverandørane av programvare for elektronisk kommunikasjon hadde legekontora likevel mindre oversikt og var mindre klar over kven som har ansvar for kva. Datatilsynet konstaterte også at ikkje alt var like klårt når det galdt utveksling av meldingar mellom legekontora og andre aktørar innan helsevesenet.

Erfaringane frå tilsyna tyder på at primærhelsetenesta i svært liten grad har etablert ein tilfredsstillende internkontroll når det gjeld behandling av helseopplysningar. Sju av ni legekontor fekk derfor varsel om pålegg grunna manglande etterleving av føresegnene om internkontroll i helseregisterloven, mens åtte av ni fekk pålegg som følgje av manglande etterleving av tryggleiksføresegnene.

Også helseføretaket fekk pålegg om å rette opp manglande etterleving av føresegnene om internkontroll og informasjonstryggleik.

Forsvarleg i Trygdeetaten

Trygdeetaten omfattar Rikstrygdeverket, 500 einingar på fylkes- og kommunenivå, og har om lag 9 000 tilsette. Trygdeetaten har sensitive personopplysningar om nær sagt alle innbyggjarar i landet. Datatilsynet ønskte derfor å få betre oversikt over trygdeetaten si handtering av personopplysningar - særleg om vilkåra for dei ulike behandlingane av personopplysningar er oppfylte, korleis rettane til den registrerte blir tekne vare på, og om opplysningane blir godt nok sikra. Tilsynet fokuserte på internkontrollsystemet og implementeringa av dette.

Det blei gjennomført tilsyn hos Rikstrygdeverket sentralt, ved to fylkestygdekantor og to lokale trygdekantor. Sjølv om dette har vore det mest omfattande tilsynsprosjektet Datatilsynet har utført i ei og same behandlingsansvarlege verksemd, er likevel ikkje alle behandlingar av personopplysningar i etaten kartlagde. Til det er omfanget av verksemda i Trygdeetaten for stort.

Resultatet av tilsynet var oppløftande og gav eit positivt inntrykk av Trygdeetaten. Rutinane for handtering av personopplysningar i verksemda såg totalt sett ut til å vere svært gode, og var tydeleg forankra i avgjerder frå leiinga. Det såg ut til å vere viktig for leiinga og verksemda som heilskap at personopplysningar blir behandla korrekt og forsvarleg. Det ser ut til at Trygdeetaten har lagt til grunn at godt personvern er ein føresetnad for at etaten kan oppnå den tillit ein ønskjer i befolkninga.

Endå om Datatilsynet kunne konstatere at Trygdeetaten si behandling av personopplysningar i all hovudsak skjer i samsvar med regelverket, blei det avdekt enkelte avvik. Det er behov for ytterlegare utvikling av rutinane knytte til situasjonar der medlemmer ber om innsyn i opplysningar om seg sjølve. Rikstrygdeverket må også klargjere lagringsbehovet for opplysningar om misbruk av trygdemidlar når mistanken seinare blir fråfallen. Det må blant anna etablerast rutinar for sletting i samsvar med dette. Vidare må Rikstrygdeverket vidareutvikle rutinane i internkontrollsystemet, slik at ein har endå betre tryggleik for at avvik frå fastlagde rutinar blir handtert av rett nivå i organisasjonen.

7.3 Kort om andre tilsyn

Her nemner ein kort nokre av dei andre tilsyna som blei gjennomførte i 2004, men som ikkje blir nærmare omtalte i temadelen seinare i årsmeldinga.

Detaljhandel/fordelskort

Datatilsynet gjennomførte tilsyn mot to aktørar som nyttar såkalla fordelskort. Den som nyttar eit slikt kort får eit utbyte, rekna ut frå kva vedkommande kjøper hos kjeda. Kunden på si side aksepterer at opplysningar som kortnummer, tidspunkt og beløp blir overførte til eit sentralt kunderegister. Desse opplysningane blir blant anna nytta til marknadsføring og statistikk.

Tilsynet er av den oppfatning at aktørane er opptekne av personvern, og at kunnskapen om personopplysningsloven er god. Dette skuldast nok for ein stor del at bransjen er avhengig av tillit frå medlemmene, og at eit brot på personopplysningsloven kan få følgjer for forretningsverksemda.

Internettleverandørar

Hovudfokuset for Datatilsynet ved tilsyn mot leverandørar av internett-tilgang for private var å kontrollere kva praksis verksemdene hadde med omsyn til lagring og sletting av personopplysningar, utlevering av desse, pluss forvaltning av e-postkontoar for kundane.

Det blei ikkje avdekt at det blir registrert kva sider internettbrukarane besøkjer, eller kva åtferd brukarane har ved oppkopling mot Internett. Slik logging ville i følgje internettleverandørane dessutan ha vore svært ressurskrevjande å gjennomføre.

Nokre av internettleverandørane gav til kjenne ein liberal praksis med utlevering av trafikkdata til politiet. Det blei sjeldan bedt om formell rettsavgjerd før materialet blei overlevert til politiet.

Datatilsynet påpeikte overfor fleire av verksemdene at sikring av e-posten til kundane ikkje var tilfredstillande. Unødvendig mange tilsette hadde etter Datatilsynets meining høve til å tileigne seg brukarnamn og passord til kundane. Leverandørane må sikre passordfilene betre, for eksempel ved at desse blir krypterte. Datatilsynet ser på dette som eit mellombels problem, då struktur for elektronisk identifisering og digitale signaturar er i ferd med å utviklast. Slike løysingar vil truleg ta over for det tradisjonelle brukarnamnet og passordet.

7.4 Styringssvikt i organisasjonen?

Trygdeetaten har vist at det let seg gjere å innføre eit vel fungerande internkontrollsystem. Ein må da spørje seg: Korfor har Trygdeetaten fått det til, mens ei systematisk tilnærming til internkontroll er nærmast fråverande i mange av dei andre verksemdene Datatilsynet har ført kontroll med?

Hos mange verksemdar blir det ikkje oppfatta som naturleg eller viktig å etablere eit strukturert system for styring av verksemda. Jamvel i store

verksemdar kan Datatilsynet konstatere at det er ein manglande kompetanse i forhold til å etablere einskaplege system. Styringa av verksemda skjer etter heilt andre mekanismar enn kva regelverket føreset. Å ha ei systematisk tilnærming til internkontroll, som i utstrekt grad byggjer på same konsept som system for kvalitetssikring, kjennest derfor fjernt for mange. I andre verksemdar kan kompetansen vere tilstades, men ein set ikkje på dagsorden å etterleve offentleg regelverk.

Moderne regelverksutvikling er tufta på føresetnaden om eit strukturert pliktsubjekt. Ein føreset at den ansvarlege tek ansvar og handlar. Dette inneber å sørge for at noko konkret skjer i verksemda. Ingen tilsynsorgan ventar at den øvste leiaren for verksemda sjølv skal gjennomføre dei pålagde pliktene. Den ansvarlege skal likevel syte for å utløyse handling. Ofte blir store delar av arbeidet med tilpassing til regelverket delegerte til mellomleiarar i verksemda. Dette kan vere både ein føremålstenleg og riktig strategi, men det fritek likevel ikkje den øvste leiinga for sitt ansvar og plikt til oppfølging. Det systemet som blir bygd opp i linjeorganisasjonen må bli tildelt den makt og autoritet som eit leiingssystem krev. Dette føreset at den øvste leiinga for verksemda er til stades og har fokus på dette.

For den øvste leiaren handlar altså spørsmålet i stor grad om å delegere oppgåver eller plikter, forvisse seg om framdrift, gi fullmakter i samsvar med internkontrollsystemet og sørge for ei systematisk oppfølging og periodisk gjennomgang. Kor stor verksemda er, vil vere svært vesentleg for korleis dette blir løyst i praksis.

Datatilsynet konstaterer i mange av sine tilsyn at den øvste leiaren ikkje har teke det ansvaret som regelverket føreset. Korleis verksemda etterlever regelverk vil då ofte vere basert på initiativ frå linjeleiinga. I nokre tilfelle kan dette gi eit tilfredstillande resultat, men i dei fleste tilfelle manglar den autoriteten som internkontrollen føreset.

Leiarskap handlar framfor alt om å ta ansvar, vise veg og setje standard i forhold til korleis verksemda skal opptre. Internkontrollsystemet er eit verktøy i utøvinga av dette leiarskapet.

8 Tema 2004

8.1 Direkte marknadsføring

Over ein million reserveverte

Ved utgangen av året hadde 1 036 296 personar registrert seg i reservasjonsregisteret i Brønnøysund. Registeret blei oppretta 1. januar 2001 for at privatpersonar skulle kunne reservere seg mot telefonsal og adressert reklame. Sidan den gong

har det vore ei stadig aukande tilstrøyming av personar som ønskjer slik reservasjon. Talet på reserverte er nær dobla berre i løpet av det siste året. Av alle reserverte har 99 prosent reservert seg mot telefonsal, 88 prosent vil ikkje bli kontakta av humanitære og samfunnsnyttige organisasjonar, mens 56 prosent ikkje ønskjer å få adressert reklame i posten.

Tabellen nedanfor gir oversikt over utviklinga i talet på dei som har reservert seg i det sentrale reservasjonsregisteret sidan det blei oppretta i 2001 og fram til årsskiftet 2004. Tala viser det samla talet på registrerte ved utgangen av kvar enkelt år:

Pr. 31.12. 2001	233 863
Pr. 31.12. 2002	352 486
Pr. 31.12. 2003	599 425
Pr. 31.12. 2004	1 036 296

I tillegg til at svært mange reserverer seg, er eit stort tal misnøgde med måten reservasjonsordninga fungerer på. Dette til saman tilseier at ein bør sjå nærmare på heile ordninga. Berre i løpet av 2004 mottok Datatilsynet omkring 1 800 klagar frå folk som hadde reservert seg, men som likevel blei oppringde av seljarar.

Førespurnadene til Datatilsynet viser at det er ulike grunner til at folk mottek uønskt marknadsføring. Det kan vere at enkeltpersonar er registrerte i forskjellige register med ulike variasjonar i namnet, dei har fått ny adresse, dei får telefonar i namn av å vere ein juridisk person, eller marknadsførarane følgjer ikkje reglane med vask mot det sentrale reservasjonsregisteret godt nok.

På bakgrunn av dette vil Datatilsynet sjå nærmare på reservasjonsordninga. Ein av ideane som har vore lufta i den samanheng er at den direkte marknadsføringa kan baserast på førehandssamtykke og ikkje reservasjon. Det vil altså seie at ein må gjere ei aktiv handling for å bli utsett for marknadsføring, i motsetning til i dag der ein sjølv aktivt må be om å ikkje få det.

Endringar i marknadsføringsloven?

Datatilsynet har hatt forslag til endringar i marknadsføringslovens § 2 b om forbod mot ubeden e-postreklame og liknande til høring. I si høringsfråsegn gav tilsynet full tilslutning til at fysiske personar generelt bør dekkjast av kravet om førehandssamtykke ved direkte marknadsføring. Også juridiske personar bør få ei viss form for vern mot direkte marknadsføring. Kvar veke blir tilsynet kontakta av næringsdrivande som er oppgitte over mengda av direkte marknadsføring som dei ikkje

får stoppa. Særleg små enkeltmannsføretak føler dette som eit stort problem.

Tips ein venn

I høringsfråsegna kommenterte Datatilsynet også behovet for ei rettsleg avklaring når det gjeld "tips ein venn"- funksjonar. Desse har blant anna vore nytta i reklamekampanjar. Eit av problema er at det på denne måten skjer ei spreiding av personopplysningar som den enkelte sjølv ikkje har kontroll over. Det må i alle fall vere klare avgrensingar når det gjeld bruk av den oppgitte informasjonen utover å oppfylle den oppgåva vennen har akseptert. Tilsynet er likevel skeptisk til ordninga som heilskap, ettersom ho rokkar ved det grunnleggjande personvernrettslege prinsippet om at alle skal ha kontroll over sine egne personopplysningar. Mistar ein denne kontrollen, mistar ein til ein viss grad sjansen til å nytte seg av dei rettane personopplysningsloven tillegg kvar enkelt, særleg når det gjeld innsyn, retting og sletting. Dette nettopp fordi ein ikkje veit kvar eins egne personopplysningar tek vegen.

Tipsdatabase for mogleg brot på reservasjonsretten

Datatilsynet har oppretta ein tipsdatabase for intern bruk. Klagar frå publikum som hevdar at namngitte verksemdar ikkje respekterer reservasjonsretten, blir registrerte jamleg. Ordninga gir dermed godt høve til å følgje opp dei verksemdene som det særleg blir klagt over, for eksempel ved å komme på tilsynsbesøk til dei.

På bakgrunn av den systematiske registreringa kalla Datatilsynet inn leinga hos ein direkte marknadsførar til møte, med krav om forklaring på korfor tilsynet hadde motteke så mange klagar retta mot nettopp denne verksemda. Metoden viste seg å vere svært effektiv, idet det etter møtet ikkje er komne fleire klagar på den aktøren.

Adresselister frå Posten

Posten Noreg AS har eit register over dei fleste privatpersonar som bur i Noreg; Postmottakarsystemet (PMS). Ei registrering i Postmottakarsystemet er nødvendig for distribusjon av post, og skjer ved innrapportering frå postbod, gjennom meldingar om adresseendringar og gjennom datavask mot Folkeregisteret.

Posten vende seg til Datatilsynet då dei ønskte å leie ut adresselister frå dette registeret. Adresselistene skulle ikkje innehalde personar som er reserverte i det sentrale reservasjonsregisteret i Brønnøysund, personar under 15 år, personar med hemmeleg adresse eller døde personar. Datatilsynet

net gav Posten Noreg lov til å bruke adresselister over privatpersonar til å korrigere opplysningar i andre lister (listevask). Men Datatilsynet avsla at Posten skulle kunne leige ut adresselistene. Avslaget blei påklaga til Personvernemnda.

Personvernemnda fann, som Datatilsynet, at utleige av adresselistene er i strid med det opphavlege formålet; å drive postformidling. Formålet med Postens adresseregister er at post skal kunne fordelast til rett mottakar. Formålet med utleige av listene er derimot vidareformidling av adresseopplysningar til andre aktørar som ønskjer å betale for å bruke posten sine lister. Nemnda viser også spesielt til forarbeida til personopplysningsloven, som understrekar at det skal leggjast vesentleg vekt på omsynet til privatlivets fred i avveginga mot kommersielle interesser. Datatilsynet sitt vedtak blei derfor oppretthalde.

8.2 Offentleg forvaltning

Datatilsynet har i løpet av året motteke ei rekkje høringar som reiser sentrale spørsmål om behandling av personopplysningar i offentlig sektor. Felles for mange av initiativa er ønsket om å få til ei meir kostnadseffektiv og brukarretta offentlig forvaltning, i tråd med regjeringas moderniseringsprogram. Nokre av tiltaka det er gjort framlegg om inneber lagring av store mengder personopplysningar i sentrale databasar, eventuelt at det blir etablert portalar for utveksling av personopplysningar forvaltinga imellom. Eksempel på dette er Moderniseringsdepartementet sine planar om ein felles offentlig it-arkitektur og etablering av ein database med grunndata for det offentlege til bruk av ulike forvaltningsorgan. Vidare Helse- og omsorgsdepartementets "Norsk pasientregister" og Utdanningsdepartementets sentrale elevregister knytt til nasjonale prøver.

Det effektive ikkje alltid det rette

Det er naturleg, og i dei fleste samanhenger også rett, at ein også i offentlig sektor tek i bruk ny informasjonsteknologi for å effektivisere og rasjonalisere sine saksbehandlingsprosessar 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 i tillegg også ein ikkje uvesentleg grad av makt- og myndigheitsutøving. Det offentlege må derfor, i tillegg til økonomisk rasjonalitet, også leggje vekt på

omsyn som rettstryggleik, personvern og medverknad for alle delar av befolkninga. Det er i siste instans opp til dei øvste politiske styresmakter å vege reine effektivitetsomsyn opp mot slike grunnleggjande rettar.

Sentrale databasar

Datatilsynet ser med uro på ei utvikling mot store sentrale databasar med personopplysningar. Ut frå personvern- og rettstryggleiksomsyn kan det i mange samanhengar faktisk vere formålstenleg at personopplysningar framleis blir lagra på ulike stader i forvaltinga og at manglande standardisering hindrar "fri flyt" av opplysningane. Det at det krev ein del ressursar å samle inn og samanstillе personopplysningar frå ulike kjelder kan også medverke til mindre misbruk. Menneskelege "portvakter", som stiller spørsmål ved om det er rett og nødvendig å gi ut personopplysningane, kan også redusere unødig spreiding. Dersom ein fjernar desse hindringane når ein etablerer nye og meir effektive løysingar, må det i staden byggjast inn andre mekanismar som reduserer potencialet for at personopplysningar blir spreidde unødig eller misbrukte.

All erfaring tilseier dessutan at etableringa av store databasar med godt strukturerte personopplysningar raskt fører til eit press for at opplysningane også skal takast i bruk til heilt andre formål enn dei opphavleg blei samla inn for.

Felles it-arkitektur og felles grunndata

Moderniseringsdepartementet sende hausten 2004 ut to rapportar til høring, "Forprosjektrapport om arkitektur for elektronisk samhandling i offentlig sektor" og rapporten "Persondatautveksling i Norge". Begge rapportane tek opp korleis det offentlege betre kan utveksle og nytte persondata. Men rapportane har ein så overlappande og uoversiktleg tematikk at det var vanskeleg for Datatilsynet å ta stilling til innhaldet. Rapportane er lite konkrete med omsyn til mål, analysar, tiltak og konsekvensar. Vurderingar med omsyn til personvern og informasjonstryggleik er nærmast heilt fråverande. Ein har stort sett nøgd seg med å gå rett på lettvinde konklusjonar om at fordelane ville overstige dei moglege ulempene for personvernet, eller at slike spørsmål var det andre prosjekt som tok hand om. Lov og regelverk, inkludert personvernlovgivinga, blir i den eine rapporten omtalt som "hindringar" for dei nye og effektive løysingane som ein vil etablere. Dette kan vere uttrykk for ei manglande forståing for dei omsyna og gjennomtenkte vurderingane som ligg bak dagens personvernlovgiving i Noreg og Europa elles.

Maktforskyving

Rapportane tek til orde for å få til meir gjenbruk og ei meir effektiv utnytting av forskjellige typar grunndata på tvers av forvaltninga. Ein vesentleg del av den informasjonen som skal utvekslast vil naturleg nok vere personopplysningar. Det at offentlege styresmakter får enklare tilgang til ei stadig større mengd opplysningar om kvar enkelt borgar, utan å vere i direkte kontakt med vedkommande, kan isolert sett medverke til ei svært effektiv forvaltning. Men det kan også vere med å føre til sterkare maktforskyving frå kvar enkelt borgar til styresmaktene.

"Min side"

Moderniseringsdepartementet skal etablere ei felles inngangsdør til offentlege tenester på Internett i løpet av sommaren 2005. Gjennom "Min side" skal borgarane kunne få tilgang til digitale tenester uavhengig av kva for sektor eller forvaltningsnivå som tilbyr tenestene.

Innsyn gir betre personvern

Etableringa av "Min side" kan gjere det lettare for kvar enkelt å kontrollere kva for personopplysningar som ulike statlege og kommunale etatar har registrert om vedkommande. Det er også mogleg å etablere løysingar som varslar den det gjeld når ulike forvaltningsorgan utvekslar opplysningar om vedkommande. Betre høve til innsyn vil medverke til auka kvalitet i dei personopplysningane som forvaltningsorgana nyttar seg av, ved at feil i opplysningane blir oppdaga og retta, og overskottsinformasjon blir sletta. På denne måten kan "Min side" medverke til, ikkje berre ei meir effektiv og brukarvennleg forvaltning, men også til eit betre personvern. Men dette føreset at omsyna til personvern og informasjonstryggleik blir tekne inn som sentrale premisser allereie tidleg i planlegginga.

Ulike brukarar - ulike føresetnader

Når det offentlege skal etablere løysingar der ein oppfordrar alle til å ta i bruk dataverktøy i deira dialog med forvaltninga, må det også etablerast tryggleiksløysingar som tek høgd for at brukarane har høgst ulike føresetnader for å medverke til oppfyljing av den samla informasjonstryggleiken ved bruk av tenestene. Det er ei kjensgjerning at mange private databrukarar i liten grad tek i bruk heilt elementære tryggleiksløysingar, eksempelvis viruskontroll, brannmur, passord og annan konfigurasjonskontroll. Og, i endå mindre grad, elektronisk signatur og kryptering som i dag er nødvendig for

sikker kommunikasjon. Mange er også framleis avhengige av å nytte offentleg tilgjengelege PCar for eksempel på bibliotek, skolar og internettkafear.

Datatilsynet har derfor overfor Moderniseringsministeren peikt på behovet for at det blir gjort tryggleiksvurderingar og tilpassingar av løysingar også med tanke på dei store variasjonane med omsyn til dataverktøyet til sluttbrukarane, deira kompetanse og kva høve dei har til å vareta sitt eige personvern. Ved bruk av dagens nettbankløysingar er det i første rekkje bankane sjølve som tek konsekvensane ved misbruk. Brukarane lir derfor i liten grad tap dersom dei ikkje sjølve har vist grov aktløyse. Ved etablering av ein felles portal, der mange personopplysningar blir gjorde tilgjengelege, må det på same vis avklarast kven som skal ta ansvaret ved misbruk og kven som skal bere kostnadene når noko går gale. Det kan vise seg vanskeleg å setje ein prislapp på den børa borgaren må bere dersom personopplysningar skulle komme på avvegar eller bli misbrukte.

Tryggleiksnivå og klargjering av ansvar

Å få til ei sikker identifisering av brukaren vil vere heilt avgjerande. Dersom det skal nyttast ein portal med sentral pålogging må tryggleiksnivået dimensjonast i forhold til det til mest sensitive materialet som blir tilbode til kvar tid, og det samla omfanget av personopplysningar som kan hentast ut via portalen.

Moderniseringsdepartementet har sett ned ei prosjektgruppe som skal komme fram til løysingar for sikker kommunikasjon mellom publikum og forvaltninga. Viktige aktørar i denne prosessen har vore dei store offentlege etatane som har utstrakt samhandling med publikum. Datatilsynet har berre vore observatør i arbeidet. Tilsynet konstaterer at dei offentlege etatane kommuniserer ulike behov med omsyn til kva som skal reknast som tilstrekkeleg sikker kommunikasjon. Det må likevel vere omsynet til brukarane som er avgjerande for kva løysing som blir vald. Datatilsynet meiner at det bør etablerast ei einskapleg løysing som kan gi tilfredsstillande kommunikasjon mellom alle partar og nivå. Dette også ut frå ei samfunnsøkonomisk vurdering.

Før løysinga blir sett i drift må det også vere avklart kven som skal vere behandlingsansvarlege etter personopplysningsloven for dei ulike elementar av datagrunnlaget som blir presentert i portalen, og kven som skal vere behandlingsansvarleg for den samla løysinga. Dei behandlingsansvarlege vil vere sjølvstendig ansvarlege for å forankre elementa i ein tryggleiksstrategi. Gjennomførte risi-

kovurderingar må også dokumentere ein samla forsvarleg tryggleik i alle ledd av løysinga.

Skoleporten og nasjonale prøver

Utdanningsdepartementet har, i samband med nasjonale prøver, etablert eit sentralt register som lagrar karakterar, namn og fødselsnummer for alle skoleelevar i Noreg. Datatilsynet blei utover hausten 2004 kontakta av mange lærarar som var urolige over denne sentrale registreringa og den profilbygginga som følgde med. I følgje nettstaden "skoleporten.no" skal profilen følgje eleven og brukast til å gi tilpassa opplæring.

Datatilsynet ser det som uheldig at forskriftsføresegna som pålegg den sentrale innrapporteringa ikkje var lagd fram for Datatilsynet til uttale. Tilsynet bad derfor Utdanningsdepartementet om å gjere greie for kva vurderingar som ligg til grunn for å knyte karakteropplysningane til namn og fødselsnummer. Over tid kan desse profilane bli svært omfattande, og innebere personvernrisiko for kvar enkelt elev. Ein kan heller ikkje vente at barn kan ta vare på rettane sine etter loven på same måte som vaksne.

Datatilsynet har i oppfølgjande møte med Utdanningsdepartementet uttrykt sin vedvarande skepsis til den løysinga som er vald. Utdanningsdepartementet vil som følgje av dette ta løysinga opp til ny vurdering, og var ved årsskiftet framleis i dialog med Datatilsynet om dette.

Ny lov om utdanningsstøtte

Datatilsynet stiller seg kritisk til føresegna om innhenting av personopplysningar det er gjort framlegg om i forslaget til ny Lov om utdanningsstøtte. I staden for å innhente opplysningar ved samtykke frå søkeren sjølv, er det gjort framlegg om at Statens lånekasse med heimel i lov skal kunne hente inn ei rekkje opplysningar frå andre.

Tilsynet har forståing for at ein søker å etablere meir effektive og kostnadssparande tiltak for administrasjon av utdanningsstøtta. På den andre sida er det vesentleg at lånsøklarar i størst mogleg grad sjølve kjem med opplysningar som er relevante. Ein administrasjon av rettar som i stor grad baserer seg på innhenting av opplysningar frå andre, vil kunne føre til at den registrerte mistar oversikta over kva opplysningar som er lagde til grunn for behandlinga. Innhenting av opplysningar frå andre krev i tillegg at dei er pålitelege og av høg kvalitet. Tilsynet er også kritisk til forslaget om å gi ein vid lovheimel til å kunne innhente opplysningar også om tredjepersonar.

Samordning av arbeidsmarknadsetaten, trygdeetaten og sosialtenesta

Rattsø-utvalet la sommaren 2004 fram forslaget sitt om ei samordning av arbeidsmarknadsetaten, trygdeetaten og sosialtenesta. Tilrådinga frå utvalet inneber ei løysing der det blir organisert ein ny, statleg etat for arbeid og inntekt, og ein ny statleg etat for pensjonar samt stønader og refusjonar i samband med nedsett helse, pluss ei rekkje andre ytingar knytte til barn. Utvalet foreslår at kommunen framleis skal ha ansvaret for å yte sosialhjelp.

Delar av forslaget vil innebere store personvernmessige konsekvensar for kvar enkelt. Ei sentralisert og stor samling av til dels svært sensitive personopplysningar gir eit auka potensiale for misbruk. Svært mykje kunnskap om kvart enkelt menneske vil kunne bli tilgjengeleg for førstelinjetenesta. Forslaget kan også føre til eit stort press mot teieplikta mellom fagområda og internt i etatane.

Utvalet ønskjer at ein skal ha ein stor grad av organisatorisk fleksibilitet. Det tilrådde forslaget legg derfor opp til at førstelinjetenesta skal kunne arbeide på tvers av formelle etatsgrenser. Dei skal kunne handtere opplysningar frå menneske som søker hjelp både når det gjeld pensjonsspørsmål, refusjon av utgifter for si nedsette helse, og spørsmål om manglande inntekt ved langvarig sjukdom.

Datatilsynet meiner at forslaget om ei slik førstelinjeteneste ikkje er tilrådeleg, spesielt om det blir lagt opp til at kvar enkelt saksbehandlar skal få tilgang til svært omfattande, og kanskje også sensitiv informasjon om innbyggjarane i kommunen.

Føresegnene om teieplikt bør etter Datatilsynet si oppfatning ikkje strekkjast lenger enn nødvendig. Kvar enkelt saksbehandlar bør ikkje få tilgang til fleire opplysningar enn vedkommande faktisk treng for å løyse si oppgåve. Sjølv om kvar enkelt saksbehandlar har teieplikt også overfor saksbehandlarar i same etat, har organiseringa av arbeidet mykje å seie for om personopplysningar blir spreidde eller ikkje. Mindre etatar med noko meir spesialiserte oppgåver vil medføre mindre spreiding.

Datatilsynet tilrår at ein bruker dei høve som ny IT-teknologi gir til å etablere interne tilgangsgrensingar. Slike avgrensingar i systema kan sikre at saksbehandlarane berre får tilgang til dei opplysningane dei treng for å løyse sine konkrete oppgåver. Ei utholing av teieplikta vil kunne gi etatane låg tillit i befolkninga.

Datatilsynet er elles ikkje einig i Rattsø-utvalets framstilling av at personvern og rettstryggleik ”setter unødige hindringer for et samarbeid mellom offentlige etater til brukers beste”. Regelverket på personvernområdet er nært knytt opp til internasjonale konvensjonar som Noreg er forplikta til å følge.

Supplerande stønad for personar med kort butid i Noreg

I utkast til Lov om supplerande stønad for personar med kort butid i Noreg er det gjort framlegg om at trygdekontora skal få svært vide høve til å kontrollere rettshavarane etter loven. I realiteten blir det mogleg for Trygdeetaten å hente inn alle typar opplysningar frå alle offentlege instansar. Lovforslaget vil innebere at teieplikta i ei rekkje andre særlovar blir oppheva. Datatilsynet er skeptisk til ei slik oppheving utan at det er vurdert kva teieplikta og diskresjonsomsyn representerer av verdi i kvar enkelt særlov. Trygdeetaten vil, dersom lovforslaget blir gjennomført, også få tilført mykje overskottsinformasjon.

8.3 Helse og forskning

Kan vi som pasientar lite på at opplysningar vi gir legen blir behandla fortruleg? Gjennom store, sentrale register blir det no ført oversikt over nær sagt all kontakt med helsevesenet. Opplysningane i journalane kan også i mange tilfelle lesast av andre helsearbeidarar og kontorphersonell, utan særleg etterkontroll av at det var gode grunnar for oppslaget.

Datatilsynet merker også ein tendens til at ein for forskning og administrasjon ønskjer å ha stadig større og meir overgripande datasamlingar med svært mange opplysningar om kvar enkelt, gjerne på identitet, slik at alle kan følgjast gjennom fleire år.

Dårlegare personvern med nytt Norsk pasientregister

Sosial- og helsedirektoratet foreslo i 2004 å gjere Norsk pasientregister om til eit register knytt til identitet. Dette er Datatilsynet sterkt i mot. I høringsfråseigna peikte Datatilsynet på at eit personentydig Norsk pasientregister, med sentralisert kartlegging av kvar enkelt norsk borgars helsetilstand og bruk av sjukehus frå fødsel til død, vil ha negative personvernkonsekvensar for nær sagt alle i Noreg.

Den typen Norsk pasientregister det er gjort framlegg om, er eit nøkkelregister. Ved bruk av nokre få opplysningar herfrå kan ein identifisere kvar enkelt av oss i dei fleste andre helseregister –

uavhengig av om registra i utgangspunktet er avidentifiserte eller pseudonyme. Når ein ser dei eksisterande helseregistra i samanheng med det pasientregisteret det er gjort framlegg om, blir den samla kartlegginga bortimot altomfattande.

Datatilsynet ser Norsk pasientregister som så trugande for personvernet at tilsynet heller ikkje tilrår ei løysing med eit pseudonymt register.

Allereie i dag eksisterer eit Norsk pasientregister av mindre omfang. Registeret har konsesjon frå Datatilsynet med vilkår om at namn og personnummer skal slettast. Helse- og omsorgsdepartementet ønskjer å lagre fleire opplysningar i registeret, og søkte i 2004 om konsesjon for ei utviding. Datatilsynet meiner det ikkje er heldig å fremje konsesjonssøknad om utviding samtidig som framlegg om korleis registeret skal utformast i framtida er til offentleg høring.

Lovfesting av Forsvarets helseregister

Datatilsynet var i si høringsfråsegn svært kritisk til at Forsvarets helseregister skulle lovfestast slik forslag til lov om personell i Forsvaret la til grunn. Forslaget var etter Datatilsynets meining ikkje godt nok grunngitt. Formålet med registeret blei utvida i forhold til tidlegare, og føreseigna som blei foreslått såg nærmast ut til å vere ei blankofullmakt til å forskriftsfeste det registeret Forsvaret til kvar tid måtte ønskje seg. Ein vurderte ikkje personvernulempene nokon stad i utkastet, trass i at det blei hevda at ein slik gjennomgang er viktig.

Etter høringsrunden kom ein fram til at det er formålstenleg å heimle Forsvarets helseregister i helseregisterloven. Registeret blir dermed underlagt dei same reglane som andre sentrale personidentifiserbare helseregister, og også underlagde dei same rettstryggleiks- og personvernskrankane. Det er vedteke av Stortinget at Forsvarets helseregister skal heimlast i helseregisterloven § 8. Lovendringa trådde i kraft frå 1. januar 2005.

Landsomfattande helseundersøkingar og kvalitetsregister

Datatilsynet gav i slutten av 2003 og byrjinga av 2004 konsesjonar til ei rekkje av dei store helseundersøkingane. Blant anna Helseundersøkinga i Nord-Trøndelag (HUNT), Tromsøundersøkinga og Osloundersøkinga blei tildelt konsesjonar for mange av sine prosjekt. Desse konsesjonane er i stor grad bygde over same leist. Datatilsynet aksepterte at samtykket som opphavleg er innhenta blei ført vidare, trass i at det ikkje er tilfredsstillande i forhold til krava i dagens lovverk. Det blei likevel stilt vilkår for i kva samanheng

data kan nyttast, og når ein må innhente nytt samtykke og gi ny informasjon til dei registrerte. Konsesjonen dekkjer ikkje all bruk av data. I enkelte tilfelle krev bruk av desse data at det også blir søkt om ny konsesjon frå Datatilsynet. Dette er spesielt aktuelt dersom data skal utleverast til bruk i eit prosjekt i regi av andre enn konsesjonsinnehavaren.

Kreftregisteret fekk fleire nye konsesjonar. Nokre av prosjekta til Kreftregisteret har etter Datatilsynet si oppfatning ikkje kunna dokumentere at dei tilfredsstiller grunnleggjande krav i helseregisterloven og personopplysningsloven. I fire av prosjekta har Datatilsynet gitt konsesjon med vilkår om at det må hentast nytt samtykke for vidare behandling av dei registrerte data. Desse fire vedtaka er påklaga av Kreftregisteret.

I 2004 blei det også gitt nye konsesjonar til blant anna Nasjonalt leddproteseregister, Nasjonalt MS-register, Nasjonalt korsbandregister og Nasjonalt hjertestansregister.

Stor saksmengd gir betre avklart praksis

Datatilsynet har behandla ei stor mengd saker på helse- og forskingsområdet etter at helseregisterloven og personopplysningsloven trådde i kraft i høvesvis 2002 og 2001. Saksmengda har gitt eit godt grunnlag for etablering av ein meir einsarta praksis.

Fleire avgjerder i Personvernemnda det siste året har klargjort tilsynet sin praksis vidare og trekt opp viktige prinsipp for bruk av lovverket, spesielt forholdet til kva behandlingsgrunnlag ulike forskingsprosjekt kan finne heimel i.

Overordna prinsipp

Samtykke er utgangspunktet, men det kan leggjast vekt på følgjande argument for å avvike frå utgangspunktet:

- innhenting av samtykke vil føre til låg deltaking, og dette reduserer verdien av undersøkinga
- informasjon og høve for den registrerte til å reservere seg reduserer ulempene
- om undersøkinga ikkje medfører innhenting av nye opplysningar, kan ein rekne ulempa for å vere mindre for dei registrerte
- den interesse ein går ut frå at dei registrerte har for at forskingsprosjektet blir gjennomført

Tilføring av nye opplysningar i sentrale forskriftsbaserte helseregister må ha heimel i forskrift. Datatilsynet har ikkje myndigheit til å gi konsesjon som utvidar forskriftsføresegnar.

Nedslåande funn innan helseforskning

Er behandlinga helseopplysningane får innan forskinga forsvarleg? Etter å ha ført tilsyn med 50 forskingsprosjekt kunne ikkje Datatilsynet sjå mange lyspunkt.

Datatilsynet sette ned ei prosjektgruppe som gjennomførte tilsyn med 50 forskingsprosjekt våren 2004. Det blei ført tilsyn med 26 verksemdar innanfor ulike helseføretak, lærestader, forskingsinstitusjonar og legemiddelprodusentar. Prosjektet avdekte fleire forhold som Datatilsynet ser alvorleg på. Tilsynet fann brot på konsesjonsvilkår, ulovleg oppbevaring av sensitive personopplysningar, fråvær av internkontroll og manglande oversikt over ansvarsplassering. Det er utarbeidd ein eigen rapport som gjer greie for funn og tendensar i samband med prosjektet. Rapporten er tilgjengeleg på Datatilsynets heimeside.

Brot på konsesjonsvilkår

Datatilsynet har valt å stille konsesjonsvilkår knytte til gjennomføringa av prosjekt for å få dei innanfor loven sine rammer, snarare enn å avslå konsesjonssøknaden fullstendig. Konsesjonsvilkåra er dermed eit viktig verktøy som også kjem forskarar til gode.

Av dei 17 prosjekta som hadde konsesjon, hadde 11 ikkje følgt konsesjonsvilkåra, utan at forskarane kunne gi noka god forklaring på dette. At konsesjonsvilkåra ser ut til å bli etterlevd i berre seks av 17 prosjekt er eit nedslåande resultat.

Ulovleg oppbevaring av sensitive personopplysningar

I 15 av 33 kontrollerte prosjekt fann Datatilsynet at ein ikkje hadde gyldig heimelsgrunnlag i helseregisterloven og personopplysningsloven. For fleire av prosjekta betyr det at forskaren einsidig har endra premissane for prosjektet utan at deltakaren er informert. Dette inneber at samtykket ikkje lenger er gyldig.

Låg tryggleik og brot på sletteplikt

Også når det gjeld den praktiske sikringa av opplysningane var resultatet nedslåande. Av 31 relevante prosjekt reknar Datatilsynet berre 17 for å vere utførte praktisk forsvarleg. Åtte prosjekt var utførte delvis forsvarleg, mens heile seks ikkje var forsvarleg utførte.

Tilsyna viste også jamt over at sletteplikta var dårleg ivareteken. Med ein gjennomgåande mangel på internkontroll hos dei behandlingsansvarlege er det grunn til å tru at det finst store mørketal på området.

Brot på konsesjonsplikt

I tilsynsprosjektet er det i liten grad gjort forsøk på å avdekkje om det finst forskingsprosjekt som ikkje er lagde fram for Datatilsynet eller personvernombodet. Det blei likevel avdekt to konsesjonspliktige forskingsprosjekt som det ikkje er søkt om konsesjon for etter helseregisterloven og personopplysningsloven.

Mangel på internkontroll

Verksemder som behandlar personopplysningar skal ha eit system for internkontroll for å sikre at pliktene etter personopplysningsloven og helseregisterloven blir overhaldne. Rutinane skal sikre at rettane til dei registrerte som bl.a. retten til innsyn, informasjon, retting og sletting blir ivaretekne.

Funn frå tilsyna viste at det nærmast var eit totalt fråvær av internkontroll. Berre éi av 29 verksemder kunne dokumentere eit tilnærma fullstendig implementert internkontrollsystem.

Datatilsynet følgde opp med fem tilsyn med utvalde forskingsprosjekt hausten 2004, og har valt ut forskning som eit område for tilsyn også i 2005.

Høring om forskriftsending for forskning

Datatilsynet sende hausten 2004 ut eit høringsforslag om å utvide unntaket frå konsesjonsplikt for forskning (personopplysningsforskrifta § 7-27). Som hovudregel blir det gjort framlegg om at ein held på systemet med meldeplikt. Det skal etter forslaget i større mon leggjast vekt på etterkontroll i form av tilsyn. Høringsnotatet inneheld to alternative forslag til forskriftstekst. Innholdsmessig er forslaga meint å vere like. Det første alternativet opnar for ein relativt stor grad av skjønnsmessig vurdering frå forskaren si side, mens det andre i større grad er konkretiserande.

Bakgrunnen for forslaget til endring er at Datatilsynet har sett at førehandskontrollen ikkje har hatt den ønskete verknaden i alle samanhengar. Tilsynet meiner at større fokus på etterkontroll vil kunne ha eit større potensial for personvernet. Høringsfristen var 31. desember 2004.

Forenkling av melde- og søknadsprosedyrar ved medisinsk forskning

Datatilsynet har sete i ei arbeidsgruppe, oppnemnd av Helsedepartementet i januar 2004, som vurderte forenkling og effektivisering av melde- og søknadsprosedyrar ved medisinsk forskning. I arbeidsgruppa var det deltakarar frå Sosial- og helsedirektoratet, Helsedepartementet, Den nasjonale forskningsetiske komité for medisin og Datatil-

synet. Arbeidsgruppa gjekk gjennom eksisterande skjema og søknadsprosedyrar og foreslo alternative måtar å forenkle og effektivisere utfylling og behandling av søknader og meldingar. Formålet var å vurdere i kor stor grad det var mogleg å gjere forenklingar innanfor dagens regel- og rammeverk mens ein venta på innstillinga frå Nylennautvalet.

Arbeidet resulterte i at det er blitt etablert ein oversiktleg forskingsportal på dei forskningsetiske komiteanes heimeside (sjå www.etikkom.no/REK/forskerportal)

Portalen skal hjelpe forskarar til å få ei rask oversikt over kva melde- og søknadsprosedyrar dei må gjennomgå for å starte eit forskingsprosjekt. Det er dessutan utarbeidd ein felles mal med moment kvar enkelt forskar må gjennom ved utforminga av eit informasjonsskriv.

8.4 Internett

Publisering av personopplysningar på Internett blir som hovudregel regulert av personopplysningsloven. Kva for avgrensingar gjeld når enkelt-personar blir omtalte på Internett?

Ytringsfridom og personvern på Internett

Forholdet mellom ytringsfridom og personvern på Internett blei sett på spissen i 2004. Ein nettstad hadde lagt ut informasjon om ei rekkje enkelt-personar som hadde arbeidd med barnevernsaker. Nettstaden omtalte personane i til dels sterkt kritiske ordelag, og kom med påstandar om rettsstridig behandling. Datatilsynet fekk ei rekkje klagar og spørsmål frå partane det gjeld, publikum og presse om saka.

Datatilsynet vurderte om bruken av personopplysningar på Internettsida blei regulert av personopplysningsloven, eller om sida kom inn under unntaket i loven for journalistiske, medrekna opinionsdannande formål. Datatilsynet kom fram til at klagane måtte avvisast. Grunngevinga var at endå om behandlinga av personopplysningar på Internettsida isolert sett krenkte personvernet, kunne det totalt sett truleg seiast å utgjere samfunnskritikk. Det var uklart om ytringane skulle reknast som opinionsdannande eller ikkje. Avvisningsvedtaket er klaga til Personvernemnda.

Vedtaka om å avvise klagane i denne saka er underbygde med at det er krav om ein klar heimel i lov for inngrep i grunnleggjande rettar (her i ytringsfridomen). Dette er i tråd med det såkalla *legalitetsprinsippet*. Personopplysningsloven gir, etter Datatilsynets oppfatning, ikkje tilstrekkeleg heimel for inngrep. Saka reiser prinsipielle spørsmål om kor langt Datatilsynet, i personvernet sitt

namn, kan gå i å drive sensur av ytringar på Internett. Dette spørsmålet må avklarast når personopplysningsloven skal etterkontrollerast i 2005.

I 2004 blei også aksjonærlistene til selskapet The five percent community (T5PC) publiserte av media. Fleire journalistar og enkeltpersonar tok kontakt og lurte på om dette var i strid med personopplysningsloven. Datatilsynet meinte at lista openbert var publisert til journalistiske formål, og at ho dermed ikkje var omfatta av personopplysningsloven.

Barn og unge på Internett

Datatilsynet tok i 2004 stilling til om foreldre til barn under 15 år kan krevje sletting av personopplysningar om barnet på Internett. Saka gjaldt nettstaden "deiligst.no". Barnet sine føresette hadde i denne saka kontakta innehavaren av sida og kravd at bilete og andre personopplysningar blei sletta. Innehavaren av "deiligst.no" nekta å slette opplysningane utan at den som kravde sletting først legitimerte seg. Datatilsynet konkluderte med at foreldra til barnet har samtykkekompetanse i slike tilfelle, og at retten til sletting kan utøvast utan å måtte involvere barnet. Nettstaden blei pålagd å slette opplysningane og bilda.

Datatilsynet vil følgje opp Internettsider av liknande karakter i 2005.

Publisering av festbilete på Internett

Stadig fleire utestader legg ut bilete av gjester på sine Internettsider. Bilda blir publiserte som eit ledd i marknadsføringa, og ofte utan samtykke frå gjestene. Datatilsynet har gjort fleire av utestadene merksame på at slik publisering som hovudregel krev samtykke. Dette er eit krav både i personopplysningsloven og i åndsverkslovens § 45, bokstav c. Berre informasjon om at bilete blir tekne og publiserte er ikkje nok til å oppfylle lovkravet om samtykke.

Datatilsynet gjennomførte i desember 2004 ei kartlegging av kor mange utestader som publiserer bilete av gjestene. Over 90 Internettsider administrerte av ulike utestader blei undersøkte. Omlag 20 av desse publiserte personidentifiserande bilete. Tilsynet vil følgje opp dei alvorlegaste sakene, og sikre at publiseringa skjer i tråd med regelverket.

Publisering av saksdokument på Internett

Stadig fleire forvaltningsorgan publiserer offentlege saksdokument i fulltekst på Internett på eige initiativ. Publiseringa blir grunnlagt med omsynet

til betre service og innsyn, både for pressa og allmenta elles.

I ei lovfortolking fastslo Justisdepartementets lovavdeling sommaren 2004 at forvaltninga må ta utgangspunkt i krava i personopplysningsloven når saksdokument blir publiserte på Internett etter eige initiativ. Dette inneber at forvaltninga må ha heimel for publiseringa, primært samtykke frå den omtalte, når dokumenta inneheld fleire personopplysningar enn personnamn og kva sakstype det er snakk om. Om dokumentet inneheld andre personopplysningar, for eksempel fødselsnummer, personleg økonomisk situasjon, utdanning og arbeidserfaring, må desse opplysningane sladdast, med mindre den det gjeld samtykkjer i at opplysningane blir publiserte.

Datatilsynet har gitt varsel om pålegg til fleire kommunar som publiserte dokument i strid med regelverket. Tilsynet vil halde fram med å følgje utviklinga på dette området nøye.

8.5 Samferdselssektoren

I meldingsåret har det vore store og prinsipielle saker innan samferdselssektoren. Ei sak som har vore under behandling heile året, og som enno ikkje har komme til ei løysing, er Statens vegvesen sitt prøveprosjekt med heilautomatiske bomstasjonar i Tønsberg, Bergen (og, seinare viste det seg også, Gjesdal i Rogaland). Det har også blitt gjort ei kartlegging av samferdselssektoren, medrekna telekommunikasjon. Formålet var å skaffe ei oversikt over registreringsomfanget av personopplysningar og i kva grad kvar enkelt har rett og reelt høve til å kunne ferdast utan å leggje att spor. Som eit ledd i denne kartlegginga blei det gjennomført fleire tilsyn.

Rett til sporfri ferdsel?

Personvern er vanskeleg å definere. Kva som blir oppfatta som krenkjande for ein person kan opplevast heilt annleis for ein annan. Retten til sjølv å kunne rå over egne opplysningar er derfor eit av dei heilt sentrale personvernprinsippa. Men for at sjølvråderett skal ha eit verkeleg innhald må kvar enkelt stå overfor reelle val med omsyn til om ein skal la andre få tilgang til, og behandle personopplysningar om seg i ulike samanhengar.

Retten til anonym ferdsel er ikkje uttrykkeleg slått fast i norsk lovgiving. Ein slik rett kan likevel utleiast av dei grunnleggjande rettane i blant anna menneskerettskonvensjonens artikkel åtte og av EUs personverndirektiv. Her heiter det at enkeltpersonars grunnleggjande rettar og fridomar må respekterast, særleg retten til privatlivets fred. I

både personverndirektivet og i den norske personopplysningsloven er sjølvråderetten for kvar enkelt eit av grunnprinsippa – i første rekkje uttrykt ved at det blir gitt eit frivillig, informert og uttrykkeleg samtykke til behandling av personopplysningar.

Gjeld ikkje utan vilkår

Retten til anonym ferdsel gjeld sjølv sagt ikkje absolutt. Det finst både internasjonale og nasjonale reglar som avgrensar kor stort høve kvar enkelt har til å reise utan å måtte gi frå seg personopplysningar. Dette gjeld for eksempel identifikasjonskontroll og registrering av personar som ønskjer tilgjenge til eit geografisk område, eller å reise med bestemte transportmiddel. Det finst derfor føreseigner om at alle passasjerar på skip som reiser over 20 nautiske mil skal registrerast med namn, alder og kjønn. Opplysningane skal vere tilgjengelege for redningstenesta og andre relevante styresmakter i samband med redningsarbeid.

Må leggje til rette for sporfrie løysingar

Den grunnleggjande retten det er for kvar enkelt å kunne ferdast fritt i det norske samfunnet utan å leggje igjen elektroniske spor, føreset at aktørane innan samferdselssektoren må etablere sporfrie løysingar, med mindre sterke samfunnsmessige interesser skulle tilseie noko anna. Alle som planlegg løysingar som føreset registrering av opplysningar om rørsle til enkeltindivid må derfor grunngi og dokumentere kva det er som gjer det nødvendig å gjere unntak frå den grunnleggjande retten til å kunne ferdast sporfritt.

Personopplysningar innan samferdsel - ei kartlegging

Gjennom Nasjonal transportplan og Samferdselsdepartementets IKT-strategi blir det teke til orde for auka bruk og samordning av informasjons- og kommunikasjonsteknologi innan samferdselssektoren. Det er ei uttalt målsetjing at større bruk av IKT skal medverke til betre tryggleik, effektivitet og nytte for dei reisande. Denne utviklinga kan likevel komme i konflikt med personvernomsyn, ettersom auka bruk av IKT ofte også inneber auka registrering av personopplysningar.

Datatilsynet har, blant anna gjennom forsøka med heilautomatiske bomstasjonar, erfart at det berre i liten grad blir lagt vekt på personvern når det blir etablert nye løysingar innan samferdselssektoren. Med denne bakgrunnen fann Datatilsynet det derfor nødvendig å gjennomføre ei meir systematisk kartlegging av registreringsomfanget innan samferdselssektoren. Kartlegginga tok i før-

ste rekkje for seg reiser ved bruk av fly og båt, annan kollektivferdsel og vegtrafikk. I ein meir avgrensa grad blei det også gjort kartlegging når det gjeld telesektoren.

Fly og båt

For reisande som nyttar fly og båt, blir det registrert opplysningar som kven som reiser, kjønn, passasjerkategori, eller aldersgruppe. Dersom kunden ønskjer det blir det også registrert eventuelle preferansar for reisa. Alle desse registreringane, med unntak av preferansane, er lovpålagde og har som formål å ta vare på tryggleiken til dei reisande, til bruk ved ulykker eller andre hendingar. Omfanget av registrerte opplysningar er lite og dei blir sletta kort tid etter at reisa er gjennomført.

Det blei, som ledd i kartlegginga, gjennomført tilsyn på staden hos eitt flyselskap, to reisebyrå og to ferjeselskap. Hovudinntrykket er at selskapa behandlar personopplysningar i samsvar med føresegnene i personopplysningsloven.

Elektronisk billettering for buss og bane

Kartlegginga viste at operatørane innan kollektivtrafikken er i ferd med å gå frå det tradisjonelle billetteringssystemet til elektronisk billettering. Det er ønske om å innføre compatible system, slik at kunden kan bruke same billett i eit større geografisk område, og på sikt i heile landet. Også i ein slik samanheng er det viktig at kvar enkelt, utan for store økonomiske eller praktiske kostnader, framleis skal kunne reise kollektivt utan å leggje att detaljerte opplysningar om seg og reisemønsteret sitt. Dei tankar og løysingar som til no er blitt presenterte for Datatilsynet ser ut til å ta vare på dette omsynet.

Strekningsvis automatisk trafikk kontroll

Vegstyresmaktene nyttar kjøretøyas registreringsnummer til kontroll av trafikk og trafikantar. Dette gjeld for eksempel ved passering av bomstasjonar, fartskontrollar og kontroll av kjøre- og kviletid.

Datatilsynet blei under kartleggingsarbeidet gjort kjent med eit prøveprosjekt som går ut på strekningsvis automatisk trafikk kontroll. Dette inneber at ein måler gjennomsnittsfarten mellom to kontrollpunkt. Ettersom denne typen fartskontroll reiser nokre heilt sentrale utfordringar i forhold til å vareta personvernet, følgjer Datatilsynet nøye med på prøveprosjektet. Dette skal etter planen testast ut våren 2005, i området rundt Lillehammer.

Heilautomatiske bomstasjonar

Datatilsynet blei på slutten av 2002 kontakta av Statens vegvesen i samband med eit prøveprosjekt for heilautomatiske bomstasjonar i Tønsberg og Bergen. Vegvesenet la innleiingsvis opp til alternative betalingsformer, anten abonnement basert på AutoPass-brikke, eller etterskottsfakturering basert på videoopptak av bilen sitt registreringsnummer. I tillegg blei det lagt opp til ei løysing der trafikanten kan betale kontant hos ein agent for bompengeselskapet (for eksempel bensinstasjonar) innan tre dagar etter passering. Dei registrerte passeringsopplysningane blir deretter sletta.

Løysingane inneber at alle passeringar av bomstasjonen blir registrerte (blant anna bilen sitt registreringsnummer, tid og stad). Datatilsynet melde derfor tilbake at det i tillegg må vere tilbod om eit alternativ som gjer at det, på same vis som med myntautomatar eller manuell betening, framleis er mogleg å passere bomstasjonane utan å leggje igjen personopplysningar. Datatilsynet føresette derfor at det, før prøveprosjektet blei sett i gang, måtte etablerast eit alternativ der det reelt sett ikkje blir lagt igjen passeringsopplysningar som kan knytast til trafikanten.

Framleis ikkje godt nok

For å tilfredsstille kravet om anonymitet etablerte Statens vegvesen ei løysing med ei AutoPass-brikke som fungerer som eit ihendehavarbevis. Trafikanten deponerer på ei brikke, og betaler den verdien brikka er ladd med. Ved seinare lading av brikka nyttar ein identifikasjonsnummeret for brikka som referanse for betalinga. I motsetning til abonnentsløysinga blir denne brikka ikkje knytt til eit bestemt kjøretøy hos bompengeselskapet. Registrerte passeringsopplysningar kan dermed ikkje sporast tilbake til bil og trafikant.

Då dei heilautomatiske bomstasjonane i Tønsberg og Bergen starta opp i februar 2004, var det likevel mykje som tydde på løysinga ikkje fungerte slik at dette kunne reknast som eit tilfredsstillande sporfritt alternativ. Det blei derfor gjennomført tilsyn på staden både i Tønsberg og Bergen.

Datatilsynet fann at den løysinga som var vald langt på veg sikra trafikantane sporfridom, reint teknisk sett. Likevel var løysinga langt frå tilfredsstillande. Alternativet var i stor grad underkommunisert og brikka vanskeleg å få tak i. I Tønsberg måtte besøkjande til og med passere bomstasjonen for å få tak i brikka på eit Securitas-kontor innanfor bomringen. Løysinga gav ikkje dei trafikantane som besøkjer området ein eller få gonger, reelt høve til å passere sporfritt. Det var også urimeleg

dyrt å skaffe seg brikka for dei som berre skal passere nokre få gonger, og det er ikkje tilbod om rabattar ved bruk av den anonyme brikka.

Vedtak om konsesjonsplikt

Endå om sensitive personopplysningar ikkje blir behandla i dei heilautomatiske bomstasjonane, fatta Datatilsynet hausten 2004 vedtak om at dei heilautomatiske bomstasjonane skal underleggjast konsesjonsplikt. Vilåret for å kunne gjere dette, er at behandlinga *openbert vil krenkje tungtvegande personverninteresser*. Etter Datatilsynets vurdering vil det vere ei openberr krenking av tungtvegande personverninteresser dersom kvart enkelt individ ikkje sjølv kan velje om ein vil leggje att spor om kvar ein ferdast til kva tidspunkt langs norske vegar. Med dei løysingar som til no har vore implementerte, får ikkje trafikantane tilbod om løysingar som inneber at dei har eit reelt val, når ein tek omsyn til informasjon, kor lett det er å få tak i dei, kostnader og funksjonell bruk.

Ved slutten av meldingsåret var Datatilsynet framleis i dialog med Statens vegvesen når det gjeld å finne fram til ei akseptabel løysing. Endå om ein blir einige om ei teknisk løysing som varetek trafikantane sin rett til å kunne ferdast sporfritt, vil Datatilsynet likevel innføre konsesjonsplikt for dei heilautomatiske bomstasjonane. Gjennom vilkår sett i konsesjon kan selskapa få felles reglar for blant anna utlevering av personopplysningar, praktisering av innsynsretten og sletting av passeringsopplysningane. Datatilsynet erfarte gjennom sitt kartleggingsarbeid at dette blir ulikt handtert i dei forskjellige bompengeselskapa. Det er uheldig, når ein tek omsyn til at trafikanten, som følgje av samordning selskapa imellom, kan nytte si autopassbrikke også i andre bompengeselskap enn sitt eige. Einsarta behandlingsrutinar vil gjere det lettare for publikum å vita kva dei har å halde seg til.

Datatilsynet føreset at det ikkje blir bygd ut nye heilautomatiske bomstasjonar før det ligg føre løysingar som gjer at trafikantane framleis kan ferdast langs norske vegar utan å leggje att detaljerte og personidentifiserbare passeringsopplysningar.

Mobiltelefon og posisjonering

Noreg er på verdstoppen når det gjeld utbreiing av mobiltelefonar og bruk av tenester som høyrer til. Denne teknologien føreset ei automatisk utveksling av signal, som kan gjere det mogleg å kartlegge kvar innehavaren av telefonen faktisk oppheld seg. Då melder spørsmålet seg straks: Kor fritt kan ein bruke slike lokaliseringsdata?

Eit teknisk utgangspunkt

Ein mobiltelefon treng trådløs kontakt med basestasjonar plasserte på bakken for å kunne brukast. Basestasjonane kan på førespurnad kartlegge kvar telefonsettet fysisk er å finne. Slike data kallar ein lokaliseringsdata. Kor nøyaktig posisjonen er avheng blant anna av kor tett basestasjonane ligg. I bysenter, der basestasjonane normalt ligg tett, kan lokaliseringa, slik ho blir gjort i dag, gjerast så nøyaktig som inntil hundre meter. Etter som nettverket blir bygd ut og modernisert, kan staden bli fastsett stadig meir presist.

Den grunnleggjande funksjonen for desse lokaliseringsdata er å gi informasjon om kvar beraren av mobilen oppheld seg. Ettersom lokaliseringsdataa kan knytast til enkeltpersonar (beraren av mobilen), er dei også å rekne som personopplysningar, og bruken av slike data er underlagd personvernlovgivinga. Dette gir føringar for kor lenge teleoperatørane kan lagre lokaliseringsdataa og korleis dei eventuelt kan utleverast til andre, for eksempel andre selskap som tilbyr tenester via mobiltelefon (innhaldsleverandørar).

Stor kommersiell interesse

Datatilsynet ser ei vesentleg auka interesse for bruk av lokaliseringsdata til kommersielle formål. Fleire innhaldsleverandørar har forlengst lansert tenester for sporing og gjenfinning av bilar, båtar og andre verdigjenstandar via GSM. Det er for eksempel lansert tenester som varslar mobilbrukaren om denne nærmar seg fotoboksar langs vegen, eller når ein er i nærleiken av ei eller anna nærmare spesifisert teneste, for eksempel eit underhaldningstilbod.

Abbonnentens eigen, frivillige bruk

Når det gjeld kommersielle tenester som mobiltelefonberaren sjølv nyttar seg av og har god informasjon om, vil personverntrusselen vere relativt liten. Dette føreset likevel at ein med vitande og vilje nyttar tenesta. Eit eksempel på dette er den såkalla "buddy-tenesta", levert av NetCom. Ved å sende ein etterspørsel, kan ein få ei melding tilbake om kvar den etterspurde mobiltelefonberaren fysisk oppheld seg. Føresetnaden er likevel at begge har meldt seg på tenesta, og i den samanheng har samtykt til utlevering av lokaliseringsdataa. Dersom den etterspurde har meldt seg ut av tenesta, vil posisjonen ikkje lenger kunne utleverast til den som spør. Datatilsynet føreset ved slike tenester at det med jamne mellomrom blir sendt varsel til den som blir lokalisert.

Lokalisere for å kontrollere

Det er likevel også fleire døme på at det er ønske om å ta i bruk lokaliseringsdata i heilt andre samanhengar. Datatilsynet gav i ei konkret sak uttrykk for at eit forsikringsselskap ikkje kan basere seg på samtykke frå forsikringstakarar til innhenting av lokaliseringsdata for å avdekkje mogleg forsikringsbedrageri. Tilsynet grunngav dette med at eit slikt samtykke i realiteten ikkje vil vere særleg frivillig. Det at forsikringstakaren nekter å gi samtykke til utlevering vil lett få ein til å tenkje at vedkommande har noko å skjule. Dessutan ville forsikringsselskapet få ei mengd overskottsinformasjon som det ikkje har noko med. Forsikringsselskapa bør i staden overlate til politiet å innhente denne typen materiale.

Det er også lansert tenester som er skreddarsydd for at foreldre skal kunne lokalisere barna sine. Ein kan då definere ei sone som barnet er forventet å halde seg innanfor. Dersom signala frå mobilen indikerer at barnet av ein eller annan grunn har gått utanfor den tilletne sona, går eit sms-varsel til foreldra. Ein har også tenester der ein kan følgje med på Internett kvar mobileininga er til kvar tid, vist som markørar på detaljerte kart. Den same typen teneste kan sjølvstendig nyttast også overfor andre familiemedlemmer. Ikkje minst opnar også lokaliseringsteknologien for at arbeidsgivarar kan få til ei mest mogleg effektiv drift og logistikk ('flåtestyring'). Men posisjoneringsteknologien kan også takast i bruk for å kontrollere at medarbeidarane heile tida er på dei stader der arbeidsgivaren meiner dei skal vere.

Kvar skal grensene setjast?

Dei nye lokaliseringstenestene reiser altså ei rekkje utfordringar som vedrører personvernet. Det går sjølvstendig ei grense for kor langt foreldre kan gå for å spore barna sine, eller for arbeidsgivarar å spore sine tilsette. Men kvar skal streken setjast? I tida som kjem vil det bli nødvendig å gjere ei rekkje slike grenseoppgangar, basert på heilt konkrete tilfelle. Her vil ikkje berre Datatilsynet måtte engasjere seg, men også arbeidstakarorganisasjonar, arbeidstilsyn, barneombod og så vidare.

Utlevering og samtykke

Endå om begge dei to store teleoperatørane i den norske marknaden (Telenor og NetCom) naturleg nok sjølv er innhaldsleverandørar for mange mobiltelefontenester, er det også ei rekkje andre selskap som tilbyr ulike innhaldstenester basert på mobiltelefon. Når det gjeld tenester som føreset bruk av

lokaliseringsdata, baserer både Telenor og NetCom seg på at samtykke til utlevering og bruk av desse dataa blir innhenta via innhaldsleverandørane. Det blir avtalefest at det er innhaldsleverandørane som står ansvarleg for at gyldig samtykke er innhenta frå kunden før lokaliseringsdata blir henta ut frå teleoperatøren. Hos Telenor kan mobilabonntenen få sperra all utlevering av lokaliseringsdata, også endå om ein tidlegare har samtykt til slik utlevering via ein eller fleire innhaldsleverandørar. Hos NetCom er ikkje dette mogleg for abonntenen.

Eit oversiktleg og enkelt system er ein nødvendig føresetnad for at abonntenen skal kunne ha kontroll med opplysningar om seg sjølv, og kvar dei tek vegen. Datatilsynet har derfor pålagt begge teleoperatørane å etablere løysingar som gjer det mogleg for mobiltelefonabonntane både å starte og stoppe høvet til lokalisering direkte hos teleoperatørane. Mobilabonntenen må sjølv aktivere lokaliseringstenesta før ho kan takast i bruk.

Datatilsynet har også gjennomført tilsyn overfor to innhaldsleverandørar som hentar lokaliseringsdata frå mobiloperatørane. Dei nytta seg av forskjellige framgangsmåtar for innhenting av samtykke frå abonntane, avhengig av kva slags tenester dei tilbyr. Datatilsynet ventar med å følgje opp innhaldsleverandørane til etter at forholdet til teleoperatørane er avklart.

Kontantkort og trafikkdata

Hos mobiltelefonoperatørane blei det ved gjennomgang av sletterutinane avdekt at tilsynsobjekta oppbevarer trafikkdata knytte til kontantkortkundane sine i tre til fem månader. Kontantkort fungerer slik at sluttbrukaren fyller opp ein "konto" knytt til telefonnummeret med ein sum pengar. Kostnadene blir jamleg trekte frå kontoen etter kvart som kontantkortet blir brukt. Teleoperatørane kan derfor ikkje vise til faktureringsomsyn som grunngeving for at dei lagrar trafikkdata like lenge for kontantkundane som for dei andre abonntane. På spørsmål frå Datatilsynet hevda likevel teleoperatørane at andre omsyn låg bak den lange lagringstida, blant anna tekniske forhold og forbrukaromsyn. Tilsynet sit likevel att med eit inntrykk av at også trafikkdata for kontantkortkundane blir lagra fordi dette er det enklaste for teleoperatørane, reint teknisk og administrativt. Det er lettare å hanskast med ein felles lagringsrutine, anten ein fakturerer for tenesta eller ikkje. Datatilsynet stiller seg derfor tvilande til om teleoperatørane har eit tilstrekkeleg sakleg grunnlag for å lagre trafikkdata frå kontantkort i den grad dei gjer i dag, og vil følgje opp saka.

8.6 Kameraovervaking

Trenden frå tidlegare års auke i bruk av kameraovervaking er blitt endå sterkare i 2004. At kvaliteten på opptaksutstyret er blitt betre, at det er lettare å få tak i, at prisen er lågare og funksjonaliteten breiare, gjer at kameraovervaking av mange blir sett på som eit eigna verkemiddel for å forebygge og oppklare hærverk, vald og tjuveri.

Dette gjeld både for tradisjonelle enkeltstående kamera, men også som ledd i meir omfattande byggsikring der bruk av kamera utgjer ein integrert del av eit større overvakingssystem. Det er også stadig meir vanleg at drift av overvakingssystemet blir sett bort til eigne vaktelskap. Dette kan både gjerast slik at vaktelskapet får online-tilgang til bilete eller slik at dei kan gå inn og sjå på eit opptak. I tilfelle der vaktelskapa har ein større kundemasse, vil dette i praksis kunne innebere at desse får større høve til å overvake enn sjølv politiet har høve til.

Det er også ein klar tendens til at kameraovervaking blir teke i bruk på område der dette til no har vore avgrensa. Eksempelvis er det som klar hovudregel berre offentlege styresmakter/politiet som har lov til å overvake offentlege område. Det er likevel stadig oftare aktørar som ønskjer å overvake nettopp desse områda.

Sentrumsgatene i Stavanger

Ei samanslutning av butikkeigarar i Stavanger sette i verk omfattande kameraovervaking i sentrumsområdet. Kameraa fanga opp eigne butikkfasadar, men også offentlege område som veg og fortau utanfor butikkane. Området var merka, men ikkje i samsvar med reglane i personopplysningsloven. Det var dermed vanskeleg å avdekkje kven som var ansvarleg for overvakinga. Datatilsynet gav pålegg om at den delen av overvakinga som går utover ein uvesentleg del av gata/fortauet måtte opphøre. Vidare blei det stilt krav til tidsrommet for overvakinga og til merkinga av området.

NSB og Oslo Sporveier

Eit anna eksempel er overvaking i offentlege transportmiddel. Datatilsynet gjennomførte eit tilsyn hos NSB av eit prøveprosjekt med kameraovervaking på to lokale togsett. I tillegg blei det føreteke eit tilsyn hos Oslo Sporveier som nyttar kameraovervaking på Sporveisbussene. Verken trikkar eller T-banar har kameraovervaking ombord.

Formålet med overvakinga er å oppnå ein preventiv effekt og å oppklare hærverk. Sentralt står også tryggleik overfor tilsette og passasjerar i samband med for eksempel valdsepisodar eller ran. To

viktige og tungvegande omsyn må her vurderast opp mot kvarandre: På den eine sida står omsynet til ivaretaking av dei tilsettes liv og helse i tillegg til passasjeranes behov for tryggleik. På den andre sida står behovet for ikkje å vere under kontinuerleg overvaking.

På denne bakgrunnen har Datatilsynet varsla både NSB og Sporveiene om at det ikkje er akseptabelt å overvake passasjerområdet, dvs kupeane og busseta. Saka er ikkje endeleg avslutta og Datatilsynet går ut frå at saka vil ende som klagesak for Personvernemnda.

Ny teknologi

Saman med den sterke veksten i utbreiinga, er det auka funksjonalitet ved ny teknologi som representerer dei største truslane og utfordringane for personvernet. Digitaliseringa av kvardagen gjeld også innan kameraovervaking. Digitale overvakingssystem blir selde over disk til ein låg pris, og praktisk talt kven som helst kan setje opp eit overvakingssystem knytt til ein PC, og dermed ofte også Internett. Datatilsynet gav i 2004 blant anna ein arbeidsgivar varsel om pålegg, etter at han hadde la både lyd og bilete frå overvakingssystemet "live" ut på Internett. Kven som helst kunne dermed i prinsippet både sjå og høre dei tilsette via nettet.

Ny teknologi fører med seg ei utbreiing der ein ikkje kan vente at den som set eit overvakingssystem i drift, har nødvendig kjennskap til krava i regelverket vedrørende overvaking og dei nye tryggleiksutfordringane som digitaliseringa inneber. Tilrettelegging av digitale system gjer det mogleg at bruken av opplysningane går utover det som blir sett på som kameraovervaking, nemlig digital bearbeiding. Digital bearbeiding blir i dag nytta aktivt i mange system for å detektere uønskt åtferd i eit overvaka område, eksempelvis ved at det går ein alarm til vaktpersonalet dersom nokon klatrar på eit gjerde, eller ved uventa oppstimlingar av personar. Enkelte av desse eigenskapane blir også realiserte i analoge overvakingssystem.

Gjenkjenningsteknologi er det neste steget. Det finst i dag gratis programvare som mogleggjer pålogging til din personlege PC ved hjelp av ansiktsgjenkjenning. Meir inngripande er det om dette blir sett i system i eit overvakingssystem. Det kan verke føremålstenleg at kjøpmannen blir alarmert dersom ein kjend, men uønskt, kunde dukkar opp i butikken. Faren er at det moderne kameraovervakingssystemet kan nyttast stigmatiserande.

Det er ikkje vanskeleg å sjå at overgangen til digitale system omfattar meir enn kva regelverket

reknar som kameraovervaking. Den som vel å setje opp desse systema må vurdere om ein held seg innanfor kategorien kameraovervaking, eller om ein gjennom overvakinga føreteik ei anna behandling av personopplysningar. Dersom ein hamnar utanfor det tradisjonelle kameraovervakingssomgrepet, må ein sørgje for at det ligg føre eit anna lovgrunnlag for denne behandlinga.

Avgrensa høve til utlevering

Ein konsekvens av auka overvaking er at risikoen aukar for at opptak kjem på avvegar eller blir utleverte. Ved at stadig fleire område er overvaka aukar også sjansen for at den aktuelle hendinga blir fanga opp av eit kamera. Videoopptak av ulike hendingar, som ran eller ulykker, vil kunne vere av stor interesse for ulike medium ettersom live-opptak blir rekna for å ha ein vesentleg dramatiserande effekt. Etter gjeldande reglar føreset dette anten at den som er avbilda samtykkjer til utleveringa, eller at høvet til utlevering følgjer av lov.

Videoen frå Plata

Problemstillinga blei aktualisert sommaren 2004 då Politiets særskilte etterforskningsorgan (SEFO) meinte at Oslopolitiet braut personopplysningsloven då usladda overvakingssystemet av narkomane på "Plata" i Oslo blei frigitt og seinare viste på NRK. Det vil i slike saker vere sjølve utleveringa av opptaka som er ulovleg etter personopplysningsloven. Det forholdet at opptaka seinare blir publiserte i media er unnateke frå personopplysningsloven endå om dei aktuelle bilda er framskaffa på ulovleg vis. Avgrensingar i høvet til publisering av slikt materiale vil eventuelt følgje av anna regelverk, for eksempel Ver Varsam-plakaten.

Overvaking av arbeidsplassen

Kameraovervaking er ei særleg belastning på område der tilsette oppheld seg store delar av arbeidstida. Lovverket stiller opp skjerpa krav til overvaking som blir gjorde på slike område. Datatilsynet har likevel blitt kontakta ei rekkje gonger frå tilsette i verksemdar som nyttar kameraovervaking. Eksempel på enkeltsaker frå 2004 om overvaking på arbeidsplassen:

Nesset kommune

Datatilsynet blei gjort merksam på at Nesset kommune nytta kameraovervaking for å avsløre tjuveri frå diverse felleskassar på arbeidsplassen. Kameraovervakinga var ikkje skilta, men tilsette med tenestleg tilgjenge til det aktuelle området blei

munntleg informerte. Datatilsynet konkluderte med at dette ikkje tilfredsstilte kravet til nødvendig varslng og at overvakinga dermed hadde karakter av å vere skjult. Tilfellet var også eit brot på prinsippet om at overvaking som hovudregel berre skal gjerast med preventivt formål, og at det berre er politiet som er tillagd oppgåva med å innhente bevis til bruk i straffesaker.

Politiet forfølgde saka på sjølvstendig grunnlag og utferda eit førelegg til kommunen på ti tusen kroner for ulovleg overvaking. Kommunen vedtok førelegget.

Bakehuset Kafe

Datatilsynet føretok etterkontroll ved Bakehuset Kafe i Bærum. Kafeen var også blitt kontrollert i 2002. Den gong overvaka arbeidsgivar delar av arbeidsområdet til dei tilsette. Verksemda si grunnngiving blei den gong akseptert under noko tvil, men på føresetnad av at overvakinga ikkje skulle vere permanent og behovet vurderast jamleg.

Etterkontrollen avdekte at verksemda nå i staden hadde utvida overvakinga slik at ho omfatta størstedelen av arbeidslokala. Dei tilsette var dermed under permanent overvaking. Datatilsynet påla verksemda å stanse overvakinga med unntak av område der behovet for overvaking er godt grunnngitt og dokumentert. Vedtaket er anka inn for Personvernemnda.

Delegasjon av tilsynsansvar

Det er vanskeleg å gi noko sikkert overslag over kor mange kameraovervakingssystem det finst i Noreg, ettersom meldeplikta til Datatilsynet blir etterlevd i svært avgrensa grad. Datatilsynet har motteke totalt 2 015 meldingar om kameraovervaking. Av desse er 1 006 melde i 2004. Det er grunn til å tru at det reelle talet på overvakingssystem er langt større. Av ressursmessige årsaker blir dermed Datatilsynets kontroll med kameraovervakinga nødvendigvis sporadisk.

Dette er ein av grunnane til at Datatilsynet i samarbeid med Justisdepartementet har lagt fram forslag om å overføre ansvar for kontroll og tilsyn med kameraovervaking til dei kommunar som ønskjer det. Dette vil gjelde kameraovervaking innanfor kommunegrensene. Slik vil kommunane få eit større ansvar for, og høve til, å ta del i utviklinga av personvernet innanfor kommunen sine grenser. Ei omlegging vil også kunne innebere ein ikkje uvesentleg auke i det totale talet på tilsyn med aktørar som driv kameraovervaking, i tillegg

til å heve den lokale interessa for problemstillingane.

8.7 Justissektoren

I kor stor grad det skal vere mogleg for staten å innskrenke individas integritet er eit heilt grunnleggjande viktig tema når det gjeld bruk av politimetodar for å oppklare og førebyggje kriminalitet. Det er eit openbert dilemma at dei som samfunnet i første rekkje ønskjer å ramme med nye og utvida politimetodar, dei mest ressurssterke og farleg kriminelle, raskt vil tilpasse seg den nye røyndommen. På denne måten kjem samfunnet inn i ein vond sirkel, der politiet ser behov for å ta i bruk stadig meir inngripande og integritetskrenkjande metodar. Datatilsynet er også betenkt over den aukande usynleggjinga av politiet og metodane dei nyttar, i ei tid der dei fleste politikarar tek til orde for eit meir synleg politi.

Politimetodeutvalet

Politimetodeutvalets rapport *Mellom effektivitet og personvern* (NOU 2004:6) blei lagd fram våren 2004. Juridisk seniorrådgivar i Datatilsynet Guro Slettemark var oppnemnd som utvalsmedlem. Ho hadde grunnleggjande dissensar i forhold til fleirtalets forslag og var representert i utvalets mindretal, som også kom med eit eige lovforslag. I Datatilsynets seinare høringsfråsegn blei det særleg reagert på framlegga om dataavlesing og romkontroll.

Førebygging av kriminell aktivitet inneber at politiet innleier ei form for etterretning før handlinga faktisk skjer. Førebyggingsarbeidet kan dermed føre til at politiet samlar inn informasjon om menneske som ikkje har gjort noko kriminelt, og som kanskje heller ikkje vil komme til å gjere det.

Å sameine personvern og politiets behov for nye metodar for førebygging av straffbare handlingar er vanskeleg. Metodane som politiet nyttar seg av vil i seg sjølv kunne føre til alvorlege krenkingar av personvernet og andre verdiar som er sentrale i ein rettsstat.

Dataavlesing – eit inngrep i tanken?

Dataavlesing er ein svært integritetskrenkjande metode. Metoden inneber at informasjon som ikkje er kommunisert kan bli nærmare undersøkt av politiet. Dette kan for eksempel skje ved at politiet installerer ein spionprogramvare på datamaskinen til vedkommande. Programmet registrerer kvart einaste tastetrykk, også tekst og tal som brukaren seinare slettar. Programmet sender alle desse detaljregistreringane fortløpande til politiet.

Alt dette skjer utan at eigar og brukar av datamaskinen er klar over det.

Ved bruk av denne metoden kjem ein inn på eit svært problematisk område når det gjeld rettstryggleik. Tankar, assosiasjonar og ønske, som kanskje aldri eingong var tenkt kommunisert til andre, skal vere med å bevisе at nokon er skyldig. Då må vi stille oss spørsmålet: Kven kan eigentleg vere i stand til å vurdere om det eine tankesettet er meir mistenkeleg enn det andre?

Ei anna grunnleggjande problem er dei store sjansane for at også uskyldige blir ramma ved bruk av metoden. Det kan vere mange brukarar av ein datamaskin. Dermed vil også familiemedlemmer, arbeidskollegaer og andre som slett ikkje har noko med ei mogleg kriminell handling å gjere bli utsette for direkte overvaking frå politiet.

Datatilsynet meiner at behovet for, og konsekvensane av dataavlesing er så mangelfullt utgreidd at det ikkje bør akseptast at metoden blir teken i bruk.

Også spørsmålet om romkontroll (romavlytting) inneber mange av dei same problemstillingane som dataavlesing. Datatilsynet ser også her openberre problem i forhold til uskyldige tredjepersonar, og opphopping og bruk av overskottsinformasjon.

PSTs særlege behov

Politimetodeutvalets fleirtal ønskjer at også det alminnelege politiet skal få tilgang til dei fleste ekstraordinære metodane det er gjort framlegg om. Datatilsynet er einig med mindretallet i utvalet som hevdar at Politiets tryggleiksteneste (PST) treng betre heimlar for metodane dei nyttar no, i tillegg til at også nye metodar må lovfestast. Det alminnelege politiet har likevel ikkje eit tilsvarende behov som PST og bør dermed heller ikkje få det same armslaget.

Eit paradoks

For Datatilsynet er det eit paradoks at mens ein roper etter stadig nye og meir inngripande politimetodar for å avdekkje alvorleg kriminalitet, kan dei kriminelle miljøa i ro og mak lytte til politiets kommunikasjonssamband, for dermed å følgje med i kva politiet til kvar tid føreteik seg. Datatilsynet kan ikkje sjå at ei stadig utviding av politiet sine heimlar er det rette svaret på behovet for eit tryggare samfunn. Det er allment kjent at politiet ikkje har teke i bruk mange av dei metodane som dei tidlegare har bedt om og fått lovheimla. Datatilsynet ser også ein fare for at dei uskyldige blir stadig

tettare overvakte, mens dei kriminelle tilpassar seg og finn nye måtar å drive verksemda si på.

Heimlar

Datatilsynet er einig med Politimetodeutvalet i at dagens metodebruk bør få klarare lovheimlar. Jo meir inngripande ein metode er, jo klarare lovheimel bør denne ha. Det bør også i rimeleg grad vere mogleg for kvar enkelt å rekne med under kva omstende ein kan risikere å bli utsett for metodebruken til politiet. Behovet for metodebruken må også dokumenterast, slik at ein i etterkant kan sjekke om inngrepet var rettkome.

Underretning om bruk av metodar

Prinsippet om underretning er eit viktig verktøy for kvar enkelt til å vareta sin eigen rettstryggleik. Politiets metodebruk blir meir og meir teknologisk sofistikert, og sjansen for at metodebruken ikkje kjem kvar enkelt til kunnskap gjennom ein straffeprosess, vil alltid vere til stades der metodar blir nytta i førebygging. Grunnleggjande prinsipp som rett til innsyn og underretning til dei det vedgår, i det minste i ettertid, må vere eit vilkår for å tillate metoden. Unntak eller utsetting av desse rettane bør avgjerast av ein domstol.

Ny lov om politiregister

Også forslaget til ny politiregisterlov tek opp sentrale spørsmål om korleis politiets informasjonstilfang bør regulerast. Ikkje minst er det heilt sentralt å ta stilling til kva rettar borgarane skal få i forhold til å få innsyn i, og kontrollere kvaliteten på den informasjonen politiet samlar inn.

Politiregisterutvalets utgreiing *Kriminalitetsbekjempelse og personvern* (NOU 2003: 21) blei sendt på høring i meldingsåret. Datatilsynets avdelingsdirektør Knut B. Kaspersen sat som medlem i utvalet. Innstillinga frå utvalet var samrøystes.

Rettstilstanden når det gjeld personvernlovgivinga på politisektoren er i dag uklar. Datatilsynet har derfor i fleire år etterlyst eit betre lovgrunnlag for politiets innsamling, lagring, bruk og utlevering av personopplysningar. Etter Datatilsynets vurdering er utgreiinga og lovframlegget frå utvalet godt gjennomarbeidd og personvernet gjennomgåande teke vare på. Datatilsynet hadde likevel nokre prinsipielle merknader til utgreiinga.

Ansvar for behandling av personopplysningar i politiet

Det må vere avklart og tydeleg presisert kva nivå innetter i politiet som har ansvar for behandling av

personopplysningar. Den som blir pålagt ansvaret må vere godt kjend med, og føle ein nærleik til det lovverket det er gjort framlegg om. Innanfor politiet er dette ekstra viktig, då dei fleste av politiets register er sentraliserte. Datatilsynet meiner at politimeisteren i kvart enkelt politidistrikt må tilleggjast dette ansvaret.

Personvernombod

Datatilsynet har i fleire samanhenger teke til orde for at det bør utnemnast personvernombod innan politiet. Tilsynet er derfor tilfreds med at utvalet har komme med forslag om dette. Likevel burde det har blitt lagt større vekt på ordninga i framlegget til ny politiregisterlov. Kvart politidistrikt bør ha sitt eige personvernombod. Det kan også vurderast å gi personvernombodet avgjerdsrett når det gjeld bruk av politimetodar som ikkje krev rettsavgjerd.

Individets rettar

Rettar knytte til innsyn, retting og sletting av opplysningar som vedgår ein sjølv, er heilt grunnleggjande personvernprinsipp. Det har derfor mykje å seie for rettstryggleiken at den det gjeld får sjansen til å få kunnskap om at vedkommande er registrert hos politiet. Dette gjeld også endå om ein ikkje får vite meiningsinnhaldet, eller om kunnskapen først blir gitt i ettertid. Retten til innsyn, retting og sletting må derfor etter Datatilsynets vurdering speglast att i den nye politiregisterloven.

Datatilsynets rolle

Lovforslaget presiserer Datatilsynets kompetanse i forhold til klagesaker og generelle kontrolloppgåver. Ei presisering av Datatilsynets oppgåver i forhold til politiet er eit steg i riktig retning. Men Datatilsynet er kritisk til forslaget om at tilsynet skal få tilgang til kva som er registrert om ein person, utan at dei same opplysningane skal kunne formidlast vidare til vedkommande. Det blir i staden lagt opp til at Datatilsynet må nøye seg med å gi ei erklæring om at politiets behandling av personopplysningar eventuelt er tilfredsstillande. Dette er ingen ønskt situasjon for ein institusjon som legg stor vekt på omsynet til den personlege integritet og at kvar enkelt sjølv skal kunne kontrollere opplysningane som er registrerte om seg. Tilsynsoppgåva vil også bli vanskeleg å utøve på ein tilfredsstillande måte dersom Datatilsynet ikkje kan følgje opp eventuelle avdekte avvik med å gi politiet

pålegg. Tilsynsheimelen blir, sett i denne samanheng, ufullstendig og lite slagkraftig.

Sikring av politiets nødsamband

I 2001 trådde ei lovendring i kraft som førte til at det ikkje lenger er ulovleg å lytte på politiets radiosamband. Politidirektoratet orienterte derfor politieiningane om korleis dei skulle innrette seg i forhold til bruken av radiosambandet. Det blei særleg peikt på at ein framleis må overhalde teieplikta. Det blei oppfordra til bruk av alternative kommunikasjonsmetodar, slik som mobiltelefon eller avlyttingssikkert (kryptert) samband.

I kjølvatnet av denne lovendringa har det oppstått ei ny problemstilling ved at kommunikasjonen frå politisambandet også er blitt vidareformidla og lagd ut på Internett. Personopplysningar blir dermed gjort tilgjengelege for ein uavgrensa krins av personar. Politidirektoratet meinte at ei slik vidareformidling under alle omstende er kritikkverdig, og oppfordra Justisdepartementet, Post- og teletilsynet og Datatilsynet til å vurdere saka nærmare.

Brot på teieplikt

Datatilsynet kom til at vidareformidlinga er i strid med personopplysningsloven. Tilsynet deler også Politidirektoratets oppfatning av at formidling av informasjon som andre kan ta del i, er brot på politiets teieplikt. Det blei derfor gitt pålegg til politiet om at personopplysningar ikkje skal kommuniserast over det opne radiosambandet.

Datatilsynet er elles tilfreds med Stortingets avgjerd om å etablere eit nytt nødsamband. Dette ser ut til å kunne oppfylle dei krav som Datatilsynet har stilt.

DNA og biologisk materiale

DNA-profilar har blitt eit stadig viktigare bevis i straffesaker. På grunn av ny kunnskap og betre teknologi er det mogleg å få ut stadig meir informasjon, ikkje berre om dei personane som biomaterialet er henta frå, men også om slektningane deira. Desse nye moglegheitene stiller samfunnet overfor store etiske og personvernmessige utfordringar.

Regjeringa har derfor sett ned eit utval for å vurdere om høvet til å ta DNA-prøver skal utvidast, for eksempel slik at det blir same høve til dette som for fingeravtrykk. I tillegg skal utvalet vurdere om det skal opnast for å registrere DNA-profilar i fleire typar av saker og om sikting skal vere eit tilstrekkeleg vilkår for å registrere DNA-profilen til vedkommande. I dag er det krav om rettskraftig domfelling. Utvalet skal også vurdere eventuelle end-

ringar i saksbehandlingsreglane for registrering og søk i DNA-registeret.

Datatilsynets direktør er oppnemnt som utvalsmedlem. Utvalet skal slutføre arbeidet innan utgangen av 2005.

Politiets tilgang til biobankar

Interessant frå eit personvernperspektiv er også ei lovtolkingssak frå Justisdepartementet som konkluderer med at politiet ikkje utan vidare skal ha tilgang til biologisk materiale som ligg lagra i biobankane. Tolkinga gjeld biologisk materiale lagra med heimel i biobanklova, det vil i hovudsak seie prøver tekne for behandling eller forskning. Justisdepartementets lovavdeling strekar under at bruk av biologisk materiale er omfatta av strenge vilkår i biobankloven, og kan ikkje sjå at det er lovgrunnlag for regulær tilgang til biologisk materiale for å identifisere personar i samband med straffesaker. Berre unntaksvis, i tilfelle der politiet kan gjere nødrett gjeldande, kan det vere aktuelt å krevje tilgang på materialet, endå om det i utgangspunktet er i strid med loven. Lovavdelinga understrekar likevel at det skal mykje til før nødrett kan heimle handlingar som er i strid med ei klar lovføresegn.

Ein slik situasjon meinte Datatilsynet låg føre heilt på slutten av meldingsåret. Det blei i samband med flodbølgekatastrofen i Asia gitt løyve til at biologisk materiale frå mor og barn-undersøkingane kunne nyttast til identifikasjon av offer etter flodbølgekatastrofen.

Nye mobile fartsmålarar i politiet

Politiets data- og materiellteneste kontakta Datatilsynet for å få ei vurdering av eit prøveprosjekt der nye mobile fartsmålarar med nummergjenkjenning er under uttesting. Datatilsynet har gitt politiet tilbakemelding om at det nye systemet må vurderast opp mot politiets heimlar for å drive fartskontroll. Datatilsynet set spørsmålsteikn ved om det i vegtrafikkloven er eit tilstrekkeleg heimelsgrunnlag for bruk av den nye typen målarutstyr. Dette må avklarast før utstyret eventuelt blir teke i bruk.

Formålet må vere utvitydig

Utstyret vil kunne nyttast for to ulike formål, nemlig fartskontrollar og nummergjenkjenning. Ved fartskontrollar vil funksjonen nummergjenkjenning vere ein del av kontrollen. Men nummergjenkjenninga vil også kunne nyttast som ein separat funksjon, for eksempel i samband med ettersøking av bestemte kjøretøy. Dersom politiet ønskjer å ta i bruk utstyret til begge formål, må det også ligge

føre eit heimelsgrunnlag som dekkjer begge dei ulike formåla.

Utstyret inkluderer også ein digital biletfunksjon. Denne vil ikkje falle inn under føresegnene om kameraovervaking i personopplysningsloven. Heimelsgrunnlaget for denne bilettakinga må derfor søkjast i eit anna regelverk.

Risikomoment

Tendensen til at politiets utstyr i aukande utstrekning blir mobilt, set andre og heilt nye krav både til både lovgiving og informasjonstryggleik. Personvernomsyn og kravet til at kvar enkelt skal kunne vite kva ho kan rekne med må alltid vere sentrale element ved innføring av nye system. Klare lovheimlar må derfor vere eit minimumskrav.

Nummergjenkjenningssystemet inneber eit stort overvåkings- og misbrukspotensiale. Dette gjeld i forhold til kva register systemet kan koplatt opp mot, men også ved at brukaren av utstyret systematisk kan spore kjøretøy ved å utplassere dette på fleire stader. Ein generell risiko som følgjer kvart innkjøp av teknisk meir avansert utstyr er dessutan at dei nye moglegheitene i seg sjølv vil auke bruken av utstyret. Samtidig vil det bli eit press for å kunne ta utstyret i bruk for andre formål enn kva det opphavleg blei skaffa til vegar for.

Saka blei ikkje endeleg avklart i meldingsåret.

Tryggleiksklarering

Ei arbeidsgruppe sett ned av Forsvarsdepartementet foreslo blant anna lovheimel for bruk av lyd- og biletopptak i samband med tryggleiksklarering. Datatilsynet meiner at søkjarar for tryggleiksklarering bør kunne få innsyn i slike opptak av tryggleikssamtaler. I si høringsfråsegn etterlyste Datatilsynet også ei drøfting av kvaliteten i dei registra som blir sjekka ved tryggleiksklarering.

Framlegga arbeidsgruppa la fram kom som eit resultat av at Stortingets EOS-ugal har sett søkjelyset på rettstryggleiken til kvar enkelt som søker tryggleiksklarering. Utvalet uttrykte at det må setjast strenge krav til saksbehandlinga, og ønskte særleg betre høve til innsyn.

Opptak av tryggleikssamtale

Opptak av tryggleikssamtaler er grunnlagt med rettstryggleiksomsyn. Likevel kom arbeidsgruppa til at det ikkje skulle givast innsyn i opptaka. Datatilsynet støttar ikkje dette synspunktet. Innsyn i opplysningar som vedgår ein sjølv er ein viktig rettstryggleiksgaranti. I dette tilfellet er opplysningane opptak av kva ein faktisk har sagt og gjort. Datatilsynet ser det som underleg at ein vel å grunngi eit

tiltak med omsyn til rettstryggleik, samtidig som ein eliminerer eit svært viktig aspekt nettopp ved rettstryggleiken.

Kor korrekte er registra?

Når ein vurderer ei tryggleiksklarering, konsulterer ein ei rekkje register for å finne opplysningar om søkjaren. Arbeidsgruppa drøfta berre spørsmålet om kvaliteten på desse registra i saker der det kan vere aktuelt å nekte klarering på grunn av økonomiske forhold. Dette blir grunnlagt med at kredittopplysningsbyråa sine register ikkje alltid er oppdaterte.

Problemet med manglande kvalitet kan likevel vere like utbreidd i dei andre registra som blir nytta i klareringssaker.

Kvalitetsnivået i kredittopplysningsføretaka sine register er godt kjent. Årsaka er den opne bruken av registra, og at det blir gitt gjenpart til den registrerte. Feil er dermed relativt lette å oppdage. Opplysningar i politiets register er derimot skjulte for vedkommande. Ein har dermed ikkje dei same mekanismene for å få verifisert opplysningane. Denne situasjonen gjer det viktig å kvalitetssjekke også opplysningar av ikkje-økonomisk karakter som blir nytta i ei klarerings-sak.

Underretning til dei det gjeld

Datatilsynet er også oppteke av at søkjarar som er blitt tryggleiksklarerte skal underrettast.

Lagringsplikt for tele- og internettrafikk?

Å påleggje teleoperatørane ei lagringsplikt for trafikkdata har lenge vore eit omdiskutert tema både i Noreg og elles i Europa. Terrorangrepet i Madrid utløyste eit nytt politisk press på EU-nivå om å avklare forholda rundt slik datalagring. På EU-toppmøtet i mars 2004, blei det vedteke at eit forslag om dette skal utarbeidast og vedtakast seinast juni 2005. Storbritannia, Sverige, Irland og Frankrike kom seinare med eit forslag til rammevedtak. Dette blei i desember 2004 drøfta av justisministrarane i EU. Forslaget inneber at data frå "allment tilgjengelege kommunikasjonstenester" skal lagrast i 12-36 månader. Forslaget innskrenkar seg dermed ikkje til telefoni. Også datatrafikk inngår, det vil seie opplysningar om kva nettstader du har besøkt og til kva adresser du har sendt e-post. I tillegg handlar det ikkje berre om bruke tele- og trafikkdataa til å oppklare, men også til å førebygge kriminalitet.

Forslaget til rammevedtaket gjeld det såkalla tredjepillars-samarbeidet, (Justis- og tryggleiksområdet i EU). Det blir dermed ikkje omfatta av EØS-samarbeidet. Likevel må det, dersom forslaget går igjennom, ventast eit sterkt press også på norske styresmakter for å innordne seg det same regelverket. Også fleirtalet i politimetodeutvalet foreslo at politiloven skal få føresegner om lagringsplikt. Datatilsynet gjekk i si høringsfråsegn mot dette forslaget. Tilsynet ser behov for å utgreie spørsmålet nærmare og etterspør ei reoppnemning av Datakrimutvalet. Dette utvalet hadde, i motsetning til Politimetodeutvalet, i mandatet sitt å vurdere spørsmålet om lagringsplikt.

Brot på menneskerettane

Det er eit grunnleggjande personvernprinsipp at opplysningar som er meint å skulle brukast for eitt formål, ikkje skal brukast til andre formål. Når formålet er oppfylt, skal opplysningane slettast.

Lagring av trafikkdata ut over det som er nødvendig for gjennomføring av tenesta, vil bety at det blir lagra mange trivielle opplysningar om mange abonnentar. Store mengder informasjon om ei heil befolknings bruk av elektronisk kommunikasjon vil bli lagra, for at ein liten del som gjer noko kriminelt skal kunne etterforskast meir effektivt. Dette rokkar ved den grunnleggjande retten det er å kunne røre seg fritt utan at nokon held auge med ein.

Dei europeiske datatilsynsstyresmaktene har derfor, gjennom sitt samarbeidsorgan "artikkel 29-gruppa", retta ein skarp kritikk mot forslaget om lagringsplikt. I ei felles kunngjering hevdar tilsynsstyresmaktene at heile forslaget strir mot den europeiske menneskerettskonvensjonens artikkel 8, der det heiter: "*Kvar og ein har rett til vern for sitt privatliv og familieliv, sin heim og sin korrespondanse*".

Amerikanarane sitt krav om utlevering av passasjeropplysningar

Saka blei utførleg omtalt i årsmeldinga for 2003. Kravet frå amerikanarane blei innfridd ved ei Kommisjonsavgjerd i 2004. Dei europeiske datatilsynsstyresmaktene har utforma retningslinjer for å sikre at passasjerane får tilstrekkeleg informasjon om kva opplysningar som blir overførte til amerikanarane og kva dei skal brukast til. For Noregs del vil kommisjonsavgjerda bli ein del av norsk regelverk, med mindre Noreg reserverer seg mot avgjerda. I eit brev til Justisdepartementets lov-

avdeling har Datatilsynet teke til orde for ein slik reservasjon.

Politisamarbeid over landegrensene

Innan EU har det vore stor aktivitet i forhold til auka politisamarbeid medlemslanda imellom. Etter terroråtakene i Madrid i mars 2004, har det komme ei rekkje forslag frå EU om effektivisering og tettare samarbeid mellom politimyndigheitene. I eit personvernperspektiv ligg dei største utfordringane i ønsket om auka utveksling av personopplysningar over landegrensene. På det politiooperative, administrative og politiske plan i Noreg, er interessa svært stor for eit tett samarbeid med EU. Dette er ei urovekkjande utvikling både ut i frå grunnleggjande demokratiske og personvernsmessige omsyn.

For Noregs del har det vist seg relativt enkelt å få delta i det operative samarbeidet meir eller mindre på lik linje med EU-landa ved å inngå samarbeidsavtalar. Men når det kjem til dei organ som skal sikre rettane for individ og føre kontroll med politisamarbeidet, har Noreg ikkje fått bli med. Eit godt eksempel på dette er Europol-samarbeidet, der Noreg ikkje deltek i det felles tilsynsorganet Joint Supervisory Body (JSB). Datatilsynet har også tidlegare uttrykt bekymring over dette.

Schengen informasjonssystem

JSA er det felles tilsynsorganet for Schengen informasjonssystem (SIS). Informasjonssystemet inneheld opplysningar om personar som er ettersøkte, sakna, nekta innreise til Schengenområdet, eller er straffedømde i eit av medlemslanda. Datatilsynet møter med ein fast observatør. JSA hadde i 2004 eit høgre aktivitetsnivå enn vanleg. Dette er hovudsakeleg grunna i generelt stor aktivitet innan Schengensamarbeidet. JSA har i tillegg hatt fellesmøte med tilsynsorganet for Europol, og tilsvarande når det gjeld tollsamarbeidet.

JSA har særleg hatt fokus på personvernutfordringane i forhold til forslag om utviding av Schengen informasjonssystem (SIS). I mai kom JSA med ei offentleg fråsegn om utviklinga. JSA stiller seg kritisk til at fleire etatar skal få tilgang til opplysningane som er registrerte i SIS. Dette aukar faren for at opplysningane vil bli brukte til andre formål enn dei opphavleg var innsamla for. JSA er også uroleg over det presset som heile tida er der for å ta inn nye kategoriar av opplysningar i Schengen informasjonssystem. Det blir åtvara mot ei utvikling der sjølve formålet med systemet ikkje lenger er retningsgivande for kva opplysningar som kan regis-

trerast. I staden legg ein vekt på kva det er mogleg å leggje inn av nye kategoriar av opplysningar. Biometriske data er eit eksempel på nye kategoriar som ein ønskjer å få registrert.

Samarbeidsavtale med Eurojust

Datatilsynet er i ei viss utstrekning blitt rådført i samband med forhandlingar om å inngå ein samarbeidsavtale med Eurojust (samarbeid på påtalesida innan EU). Som ein viktig premisse for Stortingets behandling av spørsmålet om å inngå avtale, er Datatilsynet oppteke av at det blir gjort nødvendige avklaringar rundt individas rettar, medrekna at norske borgarar blir sikra eit like godt personvern som borgarane i EU. Ei anna utfordring er at personopplysningsloven har eit svært avgrensa verkeområde. Denne kan derfor ikkje nyttast som trygd for at individas rettar blir tekne vare på i samband med Eurojust.

8.8 Arbeidsliv

Som tidlegare år er problemstillingar knytte til personvern i arbeidslivet eit av dei områda der Datatilsynet mottek flest førespurnader frå publikum. Førespurnadene fordeler seg jamt mellom arbeidsgivar- og arbeidstakersida og dreier seg i stor grad om arbeidsgivarar sin innsyn i e-post og internettloggar, kontroll av telefonbruk, kameraovervaking og opptak av telefonsamtalar. Ettersom mange førespurnader også dreier seg om forhold som ligg i grenselandet mellom personopplysningsloven og arbeidsmiljøloven har Datatilsynet etablert ein nærmare dialog med Direktoratet for arbeidstilsynet. Dei to tilsynsetatane utvekslar informasjon om aktuelle saker, blant anna om bruk av vandelsattestar, rusmiddelkontroll og ulike typar arbeidsmiljøundersøkingar.

Felles nordisk tilsynsprosjekt

Det nordiske Datatilsynssjefsmøtet vedtok i 2003 at det skulle gjennomførast eit samnordisk tilsynsprosjekt for å sjå nærmare på behandling av personopplysningar i tilsetjingsprosessar. Det blei for Noregs del gjennomført tilsyn mot vaktelskapa Falck Norge AS og Securitas AS. I tillegg også mot teknologikonsernet Nokia Norge.

Manglande sletting av personopplysningar

Eit trekk som gjekk igjen i dei tre kontrollerte verksemdene var at det mangla retningslinjer for korleis ein skulle ta vare på kvar enkelt sin rett til innsyn i registrerte opplysningar. Det var heller ikkje tilfredsstillende rutinar for retting og sletting

av personopplysningar. Alle dei tre selskapa oppbevarte opplysningar i personalmappene som skulle ha vore sletta. Hos begge vaktelskapa låg også tidlegare innhenta politiattestar framleis lagra i personalmappene. Dette strider mot lov om strafferegistrering og krava til sletting i personopplysningsloven. Formålet med politiattesten er oppfylt så snart det er godtgjort at den tilsette har tilfredsstillandeandel. Politiattesten skal deretter makulerast. Av andre opplysningar som burde vore sletta var blant anna svært gamle åtvaringar og sjukemeldingar. Dei tre verksemdene fekk pålegg om å gjennomgå personalmappene for å slette unødige personopplysningar. Dei fekk også pålegg om å utforme skriftlege rutinar for innsyn, retting og sletting.

Securitas har anka pålegget om å makulere tidlegare innhenta politiattestar inn for Personvernemnda.

Eigenerklæring omandel

Vaktelskapa har gjennom Lov om vaktvirksomhet med forskrift heimel til å innhente politiattest. Attesten viser om søkjaren tidlegare har vore straffa eller bøtelagd, eller om vedkommande er under etterforsking.

Securitas henta i tillegg inn eigenerklæringar omandel. Her blei søkjarane bedt om å gjere greie for forhold som går ut over dei opplysningane som går fram av politiattesten.

Dette er ein tendens Datatilsynet har sett også hos arbeidsgivarar i andre bransjar, som ikkje har høve til å innhente politiattest. I mangel av nødvendig lovheimel ber arbeidsgivar jobbsøklarar og tilsette om at dei i staden fyller ut eigenerklæringar omandel, for eksempel om vedkommande nokongong har vore mistenkt eller skulda for moglege straffbare forhold. Innhenting av denne typen eigenerklæringar inneber etter Datatilsynets vurdering ei omgåing av lovgivars intensjonar med å avgrense tilgangen til vandelsopplysningar.

Datatilsynet påla Securitas å avvike ordninga med å innhente eigenerklæring omandel.

Eigenerklæring om helse

Securitas nytta også ei svært omfattande eigenerklæring om helse, der søkjaren blei bedt om å gi opplysningar om blant anna syn, hjarteproblem og kondisjon.

Datatilsynet gav vaktelskapet pålegg om å avslutte innhentinga av helseopplysningar via eigenerklæring. Etter å ha vore i ein etterfølgjande dialog med Securitas har Datatilsynet gjort om vedtaket, slik at enkelte relevante helseopplysningar no blir rekna som lovleg innhenta, under føresetnad

av at arbeidstakaren samtykkjer til dette. Dette gjeld blant anna opplysningar om hørsel, syn og fargesans. I tillegg også opplysningar om sjukdomstilstandar som kan gjere den tilsette uskikkelig til å utføre enkelte arbeidsoppgåver innan vaktverksemda.

Ikkje samtykke for rusmiddeltesting

Securitas hadde også etablert eit system for rusmiddeltesting av sine tilsette, basert på samtykke. Datatilsynet meiner likevel at arbeidsgivars styringsrett og samtykke frå dei tilsette ikkje er eit tilstrekkeleg heimelsgrunnlag for å kunne gjennomføre rusmiddeltestar. Endå om Datatilsynet må vise varsemd med å overprøve eit gitt samtykke, er det ikkje tvil om at mange arbeidstakarar føler seg forplikta til å seie ja til denne typen inngrep. Konsekvensen av å ikkje gi samtykke til rusmiddeltesting vil lett vere at ein heller ikkje får jobb.

Når ein tek omsyn til den inngripande karakteren som rusmiddeltesting inneber, og den manglande maktbalanse det er mellom arbeidsgivar og arbeidstakar, meiner Datatilsynet at det er lovgivar som må avgjere kva for bransjar og arbeidsforhold som gjer det nødvendig med rusmiddelkontrollar. Både formålsføresegnene i personopplysningsloven, omsynet til menneskerettane og legalitetsomsyn tilseier ei restriktiv holdning.

Endå om vaktelskapet hevder at kundane og allmenta forventar ein særskilt kontroll av tryggleikspersonellet, meiner Datatilsynet at Securitas ikkje har dokumentert eit større behov for rusmiddeltesting enn kva andre arbeidsgivarar kan føre i marka. Personar som på grunn av rusproblem ikkje er eigna til å arbeide i vaktelskapa må fangast opp på anna vis.

Vedtaket er påklaga til Personvernemnda.

Ny arbeidslivslov

Arbeidslivslovsutvalet leverte våren 2004 ei svært omfattande utgreiing.

Formålet med utgreiinga var å få til ei forbe-tring og forenkling av den gjeldande arbeidsmiljøloven. Når det gjeld dei delane av utgreiinga som omtaler kontroll og overvaking i arbeidslivet kan Datatilsynet likevel ikkje sjå at dei endringane det er gjort framlegg om medverkar til verken forbe-tring eller forenkling.

Føresegnene i forslaget gir berre generelle overordna prinsipp, som allereie finst i personopplysningsloven. Framlegga vil ikkje gi dei presiseringar som Datatilsynet har sett behov for når det gjeld bruk av personopplysningar i arbeidslivet. Etter Datatilsynet si oppfatning høyrer denne typen

presiseringar og konkretiseringar heime i forskrifta til personopplysningsloven, og ikkje ny arbeidslivslov. Det er uheldig når regelverk som gjeld bruk av personopplysningar blir spreidde utover i lovverket. Det er upedagogisk og lite formålstenleg at behandling av personopplysningar i personalmapper skal følgje reglane i personopplysningsloven, mens opplysningar knytte til tilsette sin e-post skal regulerast i ny arbeidslivslov.

Utvalet legg stor vekt på bruk av samtykke som grunnlag for kontroll av tilsette. Både i EUs personverndirektiv og i vår eigen personopplysningslov er samtykke eit sentralt utgangspunkt for å kunne behandle personopplysningar. Innan arbeidslivet knyter det seg likevel vesentlege avgrensingar til eit slikt samtykke. I mange situasjonar vil den tilsette ikkje stå overfor eit reelt val når det gjeld å gi samtykke eller ikkje. Skal eit samtykke vere reelt må det vere frivillig. Arbeidstakar må også seinare, utan at det fører til negative konsekvensar, kunne trekkje samtykket sitt tilbake.

Datatilsynet er derimot tilfreds med at utvalet ikkje legg opp til samtykke som behandlingsgrunnlag for helseundersøkingar og liknande.

Tillitsvalde får innsyn i lønnsopplysningar

I 2001 avgjorde Datatilsynet at arbeidsgivar ikkje, utan samtykke frå arbeidstakar, kunne utlevere lønnsopplysningar til tillitsvalde om uorganiserte eller organiserte i andre arbeidstakarorganisasjonar i forkant av lønnsforhandlingane. Det var berre få unntak frå regelen, blant anna ved spørsmål om brot på det såkalla ufråvikelegprinsippet, eller saker som vedgår likestillingsloven.

Etter at det kom fram nye moment frå Landsorganisasjonen vurderte Datatilsynet saka på nytt i 2004.

Datatilsynets vurdering

I dei fleste tilfella er det tilstrekkeleg for tillitsvalde å få opplysningar om tilsettes lønn på gruppenivå i samband med lønnsforhandlingane. Så lenge kategoriseringa, det vere seg stilling, kva organisasjon ein tilhører, eller kjønn inneheld opplysningar om fem eller fleire personar, vil opplysningane ikkje omfattast av personopplysningsloven.

Når det dreier seg om færre enn fem personar kan enkeltpersonar kunne identifiserast indirekte

og personopplysningsloven gjeld. Etter Datatilsynets nye vurdering kan dei tillitsvalde likevel få tilgang til lønnsopplysningar om færre enn fem personar. Men den tillitsvalde må då skrive under på ein teielovnad.

Til grunn for at Datatilsynet har endra oppfatning er også omsynet til forskjellen mellom offentlig og privat sektor på grunn av reglane i offentlegloven.

Personlegdom i panna

Ei sak som dukka opp heilt i slutten av meldingsåret illustrerer at Datatilsynet enkelte gonger må stille spørsmål ved arbeidsgivars respekt for den personlege integriteten til den tilsette, endå om personopplysningar ikkje direkte blir behandla.

For å betre kommunikasjonen internt i selskapet Transocean blir dei tilsette oppfordra til å ta ein personlegdomstest. På bakgrunn av testen blir arbeidstakarane så kategoriserte i ein til to av fire førehandsdefinerte kategoriar, symboliserte gjennom fire ulike dyrearter og fargar. Ein klistrelapp som viser kva kategori den tilsette tilhører blir deretter sett på vedkommande sin hjelm eller kontordør. På denne måten skal det synleggjerast for alle kva slags karaktertrekk vedkommande har. Dette skal lette kommunikasjonen medarbeidarane imellom.

Etter førespurnad frå Datatilsynet hevdar selskapet at gjennomføring av testen er frivillig. Dei tilsette utfører testen på eiga hand og finn sjølve ut kva kategori dei tilhører. Dei detaljerte testresultata blir heller ikkje oppbevarte. Det skjer dermed inga behandling av personopplysningar, slik personopplysningsloven definerer det.

Datatilsynet meiner likevel at tiltaket, slik det er gjennomført, kan krenkje den personlege integriteten til kvar enkelt. Arbeidstakaren vil lett oppleve press i retning av å måtte gjennomføre testen, for deretter å feste klistremerket som signaliserer personlegdom på hjelmen. Dette vil lett kunne virke stigmatiserende, også om ein, som ein av få, skulle nekte å la seg merke på denne måten.

Datatilsynet meiner at det bør vere mogleg å skape medvit om kor viktig det er med god kommunikasjon mellom menneske på ein arbeidsplass på mindre potensielt krenkjande måtar.

Undervedlegg 1

Rettsikkerhet på vikende front

av Anders Ryssdal, leder Advokatforeningen

Når terror og organisert kriminalitet rammer, tar frykten grep. Samfunnets vilje til å beskytte seg øker, og politikernes ønske om å vise handlekraft blir tilsvarende sterkere. Dette tvinger oss til å ta noen avgjørende valg med hensyn til hva slags samfunn vi ønsker å leve i, og hvordan vi veier frihet mot trygghet.

Teknologisamfunnet åpner for nye og uoverskuelige muligheter når det gjelder innsamling, lagring og bruk av informasjon, både for forvaltning og næringsliv. Potensialet for effektivisering og rasjonalisering er stort, men registrering av data åpner også for misbruk av den informasjon som samles inn. Det må derfor være klare grenser for bruk, gjenbruk og sammenkopling av informasjon. Det må også utvises forsiktighet ved utvidelse av eksisterende hjemler til bruk av ny teknologi til overvåkning.

Dette prinsipielle utgangspunkt mistes lett av synet når utviklingen skjer fra sak til sak under press fra media, og etter oppslag om terrortrusler, alvorlige ran og andre hendelser som medfører frykt. Derfor trenger vi Datatilsynet, som på et prinsipielt grunnlag kan vurdere hver enkelt utvidelse av reglene for innsamling, oppbevaring og sammenkopling av informasjon. Noen må forsøke å bremse utviklingen når en rekke velmente enkeltreguleringer gjør at vi får et samfunn der myndighetenes kunnskaper om den enkelte blir så omfattende at det går på bekostning av friheten og retten til privatliv. Advokatforeningen ønsker å være med på å ta sin del av ansvaret. Advokater er i sitt arbeid avhengige av en velfungerende rettsstat, og derfor må også vi være voktere av rettsstatens grunnleggende verdier.

Enhver vurdering av nye tiltak forutsetter at man har noen klare prinsipper og begreper som nye tiltak kan vurderes opp mot. Et viktig grunnleggende begrep er rettsikkerhet. Begrepet har imidlertid fått et upresist innhold. I dag blir begrepet rettsikkerhet benyttet i to betydninger. Rettsikkerhet blir brukt både i betydningen "et vern for borgerne mot vilkårlighet, uforutsigbarhet og usaklig forskjellsbehandling fra staten", men også i betydningen "en plikt for staten til å beskytte borgerne mot trusler som kriminalitet og terror." I kjølvannet av de senere års terrorhendelser og økte fokus på organisert kriminalitet, har det blitt mer vanlig å benytte rettsikkerhetsbegrepet i den siste betydningen.

De to definisjonene av begrepet er til dels motstridende. De virkemidler som ønskes tatt i bruk for å bekjempe den antatte økte trusselfaren kan få den konsekvens at risikoen for overgrep fra myndighetene øker. Jeg vil derfor benytte begrepet rettsvern om statens plikt til å beskytte borgerne. Ved å bruke to begrep synliggjøres i større grad hvilke hensyn som står mot hverandre, og at rettsvern og rettsikkerhet i noen grad er uforenlige hensyn som må balanseres.

Rettsikkerhet er et vern for borgerne mot overgrep, vilkårlighet og usaklig forskjellsbehandling fra staten. Begrepet må, hvis det skal være en garanti for frihet og sikkerhet, peke mot hva som kreves før inngrep i borgernes rettigheter kan skje. Det ligger i rettsikkerhetsbegrepet et krav til at inngrep i borgernes rettssfære ikke kan skje uten hjemmel i lov, og at myndighetene holder seg innenfor sin lovhjemmel. Lovskravet er et uttrykk for demokratiet, borgerne styrer seg selv gjennom valg. Lovskravet er også en forutsetning for forutsigbarhet.

Rettsikkerhet er imidlertid ikke nødvendigvis godt ivaretatt selv om alle inngrep skjer med hjemmel i lov. Lover som hjemler overgrep er ikke uvanlige i totalitære stater, og statlige overgrep kan godt skje med hjemmel i lov. Begrepet må således innebære noe mer enn at hvert inngrep må skje med hjemmel i lov. I rettsikkerhetsbegrepet må det derfor også ligge en verdivurdering. Særlig krenkende handlinger eller inngrep i den fysiske eller psykiske integriteten kan ikke skje med mindre integritetskrenkelsen er vurdert og funnet helt nødvendig av hensyn til samfunnet.

Materiell rettsikkerhet har vi således først når alle inngrep i borgernes rettssfære skjer med hjemmel i lov, og når utformingen og anvendelsen av lovhjemmelen har vært underkastet en verdi- og nødvendighetsvurdering. Anvendelsen må skje uten usaklig forskjellsbehandling og vilkårlighet. Staten må også legge til rette for uavhengig prøvelse av om myndighetene har handlet i strid med ovennevnte krav. Slike prosessuelle garantier for at rettsikkerheten blir ivaretatt, er formelle rettsikkerhetsgarantier. De utgjør en forutsetning for materiell eller faktisk rettsikkerhet. Særlig viktig er det å få prøvet inngrep i den enkeltes fysiske og psykiske integritet.

Når politikere ønsker å innføre mer inngripende virkemidler, blir dette unntaksløst begrunnet med hensynet til effektivitet og hensiktsmessighet. Nye metoder for informasjonsinnhenting og sammenkopling av opplysninger fremstilles som uviktige og ubetydelige for den jevne borger, fordi de ikke rammer "den som ikke har noe å

skjule”. Virkemidlene blir av samme grunn akseptert. Ønsket om sammenkopling av registre med personopplysninger er et eksempel. Først forskyver man punktet for hvilke opplysninger som kan registreres og oppbevares. Dernest kobler man opplysningene sammen ved å vise til at dette forenkler forvaltningens arbeid. Dette gjelder både de virkemidler forvaltningen, for eksempel skatteetaten, ønsker for å lette sitt arbeid, og de virkemidler som ønskes av politi og påtalemyndigheten. Dette er synlig særlig på straffeprosessen område fordi de virkemidler som der ønskes innført, for eksempel romavlytting, er særlig inngripende. De virkemidler som forvaltningen ønsker innført, er langt mindre inngripende, men rammer langt flere.

Ønsket om å innføre romavlytting er et særlig inngripende virkemiddel. Ved å tillate romavlytting som etterforskningsmetode passerer man en grense inn i borgernes rettssfære som man tidligere ikke har ønsket å passere – fra overvåkning

av kommunikasjon til overvåkning av borgernes egne hjem. En stadig forskyvningen av balansepunktet, kan føre til at synet på hva som er en akseptabel og nødvendig integritetskrenkelse forskyves i individets disfavør. Dette er etter Advokatforeningens syn et skritt i gal retning i forhold til hvilket samfunn vi vil ha.

En velfungerende rettsstat hvor rettssikkerheten er tilfredsstillende ivarettatt forutsetter en stor grad av frihet for borgerne. Det er et problem for frie demokratiske stater å avgjøre hvilke virkemidler man kan ta i bruk uten å ødelegge den skjøre avveiningen mellom rettsvern og rettssikkerhet. Dette er langt på vei et prinsipielt spørsmål om hva slag samfunn man ønsker å leve i, og for tiden ser det ut til at frykten gjør at rettssikkerheten taper, men Datatilsynet vil sikkert ikke gi opp kampen for rettssikkerheten og fornuften. Det vil ikke Advokatforeningen heller.

Undervedlegg 2

Oversikt over gjennomførte tilsyn 2004

<i>Saksnr.</i>	<i>Tilsynsobjekt</i>	<i>Poststed</i>	<i>Bransje/sector</i>
2004/0311	Nokia Norge AS	Lysaker	Arbeidsliv
2004/1355	Advokatfirmaet Kvale & Co.	Oslo	Arbeidsliv
2004/1012	UPC AS - Kundesenter	Oslo	Arbeidsliv
2004/0587	Posten Norge AS	Oslo	Arbeidsliv
2004/0582	Hennes & Mauritz AS	Oslo	Arbeidsliv
2004/0312	Falck Noreg AS	Oslo	Arbeidsliv
2004/0310	Securitas AS	Oslo	Arbeidsliv
2004/0573	Peppes Pizza AS	Sandvika	Arbeidsliv
2004/0553	NoregsGruppa ASA	Oslo	Detaljhandel
2004/0552	COOP-kjeden	Oslo	Detaljhandel
2002/0768	Bakevarehuset AS	Asker	Kameraovervaking
2004/1505	Hydro Texaco	Bergen	Kameraovervaking
2004/1504	Bergen Storsenter	Bergen	Kameraovervaking
2004/0380	Sandviken Daglegvare	Bergen	Kameraovervaking
2004/1547	Terje Høili	Fredrikstad	Kameraovervaking
2004/1370	Torvbyen	Fredrikstad	Kameraovervaking
2004/1368	Hydro Texaco	Fredrikstad	Kameraovervaking
2004/1320	Narvesen Gardermoen	Gardermoen	Kameraovervaking
2004/1626	Mosaiske trossamfunn	Oslo	Kameraovervaking
2004/1566	ICA Norge AS v/Rimi Østbanehallen	Oslo	Kameraovervaking
2004/1538	XXL sport & villmark, Storgata	Oslo	Kameraovervaking
2004/1377	Elkjøp Stormarknad	Oslo	Kameraovervaking

<i>Saksnr.</i>	<i>Tilsynsobjekt</i>	<i>Poststed</i>	<i>Bransje/sector</i>
2004/0915	Oslo Sporveier	Oslo	Kameraovervaking
2004/0894	NSB Persontog AS	Oslo	Kameraovervaking
2004/0866	Profilhuset Meny-Ultra	Oslo	Kameraovervaking
2004/0865	Statoil Detaljist v/Skedsmo	Oslo	Kameraovervaking
2004/0864	Steen og Strøm Norge AS	Oslo	Kameraovervaking
2004/0862	Rimi Norge	Oslo	Kameraovervaking
2004/0861	Esso Tiger AS	Oslo	Kameraovervaking
2003/1104	Car Park (Oslo City)	Oslo	Kameraovervaking
2004/1475	Nygaten Vel	Stavanger	Kameraovervaking
2004/1410	Stavanger Storsenter	Stavanger	Kameraovervaking
2004/0863	Nille AS v/stovner senter	Ytre Enebakk	Kameraovervaking
2004/1328	it:solutions	Bergen	Internettrelatert
2004/0523	BGNett AS	Bergen	Internettrelatert
2004/0521	Telenor internett AS - Privatmarknad	Fornebu	Internettrelatert
2004/0524	Freewave AS	Lysaker	Internettrelatert
2004/1332	Netcom A/S	Oslo	Internettrelatert
2004/1331	FleetOnline Nordic	Oslo	Internettrelatert
2004/1330	800RINGE	Oslo	Internettrelatert
2004/1329	Fronter A/S	Oslo	Internettrelatert
2004/0522	UPC/Chello AS	Oslo	Internettrelatert
2004/1292	Grimstad Kommune	Grimstad	Kommune
2004/1293	SAS-Braathens AS	Oslo	Marknadsførarar
2004/0027	Bonnier DM AS	Oslo	Marknadsførarar
2004/1282	Klæbu Legesenter	Klæbu	Primærhelseteneste
2004/1284	Kvaløysletta legekantor	Kvaløysletta	Primærhelseteneste
2004/1281	Nermo Legesenter	Mo i Rana	Primærhelseteneste
2004/1283	Skåla legekantor	Skåla	Primærhelseteneste
2004/0355	Fjelstrup legeservice	Stavanger	Primærhelseteneste
2004/1276	Utsikten Legesenter	Tromsø	Primærhelseteneste
2004/1275	Nordbyen Legesenter	Tromsø	Primærhelseteneste
2004/1279	Risvollan Legesenter	Trondheim	Primærhelseteneste
2004/1280	Vikhammer Legekantor	Vikhammar	Primærhelseteneste
2004/1277	Ytteren Legesenter	Ytteren	Primærhelseteneste
2004/1018	Krisesenteret i Fredrikstad	Fredrikstad	Ideelle organisasjonar
2004/1020	Krisesenteret i Hamar	Hamar	Ideelle organisasjonar
2004/1291	Redningsselskapet	Høvik	Ideelle organisasjonar
2004/1290	Landsforeningen til støtte for krybbedød	Oslo	Ideelle organisasjonar
2004/1021	Krisesenteret i Oslo	Oslo	Ideelle organisasjonar
2004/1019	Krisesenteret i Sarpsborg	Sarpsborg	Ideelle organisasjonar
2004/0906	Krisesenteret i Tromsø	Tromsø	Ideelle organisasjonar
2004/1373	Stena Line Noreg AS	Oslo	Reiseverksemd
2004/1367	Skandinavisk reisefeber AS	Oslo	Reiseverksemd
2004/1363	Color Line	Oslo	Reiseverksemd
2004/1362	Mytravel Norway (ving)	Oslo	Reiseverksemd
2004/1376	Widerøes Flyveselskap	Sandvika	Reiseverksemd
2004/1574	Helse Vest RHF	Bergen	Større helseføretak
2004/1575	Helse Nord RHF	Harstad	Større helseføretak
2004/1451	Helse SØR RHF	Kristiansand	Større helseføretak
2004/1278	Helgelandssjukehuset HF (Mo i Rana)	Mo i Rana	Større helseføretak

<i>Saksnr.</i>	<i>Tilsynsobjekt</i>	<i>Poststed</i>	<i>Bransje/sektor</i>
2004/1573	Helse Øst RHF	Oslo	Større helseføretak
2004/1576	Helse Midt-Norge RHF	Trondheim	Større helseføretak
2004/0565	Telenor Mobil AS	Fornebu	Telekommunikasjon
2004/0577	Tele 2 AS	Oslo	Telekommunikasjon
2004/0571	Sense Communication AS	Oslo	Telekommunikasjon
2004/0569	Telio AS	Oslo	Telekommunikasjon
2004/0567	Netcom AS	Oslo	Telekommunikasjon
2004/0204	Bom- og Tunnelselskapet AS	Bergen	Transport
2004/1274	Rikstrygdeverket - sentralt	Oslo	Trygd
2004/1274	Fylkestygdekontor i Akershus	Oslo	Trygd
2004/1274	Trygdekontor i Oslo	Oslo	Trygd
2004/1274	Fylkestygdekontor i Sør-Trøndelag	Trondheim	Trygd
2004/1274	Trygdekontor i Trondheim	Trondheim	Trygd
2004/1491	Universitetet i Bergen	Bergen	Forsking
2004/1490	Universitetet i Bergen	Bergen	Forsking
2004/1489	Universitetet i Bergen	Bergen	Forsking
2004/1488	Universitetet i Bergen	Bergen	Forsking
2004/1487	Universitetet i Bergen	Bergen	Forsking
2004/1484	Universitet i Bergen	Bergen	Forsking
2004/0763	Universitetet i Bergen	Bergen	Forsking
2004/0665	Haraldsplass Diakonale Sjukehus AS	Bergen	Forsking
2004/0528	Helse Bergen HF	Bergen	Forsking
2004/0345	Helse Bergen, Haukeland (barneleukemi)	Bergen	Forsking
2004/0344	Helse Bergen, Haukeland (prosjekt)	Bergen	Forsking
2004/0343	Helse Bergen, Haukeland (kreft)	Bergen	Forsking
2004/0338	Helse Bergen, Haukeland (Ernæring)	Bergen	Forsking
2004/0333	Helse Bergen HF	Bergen	Forsking
2004/0757	Nordlandsforskning	Bodø	Forsking
2004/0760	Helse Finnmark	Hammerfest	Forsking
2004/0337	Akershus Universitetssjukehus HF	Nordbyhagen	Forsking
2004/1183	Radiumhospitalet	Oslo	Forsking
2004/1155	Eli Lilly Norge AS	Oslo	Forsking
2004/1080	Universitetet i Oslo	Oslo	Forsking
2004/0759	Universitetet i Oslo	Oslo	Forsking
2004/0758	Universitetet i Oslo	Oslo	Forsking
2004/0754	Universitetet i Oslo	Oslo	Forsking
2004/0645	Aker universitetssjukehus - Prosjekt II	Oslo	Forsking
2004/0644	Aker universitetssjukehus - Prosjekt I	Oslo	Forsking
2004/0638	Rikshospitalet	Oslo	Forsking
2004/0603	Radiumhospitalet	Oslo	Forsking
2004/0362	Eli Lilly Norge AS	Oslo	Forsking
2004/0361	GlaxoSmithKlein II	Oslo	Forsking
2004/0360	SIRUS IV	Oslo	Forsking
2004/0359	SIRUS III	Oslo	Forsking
2004/0358	SIRUS II	Oslo	Forsking
2004/0357	Eli Lilly Norge AS	Oslo	Forsking
2004/0356	Aker sjukehus - Generell	Oslo	Forsking
2004/0354	Rikshospitalet	Oslo	Forsking
2004/0351	SIRUS	Oslo	Forsking

<i>Saksnr.</i>	<i>Tilsynsobjekt</i>	<i>Poststed</i>	<i>Bransje/sector</i>
2004/0350	Universitetet i Oslo	Oslo	Forsking
2004/0349	Universitetet i Oslo	Oslo	Forsking
2004/0348	Universitetet i Oslo	Oslo	Forsking
2004/0346	Rikshospitalet	Oslo	Forsking
2004/0340	Ullevål Universitetssjuehus HF	Oslo	Forsking
2004/0339	Ullevål Universitetssjuehus HF	Oslo	Forsking
2004/0335	Det norske Radiumhospital HF	Oslo	Forsking
2004/0334	Ullevål Universitetssjuehus HF	Oslo	Forsking
2004/0332	GlaxoSmithKlein	Oslo	Forsking
2004/0331	AstraZeneca	Oslo	Forsking
2004/0330	Novartis	Oslo	Forsking
2004/0329	Genova AS	Oslo	Forsking
2004/0328	Sirus	Oslo	Forsking
2003/1080	Universitetet i Oslo	Oslo	Forsking
2004/0762	Høgskolen i Telemark	Porsgrunn	Forsking
2004/1066	Høgskolen i Savanger	Stavanger	Forsking
2004/0365	Høgskolen i Stavanger	Stavanger	Forsking
2004/0364	Høgskolen i Stavanger	Stavanger	Forsking
2004/0363	Høgskolen i Savanger	Stavanger	Forsking
2004/1034	Universitetet i Tromsø (prosjekt 3)	Tromsø	Forsking
2004/1033	Universitetet i Tromsø (prosjekt 2)	Tromsø	Forsking
2004/0764	Universitetssjuehuset i Nordland	Tromsø	Forsking
2004/0635	Tromsø universitet - generell	Tromsø	Forsking
2004/0367	Universitetet i Tromsø	Tromsø	Forsking
2004/0366	Tromsø universitet (prosjekt 1)	Tromsø	Forsking
2004/0704	SINTEF Unimed prosjekt I	Trondheim	Forsking
2004/0703	SINTEF Unimed prosjekt II	Trondheim	Forsking
2004/0702	SINTEF Unimed prosjekt III	Trondheim	Forsking
2004/0557	NTNU - Prosjekt IV	Trondheim	Forsking
2004/0556	NTNU - Prosjekt III	Trondheim	Forsking
2004/0555	NTNU - Prosjekt II	Trondheim	Forsking
2004/0554	NTNU - Prosjekt I	Trondheim	Forsking
2004/0543	St. Olav - Prosjekt V	Trondheim	Forsking
2004/0541	St. Olav - Prosjekt IV	Trondheim	Forsking
2004/0536	St. Olav - Prosjekt III	Trondheim	Forsking
2004/0535	St. Olav - Prosjekt II	Trondheim	Forsking
2004/0534	St. Olav - prosjekt I	Trondheim	Forsking
2004/0342	St. Olavs Hospital HF	Trondheim	Forsking
2004/0341	NTNU	Trondheim	Forsking
2004/0352	Sjuehuset innlandet HF Tynset	Tynset	Forsking
2004/0353	Kompetansesenteret for Sikkerhets-, fengsels-, og rettspsykiatri	Oslo	Forsking

Vedlegg 2

Personvernemndas årsmelding 2004

1 Samandrag

Dette er Personvernemndas fjerde årsmelding, og representerer det siste året i nemndas første periode.

I løpet av 2004 har det komme ni klagar, av desse er tre ferdigbehandla. Samtidig er tre klagar frå 2003 ferdigbehandla. Nemnda begynner å få eit visst erfaringsgrunnlag. Klagesaker er sjølv sagt konkrete, men fleire av dei har likevel vore prinsipielle.

Av dei i alt seks sakene som blei ferdigbehandla Personvernemnda i 2004, er Datatilsynets vedtak omgjort heilt eller delvis i tre av sakene. Blant klagesakene vil det naturleg nok vere ein forholdsvis stor del der det knyter seg tvil til tolkinga av føresegnene i personvernlovgivinga eller dei vurderingar dei føreset. Personvernemnda søker å ha for auga at dei konkrete vedtaka også skal medverke til ei avklaring av gjeldande rett.

2 Innleiing

Personvernemnda er oppretta med heimel i lov om behandling av personopplysninger av 2000:31. Loven trådte i kraft 1. januar 2001 og Personvernemnda skal behandle klager på vedtak som Datatilsynet fattar etter personopplysningsloven. Personvernemnda skal også behandle klager på vedtak som Datatilsynet fattar etter helseregisterloven (2001:24).

Personvernemnda er eit uavhengig forvaltningsorgan administrativt underlagt Kongen og Moderniseringsdepartementet.

Personvernemndas arbeid blir regulert av personopplysningsloven, forskrifter til denne, samt ein instruks som Moderniseringsdepartementet (tidlegare Arbeids- og administrasjonsdepartementet) har utarbeidd. Forvaltningsloven og offentlegloven kjem også til bruk som forvaltinga elles.

Sjølv om Moderniseringsdepartementet har utarbeidd instruks, inneber dette ikkje noka form for instruksjonsrett i enkeltsaker. Departementet

kan heller ikkje gi generelle instruksar om lovtolkning eller skjønnsutøving.

Personvernemnda skal kvart år orientere Kongen om behandling av klagesakene.

3 Medlemmer

Personvernemnda har sju medlemmer som blir oppnemnde for fire år med høve til oppnemning for ytterlegare fire år. Første gongs oppnemning skjedde i 2001. Personvernemndas leiar og nestleiar blir oppnemnde av Stortinget, mens dei andre medlemmer blir utnemnde av Kongen.

PVN er samansett av desse personane:

- Jon Bing, leiar
- Gro Hillestad Thune, nestleiar
- Per Anders Stalheim
- Dag Elgesem
- Siv Bergit Pedersen
- Sidsel Rogde
- Hanne I Bjurstrøm

I tillegg er det oppnemnt personlege vararepresentantar.

4 Andre organisatoriske forhold

Sekretariatet har i 2004 vore advokat Camilla Sivesind Tokvam, avtalen gjeld fram til august 2005.

Personvernemnda held sine møte i lokale utanfor Datatilsynet og Regjeringskvartalet for å markere sjølvstende.

Personvernemnda har ei eiga heimeside, www.personvernemnda.no, der blant anna vedtaka er publiserte. Heimesida har lenke frå Datatilsynets heimeside, og lenker til personvernrelatert materiale tilgjengeleg på nettet. Jamvel om det totale talet vedtak ikkje er stort, er det oppnådd semje med Lovdata om at vedtaka også skal leggjast inn i ein egen database lenka til det andre dokumenterte materialet. Dermed kan ein brukar lett slå opp på Personvernemndas vedtak ved opp-

slag på paragraf i personopplysningsloven, andre lovar, dommar mv. som vedtaka viser til.

I 2004 har Personvernemnda arbeidd med eit prosjekt for sikker e-post-utveksling mellom medlemmene og sekretariatet. Prosjektet var venta ferdig i 2004, men har mått utsetjast etter at leverandøren som var vald (Posten) terminerte den tenesta som ein hadde planar om å nytte.

5 Møte og seminar i 2004

Personvernemnda har i 2004 hatt i alt ni møte. Møta blei i hovudsak nytta til å behandle klagesaker, men også administrative forhold som arbeidsform og saksbehandling, pluss vurdering av budsjett og budsjettforslag for 2005, er blitt behandla i møta. I tillegg til nemdsmøte har det vore førebunde møte med sekretariatet og ein eller fleire medlemmer, samt enkelte tilsvarande møte i samband med behandling av klagesaker.

Personvernemnda har hatt to møte med Moderniseringsdepartementet.

Nestleiar Gro Hillestad Thune, medlem Hanne I. Bjurstrøm og sekretæren Camilla S. Tokvam deltok på den internasjonale konferansen for datatilsynsmyndigheiter i Wroclaw - Polen, 14. – 17. september 2004.

Personvernemnda ytte økonomisk støtte til "Personvernkonferansen 2004", som blei arrangert av Avdeling for forvaltningsinformatikk, Universitetet i Oslo. Om budsjettsituasjonen tillet det, tek Personvernemnda sikte på å medverke til at det kvart år kan haldast ein slik fagleg konferanse for diskusjon av aktuelle personvernspørsmål. Utover det økonomiske bidraget og ei generell utsegn om kva hovudemne som interesserer Personvernemnda, har nemnda ikkje noko med sjølve arrangementet å gjøre. Det blir lagt vekt på at dette skal vere eit ope, fagleg forum. Personvernemndas medlemmer deltek på konferansen, men det er semje om at ein skal vere tilbakehalden med der å gi uttrykk for haldningar til faglege spørsmål i tråd med Personvernemndas ønske om å reindyrke rolla som klageorgan.

Konferansen tok sikte på å kaste lys over personvern og forskning, inkludert diskusjon av sentrale rettsreglar som styrer korleis forskaren bruker personopplysningar.

6 Klagesaksbehandling

Personvernemnda mottok i 2004 totalt ni klagesaker. Tre av disse var ferdigbehandla ved utgangen av året. Oversikt over vedtak, og sjølve vedtaka er lagde ut på Personvernemndas heimesider, i tillegg til at vedtaka blir sende elektronisk over til Datatilsynet som publiserer desse på sine eigne heimesider.

Talet på saker i 2004 har auka med ei sak i forhold til 2003. Erfaringane frå Justisdepartementet som var klageorgan under den tidlegare personregisterloven kan tyde på eit årleg tal på ca 10 - 12 saker. Ved inngangen til 2005 fekk Personvernemnda oversendt åtte nye saker, det er derfor grunn til å gå ut frå at det vil skje ein auke relativt sett i dette året, minst opp til det nivået som Justisdepartementet sine erfaringar tilseier.

Saker som er behandla i 2004 er:

Klage på Datatilsynets vedtak om vilkår om samtykke for konsesjon for delstudie 1 og 2 - Statens Arbeidsmiljøinstitutt - STAMI

Sak nr. 2004-01 STAMI: Saka gjeld ein klage frå Statens Arbeidsmiljøinstitutt (STAMI) i samband med ein oppfølgingsstudie om kreft og lungesjukdommar blant tilsette i norsk silisiumkarbidindustri. Hovudspørsmålet er om det skal vere krav om informert samtykke for å tillate oppfølgingsstudien, eller om denne kan baserast på ei av grunngevingane for at tiltaket er nødvendig, jf. personopplysningsloven § 11 jf. §§ 8 og 9. Med utgangspunkt i personopplysningsloven § 11, peiker Personvernemnda på at for sensitive opplysningar må både vilkåra i § 8 og i § 9 i personopplysningsloven vere oppfylte. Av dei tre alternative grunngevingane i personopplysningsloven § 8 sluttar Personvernemnda seg til Datatilsynets tolking av loven, som gir samtykke prioritet. Men Personvernemnda tolkar loven slik at dersom det ligg føre tilstrekkelig grunngeving for å avvike frå hovudregelen, kan dette gjerast. Ei slik grunngeving finn Personvernemnda i den konkrete saka i omsynet til kvaliteten på undersøkinga. Når personopplysningsloven § 8 er tilfredsstilt, må ein så avgjere om også vilkåra etter personopplysningsloven § 9 er til stades. Personvernemnda gjer ei konkret vurdering av saka, og finn at i dette tilfellet vil samfunnets interesse av at behandlinga skjer, klart overstige ulempene denne kan medføre for kvar enkelt, jf. 9, 1.ledd litra h. Etter dette blir klagen å ta til følge.

Klage på Datatilsynets vedtak om vilkår om samtykke til at ein framleis kan lagre opplysningar frå prosjektet "Helse- og stressreaksjoner hos oljearbeidere i Nordsjøen" - NTNU

Sak nr. 2004-02 NTNU: Etter Alexander Kielland-ulykka i 1980 blei det i 1984-85 gjennomført ei undersøking blant dei overlevande basert på munnleg samtykke frå dei overlevande og skriftleg samtykke frå ei kontrollgruppe. Det er fleire gonger søkt om konsesjon for vidare lagring med sikte på ei oppfølgingsundersøking, den siste konsesjonen (gitt etter personregisterloven) gjekk ut i 2002. Ny søknad blei lagd fram i januar 2004. Datatilsynet gav delvis avslag, og kravde at det blei henta inn skriftleg samtykke frå dei registrerte innan 1. juni 2004. Klagaren ønskte først å innhente samtykke i samband med igangsetjing av oppfølgingsstudien, og lagring for eit lengre tidsrom. Personvernemnda gav løyve til at lagringa heldt fram til det låg føre eit vedtak i nemnda. Klagen blei teken til følgje. Personvernemnda tillet lagring inntil seks månader frå datoen for vedtaket. Før oppfølgingsprosjektet blir sett i gang, må tilfredsstillande samtykke innhenta. Personvernemnda fann at føresegna om tvingande grunn i personopplysningsloven § 8 litra d her kunne nyttast, og at samfunnet sine interesser var klart større enn ulempe for kvar enkelt i dette tilfellet, jf. personopplysningsloven § 9 litra h. Saka blei send tilbake til Datatilsynet, som har kompetanse etter personopplysningsloven § 33 til å gi konsesjon.

Klage på Datatilsynets vedtak om at Postens utleige av adresselister ikkje kan forankrast i personopplysningsloven § 8 litra f – Posten Norge AS

Sak nr 2004-03 Posten. Posten har eit register over dei fleste privatpersonar som bur i Noreg (PMS). Posten ønskjer å leige ut adresselister frå dette registeret. Det blei foreslått tiltak, særleg eit eige reservasjonsregister, for å dempe ulempe for personvernet til den registrerte. Personvernemnda fann at teiepliktføresegna i postloven § 13 ikkje var til hinder for slik gjenbruk. Nemnda fann likevel at gjenbruk ikkje hadde heimel i personopplysningsloven § 11, 1.ledd litra c fordi formålet ved utleige av adresselistene var uforlikeleg med registrering av opplysningane for formidling av postsendingar. Slik gjenbruk kravde derfor samtykke. Personvernemnda tolka personopplysningsloven slik at det i ein slik situasjon ikkje skal leggjast strengare krav til gjenbruk enn til første gongs bruk, og vurderte derfor om bruken kunne heimlast i personopplysningsloven § 8 litra f. Personvernemnda kom til at den forretningsmessige inter-

essa til Posten var rettkomen etter denne føresegna, men fann ved å vise til forarbeida at denne forretningsmessige interessa ikkje kunne vege tyngre enn den registrerte si interesse i privatlivets fred og personvern.

Klage på Datatilsynets vedtak om å nekte konsesjon for å gjere ferdig forskingsprosjektet "Suicidal atferd i Bergensområdet"

Sak nr 2004-04. Klagaren har på grunnlag av ein konsesjon frå 1983 følgt ei gruppe på 470 personar som alle var innlagde for sjølvpåførte skadar. Ved ein ny konsesjon frå 1997 blei det gitt samtykke til kopling til Dødsårsaksregistret. Datatilsynet fann at det samtykke som i si tid blei innhenta, ikkje oppfylte krav til informert samtykke i personopplysningsloven § 2 nr 7. Klager fremja søknad om ny konsesjon etter at overgangsordninga i personopplysningsloven hadde gått ut. På denne bakgrunnen behandla ikkje Datatilsynet søknaden, men uttalte seg likevel om realiteten. Personvernemnda valde å behandle klagen som søknad om ny konsesjon, og fann at prosjektet kan byggje på føresegna om tvingande grunn i personopplysningsloven § 8 litra d, og at vilkåra i personopplysningsloven § 9, 1.ledd litra h var tilfredsstillt. Etter dette blei klagen teken til følgje. Fråsegn om at opplysningar om avdøde personar fell utanfor loven sitt område. (Ferdigbehandla i 2005)

Klage på Datatilsynets vedtak om konsesjon for behandling av personopplysningar i kredittopplysningsverksemd - Norske Kredittopplysningsbyråers Forening (NKF)

Sak nr. 2004-05 NKF. Klage på konsesjon frå Norske Kredittopplysningsbyråers Forening (NKF). Klagen knytte seg til fleire punkt i konsesjonen.

Personvernemnda drøftar spørsmålet om kva tidspunkt som skal leggjast til grunn for registrering av inkassoopplysningar. Her deler nemnda seg i eit fleirtal og et mindretal. Fleirtalet meiner at ein først kan tillate at ei fordring blir registrert når det er teke rettslege steg for å drive inn fordringa, og sluttar seg slik til det synet som ligg til grunn for Datatilsynets vedtak.

Når det gjeld slettefrist for fordringar som er gjorde opp, meiner Personvernemnda at dei skal slettast straks dei er gjorde opp, og sluttar seg også her til Datatilsynets vedtak.

Når det gjeld behandling av personopplysningar ved berekning av nyetablerte føretak i tida fram til første rekneskap er offentleg tilgjengeleg, gir Personvernemnda klagaren medhald i at ein skal kunne basere seg på opplysningar om dei nøk-

kelpersonar som står bak føretaket, når ein rangerer kor kredittverdig føretaket er.

Når det gjeld frist for sletting av opplysningar om misleghaldne fordringar når foreldinga blir avbrote ved at det blir teke rettsleg skritt, får klagaren medhald på eitt punkt, nemlig at det ikkje blir innført noka beløpsgrense. Dermed blir det lov å registrere fordringar som ikkje kan resultere i tvangsforretningar for nye fire år når det blir teke nye rettslege steg innanfor den første fireårsfristen. (Ferdigbehandla i 2005)

Klage på Datatilsynets vedtak om at Ullevål Universitetssjukehus ved personvernombodet ikkje sjølv får oppbevare koplingsnøklar for forskingsprosjekt

Sak nr. 2004-06 UUS. Ullevål Universitetssjukehus (UUS) klagar på eit vilkår i konsesjon for "Etterundersøkelse av pasienter innlagt for selvpåført forgiftning". Datatilsynet stilte som vilkår at et koplingsregister for pseudonym for dei registrerte blei oppbevart eksternt. UUS meinte koplingsregisteret kunne oppbevarast av personvernombodet ved sjukehuset. Personvernemnda slutta seg til Datatilsynets vurdering om at eit slikt register bør oppbevarast eksternt, bl.a. fordi personvernombodet i prinsippet kan instruerast av leiinga ved UUS. Det blei også gitt ein generell tilslutnad til Datatilsynets syn om at slike oppgaver ikkje burde leggjast til eit personvernombod. (Ferdigbehandla i 2005)

Klage på Datatilsynets vedtak om at Telenor Mobil må slette personopplysningar om tidlegare kundar

Sak nr 2004-07 Telenor Mobil. Telenor Mobil ønskte å lagre enkelte opplysningar (namn, adresse, fødselsdato, tidlegare telefonnummer og nytta teneste) om kundar med avslutta kundeforhold også etter at kundeforholdet var avslutta. Ut frå erfaring vil ein del av desse seinare ønskje å gjenopprette kundeforholdet, og Telenor Mobil ville bruke opplysningane som bakgrunn for å hjelpe kunden. Opplysningane blei ikkje brukte til andre formål. Personvernemnda meinte at det var nærliggjande at kundar qua forbrukarar føresette at den tidlegare leverandøren "hugsa" telefonnummer, kva slags type abonnement ein hadde hatt mv. Nemnda fann at lagringa av opplysningane i liten grad svekkjer personvernet til den registrerte, og at Telenor Mobil hadde ei rettkomen interesse i lagringa, jf. personopplysningsloven § 8 litra f. Klagen blei teken til følgje. (Ferdigbehandla i 2005)

Klage på Datatilsynets vedtak om at Bakehuset Kafé AS ikkje får oppretthalde fjernsynsovervaking av butikklokala i noverande omfang

Sak nr 2004-09 Bakehuset. Ein kafé overvakte arbeidsplassen ved hjelp av videokamera. Etter diskusjon mellom Datatilsynet og kafeen var det semje om bruk av slike kamera. I ettertid blei det montert ytterlegare to kamera. Det var semje om at ei viss overvaking kan tillatast etter føresegna om tvingande grunn i personopplysningsloven § 8 litra b jf. personopplysningsloven § 37, 1.ledd. Personvernemnda slutta seg til Datatilsynet i at det må finnast ei grense for kor intensiv overvaking som kan tillatast på ein arbeidsplass, og opprettheldt vedtaket som gjekk ut på at dei to siste kame-raa måtte fjernast. (Ferdigbehandla i 2005)

Vedtaka er lagde ut på Personvernemndas heimeside, <http://www.personvernemnda.no>. Inntrykket av klagesakene er at endå om dei alle er konkrete, kan ein likevel peke på eitt hovudtrekk:

Spørsmål kring forskning og personvern er vanskelige. To av sakene dreier seg om medisinske forskingsprosjekt og forholdet til samtykke. Personvernemnda har lagt vekt på den samfunnsinteresse som forskingsprosjekt representerer. Det er også uttalt kva omsyn som må vere til stades for at ein kan avvike frå å bruke samtykke som behandlingsgrunn, bl.a. omsynet til kvaliteten av opplysningane som er henta inn.

Personvernemnda har gitt uttrykk for bekymring i forhold til saksbehandlingstida. Eit kollektivt organ vil vere avhengig av felles diskusjonar for å komme fram til avgjerder, og det vil av og til bli nødvendig å diskutere formuleringa av avgjerda i fleire møte. Det er også nødvendig å la klagaren få lov til å uttale seg etter at klagen er motteken. At ikkje fleire saker av dei som er mottekne i 2004 blei ferdigbehandla innan året gjekk ut, har si hovudforklaring i at dei blei mottekne på hausten, og derfor ikkje kunne førebuast til vedtak før året var omme. Personvernemnda har ikkje motteke fråsegner som kan tolkast dit at ein meiner saksbehandlingstida er for lang, men nemnda sjølv har forholdet under oppsikt og vil søkje å treffe tiltak for at det ikkje skjer noka opphopping av saker.

7 Rekneskap og budsjett for 2004

Personvernemnda hadde i 2004 ei budsjettramme på kr 1.198.796, som kjem fram under kap 1500 Arbeids- og administrasjonsdepartementet i statsbudsjett for 2004.

Totalt forbruk: kr 1.037.131. Personvernemnda disponerte løyvinga til innkjøp av nødvendig litteratur, utstyr, tenester, drift og oppdatering av heimesider, gjennomføring av seminar, deltaking på konferanse for tilsynsmyndigheiter, arbeidsgodtgjersle og reisegodtgjersle til medlem-

mene i nemnda, godtgjersle til sekretariat og leige av møtelokale.

Oslo 4. april 2005
For Personvernemnda
Jon Bing (leiar)

Offentlege etatar kan tinge fleire eksemplar frå:
Statens forvaltningsteneste
Informasjonsforvaltning
E-post: publikasjonsbestilling@ft.dep.no
Telefaks: 22 24 27 86

Andre kan tinge frå:
Akademika AS
Avdeling for offentlege publikasjonar
Postboks 8134 Dep
0033 OSLO
Telefon: 22 11 67 70
Telefaks: 22 42 05 51
Grønt nummer: 800 80 960

Publikasjonen finst på Internett:
<http://odin.dep.no/>

Omslagsillustrasjon: Sissel Mørtvedt

Trykk: Lobo Media AS - 06/2005

