Manus til

Datatilsynets årsmelding

2004

Oversendt Moderniseringsdepartementet

11. februar 2005

Datatilsynet

Innholdsfortegnelse

1 DATATILSYNET 25 ÅR I 2005

Datatilsynet ble etablert 1. januar 1980 i samsvar med den daværende personregisterloven vedtatt i 1978. Datatilsynet markerer derfor sitt 25-årsjubileum i 2005.

Datatilsynet har til oppgave å beskytte den enkelte mot at personverninteressene krenkes gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvernhensyn som behovet for vern av personlig integritet og privatlivets fred. Det juridiske grunnlaget for Datatilsynets virksomhet er regulert i Lov om behandling av personopplysninger av 14. april 2000 (personopplysningsloven) og Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) av 18. mai 2001.

Datatilsynet er et uavhengig forvaltningsorgan, administrativt underordnet Kongen ved Moderniseringsdepartementet. Datatilsynets uavhengighet innebærer at departementet ikke kan gi instruks om, eller omgjøre Datatilsynets utøving av myndighet etter personopplysnings- eller helseregisterloven. Som klageinstans i forhold til Datatilsynets vedtak er det opprettet en Personvernnemnd. Nemnda utgir sin egen årsmelding.

Datatilsynets oppgaver
Datatilsynet skal holde seg orientert og informere om den nasjonale og internasjonale utviklingen i behandlingen av personopplysninger, og om de problemene som knytter seg til slik behandling. Datatilsynet skal identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses. Deltakelse i råd og utvalg er derfor en viktig del av Datatilsynets arbeid. Også som høringsinstans i saker som kan ha en personvernmessig konsekvens har Datatilsynet innflytelse på samfunnsutviklingen.

Datatilsynet fører en offentlig fortegnelse over alle behandlinger av personopplysninger som er meldt inn. Videre behandler Datatilsynet søknader om konsesjon, der dette kreves etter loven.

Gjennom aktivt tilsyn og saksbehandling kontrollerer Datatilsynet at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet. Datatilsynet bistår bransjeorganisasjoner med å utarbeide bransjevise adferdsnormer, og gir bransjer og enkeltvirksomheter råd om sikring av personopplysninger. Datatilsynet motiverer også til, og støtter virksomheter som på frivillig basis har oppnevnt et eget personvernombud.

Sist, men ikke minst, har Datatilsynet også en viktig ombudsrolle. I den forbindelse drives rådgivning og informasjon overfor enkeltpersoner som tar kontakt med tilsynet. Publikum generelt nås i første rekke gjennom aktiv mediekontakt og publisering på eget nettsted. For å skape oppmerksomhet og interesse omkring personvernspørsmål deltar Datatilsynet aktivt i den offentlige debatt og legger stor vekt på å praktisere meroffentlighet.

2 ORGANISASJON OG ADMINISTRASJON

Budsjett
Datatilsynets budsjettramme for 2004 ble økt i forhold til året før. Datatilsynet styrket som følge av dette innsatsen på de områder som var forutsatt for budsjettøkningen. Det vil si gjennomføring av tilsyn/kontroller innen prioriterte satsingsområder, reduksjon av saksbehandlingstiden, etablering av en Frontserviceenhet, samt forberedende arbeid til en større personvernundersøkelse.

Datatilsynets økonomiske ramme for 2004 var på i overkant av 21 millioner kroner. De rene lønnskostnadene utgjør ca 70 prosent av driftsbudsjettet. Ut over dette har bevilgningen dekket faste driftsutgifter og utgifter til operativ tilsynsvirksomhet, informasjonsarbeid og representasjon i internasjonale organer. I 2004 har det også vært ekstra kostnader forbundet med arkivavlevering og etablering av ny hjemmeside på Internett.

Organisasjon
Datatilsynet ledes av direktør Georg Apenes og er organisert i fire avdelinger, juridisk, tilsyn og sikkerhet, informasjon og administrasjon. Juridisk avdeling utgjør med sine 15 medarbeidere den største organisatoriske enheten.

Det var i virksomhetsåret 27 fast tilsatte, hvorav 17 kvinner og 10 menn. Gjennomsnittsalderen er 44 år for menn og 36 år for kvinner.

Det har vært tilsatt ekstrahjelp og vikarer for å avhjelpe arbeidssituasjonen. To engasjementsstillinger er videreført i juridisk avdeling i forbindelse med at det er etablert en førstelinjetjeneste (Frontservice). Denne består av tre juridiske saksbehandlere som besvarer innkomne telefoner og e-post, i tillegg til å bistå i saksbehandlingen. Det er videre blitt opprettet en ny stilling i tilsyns- og sikkerhetsavdelingen. Denne har som hovedoppgave å styrke tilsynsarbeidet og bistå med IT-driftsoppgaver. Det er også blitt opprettet en ny rådgiverstilling i informasjonsavdelingen.

I løpet av året har én medarbeider sluttet i Datatilsynet. Flere engasjementer og vikariater har imidlertid gått til opphør og fast tilsatte er tilbake i arbeid etter svangerskapspermisjoner.

Avtale om inkluderende arbeidsliv
Datatilsynet ble med virkning fra september 2003 knyttet til avtalen om et inkluderende arbeidsliv. Avtalen tydeliggjør samarbeidet mellom arbeidsgiver og arbeidstaker med det mål å skape et mer inkluderende og utviklende arbeidsmiljø. Datatilsynet så behov for bistand til HMS-arbeidet for å legge forholdene best mulig til rette for sunn, trygg og effektiv drift. Datatilsynet inngikk derfor i 2004 avtale med Norsk Bedriftshelsetjeneste AS og har hatt tilbud til de ansatte om en arbeidshelseundersøkelse. Det utarbeides en oppsummeringsrapport etter at arbeidshelseundersøkelsene er utført. Denne vil kunne gi innspill til prioritering av aktiviteter for 2005.

Grønn stat
Alle statlige etater og virksomheter skal innen 2005 innføre miljøledelse som en integrert del av organisasjonens styringssystemer. Datatilsynet sluttførte dette arbeidet i 2004.

Resultatindikatorer
Det er i 2004 etablert rutiner for rapportering på relevante resultatindikatorer for Datatilsynet. Disse gjøres gjeldende ved rapportering til departement og Storting i 2005.

Arkiv
Etter en tilbudsinnbydelse inngikk Datatilsynet en avtale med Stiftelsen ASTA om ordning av arkivmateriale fra perioden 1979-2000. Kassasjonsplan er utarbeidet og godkjent av Riksarkivet. Materialet som er ordnet utgjør i alt ca 160 hyllemeter. I tillegg kommer ca 25 hyllemeter med kopibøker som Datatilsynet har bundet inn selv. Arbeidet ble avsluttet i november 2004.

Revisjon av økonomiregelverket
Nytt reglement for økonomistyring i staten med tilhørende bestemmelser trådte i kraft fra 1. januar 2004. Datatilsynet har i den anledning oppdatert økonomiinstrukser og tilhørende retningslinjer.

3 SAKSBEHANDLING

Ordinær saksbehandling
Det ble i meldingsåret journalført 7 725 dokumenter, hvorav 4 129 innkomne og 3 596 utgående brev fra Datatilsynet. Dette er en liten økning fra foregående år. Helserelaterte saker utgjør den største andelen, med sine til sammen 1 552 dokumenter.

150 av sakene omhandlet problemstillinger av hovedsakelig teknisk karakter. Dette kommer i tillegg til at tekniske problemstillinger også blir berørt ved behandling av konsesjonssøknader og ved gjennomføring av tilsyn.

Konsesjonssaker
Plikten til å søke konsesjon gjelder i all hovedsak ved behandling av sensitive personopplysninger, blant annet opplysninger om helse, rase, tro, politisk tilhørighet, straffbare handlinger og seksuelle forhold. Datatilsynet kan imidlertid bestemme at også andre behandlinger av personopplysninger skal være konsesjonspliktige. Det forutsetter at behandlingen åpenbart vil krenke tungtveiende personverninteresser. Ved vurderingen skal Datatilsynet ta hensyn til personopplysningenes art, mengde og formålet med behandlingen.

Det ble i 2004 gitt 817 konsesjoner, mot 470 året før. Økningen skyldes at det er gitt likelydende konsesjoner til blant andre banker (195) og pensjonskasser (94). Det ble gitt konsesjon til 280 forskningsprosjekter.

Meldinger
Meldeplikten innebærer at den som ønsker å sette i gang behandling av personopplysninger skal orientere Datatilsynet senest 30 dager før behandlingen tar til. Det er imidlertid en del unntak fra meldeplikten.

I 2004 kom det inn 2 777 meldinger om behandling av personopplysninger som ikke er konsesjonspliktig. Totalt er det nå 14 394 aktivt gjeldende meldinger i meldingsdatabasen. Ca fire tusen meldinger ble slettet fra databasen i 2004, fordi de er "gått ut på dato".

Klagesaker
I meldingsåret oversendte Datatilsynet ni saker til Personvernnemnda for videre klagesaksbehandling:

Statens arbeidsmiljøinstitutt
Klage på konsesjonsvedtak. Saken gjaldt en oppfølgingsstudie om kreft og lungesykdommer blant ansatte i norsk silisiumkarbidindustri. Hovedspørsmålet var hvorvidt det skulle kreves informert samtykke for å tillate oppfølgingsstudien, eller om denne kunne baseres på et av de andre grunnlagene som personopplysningsloven gir for å kunne behandle personopplysninger.

Personvernnemnda omgjorde Datatilsynets vedtak, slik at oppfølgingsstudien kan gjennomføres uten informert samtykke.

Norges teknisk naturvitenskapelige universitet (NTNU)
Klage fra NTNU om krav om samtykke for fortsatt lagring av opplysninger fra prosjektet "Helse- og stressreaksjoner hos oljearbeidere i Nordsjøen". Saken gjaldt hvorvidt forsker måtte ha samtykke for fortsatt lagring av opplysninger (opplysningene skulle ha vært slettet i 2002), eller om det var tilstrekkelig at slikt samtykke innhentes når oppfølgingsstudien igangsettes.

Klager fikk medhold i Personvernnemnda. Forskeren fikk dermed tillatelse til å oppbevare personopplysningene inntil oppfølgingsstudien igangsettes, men maksimalt inntil seks måneder.

Posten Norge AS
Saken gjaldt hvorvidt Postens utleie av adresselister kunne forankres i Personopplysningsloven § 8 f. Datatilsynet sa nei. Klager fikk ikke medhold i Personvernnemnda. Saken er for øvrig omtalt annet sted i årsmeldingen.

NKS Olavviken Behandlingssenter
Saken gjelder Datatilsynets avslag på å gi konsesjon til prosjektet "Suicidal adferd i Bergensområdet". Datatilsynet avslo søknaden da dette omfattet opplysninger fra et prosjekt som skulle vært anonymisert i henhold til konsesjonsvilkår fastsatt i den opprinnelige konsesjonen. Saken var i meldingsåret ikke behandlet i Personvernnemnda.

Norske Kredittopplysningsbyråers forening
Klage på konsesjonsvilkår. Klagesaken er omfattende, men gjelder i korte trekk tidspunkt for registrering av betalingsanmerkninger om enkeltpersoner, slettefrist for fordringer som er gjort opp og behandling av personopplysninger ved beregning av såkalt "rating" for

nyetablerte foretak. Saken var i meldingsåret ikke behandlet i Personvernnemnda.

Ullevål Universitetssykehus
Saken gjelder hvem som kan sitte med koblingsnøkkelen til identifikasjon av prosjektdata. Saken var i meldingsåret ikke behandlet i Personvernnemnda.

Telenor
Saken gjelder Datatilsynets pålegg til Telenor om å slette tidligere kunder. Saken var i meldingsåret ikke behandlet i Personvernnemnda.

Finansnæringens Hovedorganisasjon-FNH
Gjelder Datatilsynets vedtak om at helseopplysninger bare kan behandles av forsikringsselskapene etter skriftlig samtykke. Saken var i meldingsåret ikke behandlet i Personvernnemnda.

Bakehuset Kafe AS
Gjelder kameraovervåking på arbeidsplass. Saken var i meldingsåret ikke behandlet i Personvernnemnda.

I tillegg behandlet Personvernnemnda to saker som var sendt inn i 2003. Dette gjaldt:

Gjensidige Nor Sparebank ASA
Saken gjaldt spørsmålet om det i Datatilsynets konsesjon til klager skal kunne stilles vilkår om at det ikke uten kundens samtykke skal tillates at et konsernkunderegister inneholder opplysninger om hvilke type tjenester og produkter kunden har avtale om hos de ulike selskapene i konsernet. Datatilsynet mente dette bare kunne skje etter samtykke.

Personvernnemnda omgjorde Datatilsynets avgjørelse og ga klager medhold i at dette kan skje uten samtykke.

Nasjonalt Folkehelseinstitutt
Klagen gjaldt nektelse av konsesjon for regelmessig overføring av data fra Utlendingsdirektorat til Tuberkuloseregisteret. Klagen ble ikke tatt til følge.

Klager over enkeltvedtak
Tidligere skulle Personvernnemnda bare behandle enkeltvedtak som Datatilsynet fatter med hjemmel i personopplysningsloven. Andre enkeltvedtak skulle behandles av Moderniseringsdepartementet. I en uttalelse på slutten av meldingsåret har imidlertid Justisdepartementets lovavdeling kommet til at Personvernnemnda er rette instans til å behandle klager over alle Datatilsynets avgjørelser, unntatt rent administrative avgjørelser, som for eksempel tilsynets egne tilsettingssaker. For tiden har Personvernnemnda ett avvisningsvedtak til behandling.

Lov- og forskriftsarbeide
I 2004 utarbeidet Datatilsynet forslag til endringer i personopplysningsforskriften. Forslaget går ut på å gjøre lettelser i konsesjonsplikten for forskningsprosjekter som blir tilrådd av en etisk komite. Forslaget er sendt på høring.

Høringssaker

I 2004 kom det inn totalt 124 høringssaker. Datatilsynet ga sitt tilsvar i 104 av sakene. I de øvrige 20 hadde Datatilsynet ikke merknader, da disse ikke reiste personvernspørsmål av betydning. Av høringssaker hvor det ble gitt viktige innspill kan nevnes:

- ny handlingsplan for elektronisk samarbeid i helse- og sosialsektoren,
- forslag til nye regler for rapportering og undersøkelser av ulykker og hendelser 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 enslige mindreårige asylsøkere og flyktninger,
- utkast til ny lov om utdanningsstøtte,
- utkast til lov om supplerende stønad for personar med kort butid i Norge,
- regler om borettsregister,
- forslag fra arbeidsgruppe om endringer i sikkerhetsloven og forskrift om personellsikkerhet,
- NOU 2004:5 Arbeidslivslovutvalget,
- etablering av et personentydig helseregister,
- NOU 2004:6 Mellom effektivitet og personvern,
- forslag om å innføre rapporteringsplikt for revisorer,
- lovhjemling og etikkomiteer og nasjonalt utvalg for uredelighet i forskning,
- persondatautveksling i Norge,
- forprosjektrapport om arkitektur for elektronisk samhandling i offentlig sektor,
- en ny arbeids- og velferdsforvaltning – om samordning av Aetats, trygdeetatens og sosialtjenestens oppgaver,
- IKT-strategi for kriminalomsorgen 2005 – 2008,
- "Fra bruk til gjenbruk",
- forslag om utprøving av dommerledet narkotikaprogram i Norge,
- forslag om endringer i barnevernloven, sosialtjenesteloven og smittevernloven,
- blodforskriften
- utredning nr. 12 fra banklovkommisjonen

4 DELTAKELSE I OFFENTLIGE RÅD OG UTVALG

Datatilsynet forsøker, så langt en begrenset kapasitet rekker, å delta forskjellige i råd og utvalg, for å sikre at personverninteressene blir ivaretatt tidlig i planleggingsprosessen. Tilsynet var i meldingsåret representert i følgende råd og utvalg:

Utvalg for politimetoder i forebyggende øyemed
Politimetodeutvalgets rapport *Mellom effektivitet og personvern* (NOU 2004:6) ble lagt frem våren 2004. Se nærmere omtale senere i årsmeldingen.

DNA-utvalg
Datatilsynets direktør er oppnevnt i et utvalg som skal vurdere om adgangen til å ta DNA-prøver skal utvides, for eksempel slik at adgangen blir den samme som for fingeravtrykk. I tillegg skal utvalget vurdere om det skal åpnes for å registrere DNA-profiler i flere typer av saker og om siktelse skal være et tilstrekkelig vilkår for å registrere vedkommendes DNA-profil. Utvalget skal også vurdere eventuelle endringer i saksbehandlingsreglene for registrering og søk i DNA-registeret. Utvalget skal sluttføre sitt arbeid innen utgangen av 2005.

Vurdering av uredelighetsutvalg for forskning
Datatilsynet er representert i en arbeidsgruppe nedsatt av Undervisnings- og Forskningsdepartementet. Arbeidsgruppa skal jobbe med en mulig lovfesting av et uredelighetsutvalg for forskning, samt de forskningsetiske komiteer.

Sertifiseringsordning for informasjonssikkerhet
Nasjonal sikkerhetsmyndighet er ansvarlig for sertifiseringsordningen for informasjonssikkerhet for IT-utstyr og systemer (SERTIT). Datatilsynet deltar i styringsgruppen for dette arbeidet. Formålet med deltakelsen er å fremme sertifiseringsordningen, slik at den kan få praktisk anvendelse for de som er underlagt sikkerhetsbestemmelsene i personopplysningsloven. Det har vært to møter i 2004.

Samarbeidsråd for helsesektoren
Rådet er opprettet av Sosial- og Helsedirektoratet med sikte på å koordinere arbeid med informasjonsteknologi i helsesektoren. Gruppens arbeid tar utgangspunkt i direktoratets strategiplan "E-2007" som omhandler strategi og planer for å fremme bruk av informasjonsteknologi. Formål med samarbeidsrådet er å styrke samarbeidet aktørene i mellom og med de sentrale myndigheter. Datatilsynet deltar som observatør og oppfatter deltakelse i rådet som et viktig ledd i å kommunisere tilsynets standpunkter. Datatilsynet deltok på tre av rådets fire møter.

Bransjenorm for helsesektoren
Sosial- og Helsedirektoratet var initiativtaker til et større prosjekt hvor formålet er å utvikle en felles bransjenorm for helsesektoren. Normen skal bidra til å harmonisere nivået på informasjonssikkerhet. De kontroller som Datatilsynet har gjennomført innen sektoren har avdekket et stort behov for et slikt felles løft. Ikke minst gjelder dette de ulike aktørenes tilknytning til det nasjonale helsenettet. Datatilsynet har derfor deltatt i styringsgruppen for arbeidet med bransjenormen, og har bistått med råd og veiledning.

Koordineringsutvalget for informasjonssikkerhet - KIS
Utvalget består av representanter for sju departementer, Statsministerens kontor og ni direktorater. Opprettelsen av koordineringsutvalget er ledd i gjennomføringen av en nasjonal strategi for informasjonssikkerhet. Arbeidet omfatter alminnelig IT-sikkerhet og spørsmål knyttet til rikets sikkerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner. Utvalget skal samordne videreutviklingen av IT-sikkerhetsregelverket, få frem felles standarder, normer, metoder og verktøy for IT-sikkerhet. Utvalget skal også drøfte aktuelle risiko- og sårbarhetsspørsmål og bidra til koordinering av informasjonstiltak og beredskapsplanlegging. Koordineringsutvalget hadde fire møter i 2004.

Referansegruppe for kravspesifikasjon for digitale signaturer
Datatilsynet deltok som observatør i en referansegruppe opprettet av Moderniserings-departementet i forbindelse med utvikling av ny kravspesifikasjon for digitale signaturer i det offentlige. Formålet med deltakelse har vært å fremme tilsynets standpunkter i forhold til dette prosjektet. Datatilsynet utgangspunkt har hele tiden vært at kravspesifikasjonen burde forutsette kvalifiserte digitale signaturer. Innstillingen fra prosjektet har blitt en tonivåmodell for digitale signaturer, hvilket ikke er i samsvar med Datatilsynets tilråding. Datatilsynets tilrådning var for øvrig i samsvar med en rekke andre aktørers standpunkt i referansegruppen.

Internett og misbruk
En internettgruppe er etablert av Post- og teletilsynet som et frivillig åpent forum, hovedsakelig bestående av Internett-aksesstilbydere og andre som direkte håndterer internettrelaterte oppgaver. I 2004 har Datatilsynet særlig tatt opp private hjemmesiders forhold til personopplysningsloven.

Datatilsynet har i tillegg deltatt i en undergruppe som konsentrerer seg om misbruksrelaterte spørsmål knyttet til Internett. Datatilsynet har deltatt som observatør i de to møtene som gruppen har hatt i meldingsåret.

5 INTERNASJONALT SAMARBEID

Personopplysninger utveksles i stadig større grad over landegrensene. For Datatilsynet er det derfor viktig å samarbeide med tilsvarende organer i andre land. Internasjonale samarbeidsfora er dessuten viktige arenaer for erfaringsutveksling. Som det går fram av oversikten nedenfor deltar Datatilsynet i mange ulike sammenhenger. Imidlertid er Norge dessverre ikke trukket inn i det personvernarbeidet som foregår innen rammen av Europarådets organer.

Artikkel 29-gruppen
Artikkel 29-gruppen har som oppgave å drive frem koordinering og synkronisering av EU/EØS-landenes nasjonale personvernarbeide med utgangspunkt i personverndirektivet fra 1995. Gruppen har ingen beslutningsmyndighet, men en rådgivende funksjon overfor Kommisjonen. Det norske Datatilsynet har observatørstatus.

Gruppen tar av eget tiltak opp en rekke saker, men blir også fra Kommisjonens side bedt om råd og kommentarer. Sakslisten er stor både i bredde og omfang. Og voksende. Dette er en hovedårsak til at man har valgt å saksforberede gjennom arbeidet i undergrupper som møtes forholdsvis uformelt. Norge har for tiden sluttet seg til en undergruppe som beskjeftiger seg med ulike sider ved politiets virksomhet nasjonalt og internasjonalt.

Av aktuelle saker under behandling nevnes for øvrig:

- Holdning til og mulig regulering av adgangen til å programmere PC-er for automatiske tilbakemeldinger.
- Vilkår for utlevering av flypassasjerlister til myndigheter i land utenfor EU til andre formål enn flyselskapenes egne.
- Bruk av biometriske data for pass og andre id-dokumenter.
- Kommersiell utnyttelse av persondata som stat og kommune innhenter for sine forvaltningsformål.

- Bruk- og bruksbetingelser for anvendelse av den nye RFID-teknologien (dvs. sporing av gjenstander og personer ved hjelp av radiobølger)

Utviklingen av Internett og de indirekte personverntrusler som knytter seg til monopoltendenser innen softwaresektoren går igjen i gruppens behandling av flere saker og temaer.

Internasjonalt datatilsynsmøte
Hvert år holdes det en internasjonal konferanse for datatilsynsjefer med deltakere fra hele verden. Polen var vertskap for 2004-konferansen. Konferansen inneholder en åpen del som også andre enn datatilsynssjefene kan delta på. Men vel så viktig er den del av konferansen hvor møtet bare er åpent for datatilsynssjefene. Et interessant tema i år var spørsmålet om tilgjengeligheten på arkivene etter de gamle regimene i Polen DDR, og Argentina.

Berlingruppen
Den internasjonale arbeidsgruppen for personvern innen telekommunikasjon (Berlin-gruppen) er primært etablert for å arbeide med tekniske problemstillinger knyttet til telekommunikasjon, men behandler også andre tekniske problemstillinger. Arbeidet i gruppen gir Datatilsynet viktige bidrag i sitt arbeid med tekniske problemstillinger. Datatilsynet deltok derfor på begge møtene som ble holdt i 2004. Sentrale saker i meldingsåret var å utvikle felles innstillinger når det gjelder:

- kommersialisering av lokaliseringsdata fra GSM mobiltelefonnett
- å oppnå tilfredstillende sikring av trådløse nettverk
- foretrukne metoder for å bekjempe elektronisk kriminalitet med personvernvennelige metoder
- personvern innen medias håndtering av personopplysninger. Dette var for øvrig et spørsmål hvor de nordiske land hadde dissens på grunn av våre bestemmelser om ytringsfrihet.

RIPE (Réseaux IP Européens)
Datatilsynet deltok med en person på to møter i RIPE i 2004. Møtene er et felles forum for alle som er interessert i IP-nettverk i Europa. Formålet med forumet er å sikre nødvendig administrativ og teknisk koordinasjon for å etablere et pan-Europeisk IP-nettverk. Diskusjonen i møtene er til stor nytte for Datatilsynets arbeid og gir mulighet til å være oppdatert på nyheter innen IP-teknologi.

Europeisk ekspertgruppe innen teknologi
Etter invitasjon fra det franske datatilsynet deltok Datatilsynet med en representant på stiftelsesmøtet for en ekspertgruppe innen teknologiske spørsmål. Gruppen skal primært tjene som nettverk for teknologisk ekspertise i de europeiske land. Videre fremdrift for gruppen er ikke avklart.

OECD
OECD har en undergruppe som arbeider med informasjonssikkerhet og personvern. Datatilsynet deltok som observatør på et møte i 2004. Det er Nærings- og Handelsdepartementet som utgjør den offisielle norske representasjonen. Sentrale tema i det aktuelle møtet var knyttet til digitale signaturer og PKI.

Nordisk teknologimøte

Nordisk teknologimøte er opprettet for å skape god kontakt mellom de teknologiske miljøene hos personvernmyndighetene i de nordiske land. Aktuelle tekniske problemstillinger diskuteres med sikte på å komme frem til en mest mulig felles håndhevelse av regelverket i de nordiske land. Møtet holdes årlig, denne gang i Finland. Sentrale problemstillinger på møtet var:

- Digitale signaturer
- Strategi og metodikk ved gjennomføring av operative tilsyn
- Hel-automatiske bomstasjoner. Utveksling av synspunkter på teknologi og løsninger
- Lokaliseringsteknologi ved bruk av GSM-nett.

Nordisk datatilsynsmøte
Danmark var vertskap for møtet. Av sentrale saker som ble tatt opp var blant annet retten til anonym ferdsel i samferdselssektoren og resultatene fra et felles nordisk tilsynsprosjekt om behandling av personopplysninger ved ansettelsesprosesser.

Saksbehandlermøte innen EU/EØS
To saksbehandlere deltok i 2004 på to møter i regi av det internasjonale samarbeidsforumet for saksbehandlere ("complaint workshop"). Møtene ble holdt i henholdsvis Stockholm og Praha. Saker som ble drøftet var blant annet politimetoder og bruk av politiregistre og overvåking i arbeidslivet.

Nordisk saksbehandlermøte
Møtet ble i år holdt på Island og omfattet tema som anonymitet innen samferdsel, elektroniske postjournaler, samordning av offentlige etater og samtykkeproblematikken innen forskning.

Joint Supervisory Authority (JSA)
JSA er det felles tilsynsorgan for Schengen informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengenområdet, eller er straffedømt i et av medlemslandene. Datatilsynet møter med en fast observatør. Det har i meldingsåret vært et ekstra høyt aktivitetsnivå. Dette skyldes generelt stor aktivitet i Schengensamarbeidet. JSA har i tillegg hatt fellesmøter med tilsynsorganet for Europol, og tilsvarende når det gjelder tollssamarbeidet.

Se egen omtale av internasjonalt politisamarbeide senere i årsmeldingen.

6 INFORMASJON SOM VIRKEMIDDEL

Personvernlovgivningen legger i stor grad ansvaret på den enkelte når det gjelder å ivareta sitt eget personvern. Samtidig er alle som behandler personopplysninger, enten det er offentlige etater eller næringsdrivende, pålagt vesentlige plikter med hensyn til å etterleve lovgivningen på området. Datatilsynet er derfor avhengig av å oppnå synlighet i samfunnet og å skape en aktiv debatt, refleksjon og bevissthet omkring sentrale personvernspørsmål. Aktiv kommunikasjonsvirksomhet er dermed et virkemiddel som vektlegges sterkt. Dette skjer i første rekke gjennom mediekontakt, Datatilsynet hjemmeside og en svartjeneste for publikum ("Frontservice").

Sentralisert betjening av telefon- og e-posthenvendelser
Datatilsynet bruker en betydelig del av ressursene til å betjene spørsmål som kommer inn via brev, e-post og telefoner. De aller fleste henvendelsene blir kanalisert til en profesjonalisert førstelinjetjeneste, "Frontservice", bestående av tre jurister som også trekker på teknologisk kompetanse når de ser behov for det. Dette sikrer at publikum raskt og enkelt får den faglige rådgivningen som er nødvendig. Etter ett års erfaring er det tydelig at publikum setter pris på denne løsningen.

2004 var det første hele året med en systematisk registrering av antall telefon- og e-posthenvendelser til Frontservice. I løpet av året er det blitt registrert i overkant av 9 000 besvarte telefonhenvendelser og 2 258 henvendelser pr. e-post. De reelle tallene er imidlertid høyere, idet en del telefonhenvendelser går direkte til øvrige saksbehandlere. Reservasjon/DM, arbeidsliv og fjernsynsovervåking utgjorde nær halvparten av alle henvendelsene.

Rådgivning om informasjonssikkerhet
Datatilsynet har lagt vekt på gi råd og veiledning til virksomheter som arbeider med å sikre personopplysninger i samsvar med regelverket. I en del saker krever dette veiledning i møter, mens mindre kompliserte spørsmål kan tas via telefon eller e-post.

Datatilsynet gjennomførte 70 veiledningsmøter. I tillegg ble det besvart om lag 700 henvendelser over telefon og 450 e-posthenvendelser om temaet. Disse kommer i tillegg til det som er besvart fra Frontservice.

Hovedvekten av henvendelsene er knyttet til behov for avklaring og fortolkning av kravet til forholdsmessig sikkerhet, samt råd om hvordan dette kan gjennomføres i praksis. En del konsulentselskaper, produsenter og leverandører tar også kontakt for å få en bedre forståelse av regelverket.

Tilsvarende holdes en rekke møter for rene juridiske avklaringer.

Stor medieoppmerksomhet
I forhold til organisasjonens størrelse og administrative ressurser var Datatilsynet også i 2004 en meget synlig aktør i samfunnsdebatten og i mediebildet. Mange ulike saksområder har aktualisert interessen for, og spørsmål om, personvern fra journalister. Det kan virke som om spørsmål som berører personvern er kommet mer på dagsorden. Personvern er en ideell interesse som er vanskelig å kommunisere verdien av, når man skal ta stilling saker der personverninteressene skal veies opp mot hensyn som i større grad kan visualiseres og vekke følelser og engasjement hos folk flest. Dette stiller store krav til måten Datatilsynet kommuniserer på.

Den økte oppmerksomheten omkring personvernspørsmål vises tydelig i antall medieoppslag hvor Datatilsynet er nevnt. Det ble i løpet av 2004 registrert 2 189 nyhetsinnslag på norske medienes internettsider, mot 1 500 året før. Det reelle antallet nyhetsoppslag antas imidlertid å være enda høyere enn dette, da mange nyheter kommer i trykk (eksempelvis i lokale medier) eller på radio/tv uten at disse samtidig gjøres tilgjengelig via Internett.

Populær Personvernrapport

I tillegg til å utarbeide den tradisjonelle årsmeldingen som legges fram for Stortinget, ble det i 2004 også utarbeidet en popularisert trykksak, "Personvernrapporten 2004". Denne fikk betydelig større oppmerksomhet enn ved tidligere tradisjonelle årsmeldinger. Personvernrapporten ble trykket og distribuert i seks tusen eksemplarer. Det kom imidlertid etterpå inn etterbestillinger av et helt annet omfang enn tidligere, deriblant flere bestillinger av klassesett til videregående skoler og høgskoler.

Fokus på kameraovervåking
Det et stadig større problem at ulike aktører som har tatt i bruk kameraovervåking ikke kjenner til regelverket på området. Det er et stort behov for å nå frem med bedre kunnskap om regelverket til brukerne av utstyret, da det er disse som også sitter med ansvaret.

Datatilsynet utarbeidet derfor en veileder om kameraovervåking. Denne er skrevet slik at den skal være lett forståelig. Etter at veilederen ble distribuert også til ulike regionale og lokale medier kom det mange presseoppslag som fokuserte på problemstillingen. Den økte oppmerksomheten bidro til så mange bestillinger av veilederen at ekstra opplag ganske raskt måtte trykkes opp.

Seminar
Det ble også innledet et samarbeide med bransjeforeningen for elektrofag, NELFO. Brosjyren ble som del av dette samarbeidet distribuert til samtlige medlemmer og en rekke andre lesere av organisasjonens fagblad. Datatilsynet samarbeider også med NELFO om en større dagskonferanse om kameraovervåking som avvikles februar 2005.

Datatilsynets hjemmeside
Arbeidet med å oppgradere veiledninger for publikum og behandlingsansvarlige virksomheter har hatt høy prioritet. Det er derfor blitt publisert nye veiledninger når det gjelder:

- Om publisering av bilde og andre personopplysninger om mindreårige på Internett
- Om detaljregistreringer i arbeidslivet
- Om personvern knyttet til arbeidsliv, herunder arbeidsgivers innsyn i e-post mv.
- Om bruk av fødselsnummer i skole/barnehage
- Internkontroll - spørsmål og svar
- Veileder om kameraovervåking
- Om overføring av personopplysninger til utlandet
- Meldeskjemaer er gjort tilgjengelig også på nynorsk og engelsk

Det ble i meldingsåret publisert 74 egenproduserte nyhetsartikler og notiser.

Nær 2 000 personer står på en abonnentliste for melding om nyhetsoppdateringer på nettstedet. Estimert antall daglig besøkende på hjemmesiden er fortsatt ca 700.

Arbeidet med å etablere en ny og mer funksjonell hjemmeside ble igangsatt i 2004. Denne lanseres mars 2005.

Seminarer og foredragsvirksomhet
I stedet for å bruke ressurser på å administrere egne kurs- og konferanser satser Datatilsynet heller på å stille opp med foredragsholder på arrangementer i regi av andre. Dette synes å ha vært en vellykket strategi. I 2004 stilte Datatilsynet opp med

foredragsholdere på i overkant av 70 ulike seminarer og konferanser. Dette er et tilsvarende omfang som året før.

Datatilsynet var initiativtaker til, og en sentral bidragsyter ved en to dagers konferanse om personvern i kommunesektoren som ble arrangert i regi av Kommunenes sentralforbund.

Personvernombud
Mange bedrifter og organisasjoner behandler daglig store mengder personopplysninger. Ved usikkerhet omkring hva som er lovlig eller ikke kontakter mange av disse Datatilsynet for å få rådgivning. Flere virksomheter har imidlertid sett at det kan være en bedre ordning på frivillig basis å opprette sitt eget personvernombud.

Personvernombudet er en ressursperson som kjenner virksomheten, hvilke formål som ligger til grunn for behandlingen av personopplysninger, hvilke fremgangsmetoder som benyttes og hvilke behandlingssystemer som er innført. Ombudet vil raskt og presist kunne håndtere problemstillinger som måtte oppstå. Ikke minst vil personvernombudet både innad i virksomheten og utad fremstå som en fagperson med spesialkompetanse, som kan bistå i for eksempel opplæring og klagesaksbehandling. I tillegg åpner oppnevnelsen av personvernombud for lettelser i forhold til den lovpålagte meldeplikten.

Norsk samfunnsvitenskapelig datatjeneste, NSD er personvernombud for alle landets universiteter og de vitenskapelige og statlige høyskolene. I tillegg har flere institutter, private høyskoler, helseforetak og sykehus valgt NSD som sitt personvernombud. Til sammen er NSD personvernombud for 115 ulike virksomheter.

I tillegg til at ytterligere 15 virksomheter har oppnevnt NSD som personvernombud, er det i løpet av 2004 kommet til følgende nye virksomheter med personvernombud:

- Kommunene Ballangen, Grane, Hamarøy, Nesna, Steigen og Øksnes har alle oppnevnt Alf Leinan, It-Con A/S som sitt personvernombud.
- Universitetssykehuset Nord-Norge HF: Personvernombud Per Bruvold
- Wyeth Lederle Norge: Personvernombud Reidar Lewis

Status ved årsskiftet er dermed at 8 personvernombud representerer til sammen 130 ulike virksomheter.

Seminar for ombudene
Datatilsynet arrangerte, i likhet med året før, et seminar over to dager for nye og allerede etablerte personvernombud. Formålet med seminaret er å gi grunnleggende opplæring i personopplysningsloven og helseregisterloven, samt å skape nettverk mellom personvernombudene.

Datatilsynet samarbeidet også med Ullevål universitetssykehus om et seminar som fokuserte på ivaretakelse av personvernet ved medisinsk forskning. Bakgrunnen for dette var at sykehuset har etablert en organisasjon som bidrar til at virksomheten ivaretar lover og forskrifter innen medisinsk forskning. Etablering av personvernombud internt i virksomheten var viktig i dette arbeidet. På seminaret orienterte sykehuset om hvordan arbeidet med ivaretakelse av personvernhensyn i forskningen er blitt organisert rent praktisk.

Politiet og kommunesektoren neste?
Datatilsynet har i flere sammenhenger foreslått at det også innen politiet utnevnes personvernombud. Med tilfredshet kan det derfor konstateres at det i forslag til politiregisterlov (NOU 2003:21) er foreslått at det opprettes personvernombud innen politiet. Også i kommunesektoren behandles det en så stor mengde personopplysninger, hvorav mye sensitivt, at opprettelse av personvernombud burde være naturlig å vurdere for mange kommuner. Større kommuner som allerede har oppnevnt byombud, bør vurdere å legge også personvern inn i ombudsfunksjonen.

Bransjevise adferdsnormer
I personopplysningsloven legges det opp til at Datatilsynet skal bistå i utarbeidelsen av bransjevise adferdsnormer. I meldingsåret sluttførte Norges Idrettsforbund arbeidet med bransjeregler for idrett. Formelt er reglene ennå ikke vedtatt, men dette vil skje på vårparten 2005. I dette arbeidet har Datatilsynet arbeidet tett sammen med Idrettens hovedorganisasjon.

Datatilsynet tar sikte på å arbeide videre med andre bransjer i kommende år.

7 TILSYNS- OG SIKKERHETSARBEID

Tilsynsvirksomheten er et viktig virkemiddel i Datatilsynets arbeid med å fremme et godt personvern i samfunnet. I tillegg til å kontrollere etterlevelsen av regelverket, er tilsynene også en viktig kanal for dialog og kunnskapsoverføring, til nytte for både tilsynsobjektene og Datatilsynet.

Datatilsynet har i rapporteringsåret innført såkalt "brevlige tilsyn" som et supplement til "stedlige tilsyn", det vil si besøk hos tilsynsobjektene. Denne fremgangsmåten velges i hovedsak ved systemrevisjoner og ved verifisering av konkret dokumentasjonsplikt. Der hvor behovet for direkte dialog er mer fremtredende, er besøk hos tilsynsobjektene fortsatt mest hensiktsmessig.

Tilsynsaktiviteten baseres på et internt utarbeidet kvalitetssystem for tilsyn. Året inndeles i to tilsynsperioder. For hver periode utarbeides en tilsynsplan. Denne omtaler i hovedsak organiseringen av tilsynsaktiviteten og de temaene som danner grunnlag for valg av tilsynsobjekter.

Datatilsynet gjennomførte til sammen 161 brevlige og stedlige tilsyn i 2004. Oversikten nedenfor viser tilsynsaktiviteten innen forskjellige områder:

Bransje / Sektor	Antall
Arbeidsliv	8
Detaljhandel	2
Fjernsynsovervåkning	24
Forskning	76 *
Internettrelatert virksomheter	9
Kommune	1
Markedsførere	2
Primærhelsetjenesten	10
Helseforetak	1
Private / ideelle organisasjoner	7
Telekommunikasjon	5
Samferdsel	7
Trygd	5
Krisesentre	5
Sum	**161**

* Det ble kontrollert 76 konsesjoner innen forskning. Antall stedlige tilsynsbesøk var 29.

En fullstendig liste over tilsynsobjektene ligger som eget vedlegg bak i årsmeldingen.

7.1 HOVEDINNTRYKK

Mange aktører har fortsatt manglende kunnskap om regelverket. Dette synliggjøres i første rekke gjennom at virksomhetene ikke har etablert en oversikt over hvilke personopplysninger de faktisk behandler. De har heller ikke satt i gang nødvendige aktiviteter for å møte de pliktene de har i følge regelverket. De aller fleste tilsynsobjektene får derfor anmerkning fra Datatilsynet om manglende internkontroll. Dette er alvorlig fordi internkontrollsystemet, og tilhørende bestemmelser om informasjonssikkerhet, skal danne fundamentet i etterlevelsen av personvernlovgivningen.

Ledelsen svikter

Rapportene fra tilsynsvirksomheten viser at et flertall av virksomhetene har etablert visse rutiner når det gjelder sin behandling av personopplysninger. Imidlertid er disse rutinene i liten grad satt inn i et helhetlig system, tuftet på en vurdering av pliktene i regelverket. Et viktig element i internkontrollsystemet er fastsettelse av ansvar og myndighet i virksomheten. Det er i manglende grad tatt initiativ fra ledelsens side når det gjelder å sette i gang nødvendige aktiviteter og å klargjøre ansvar. I den grad det er tatt formelle initiativ er disse i liten grad fulgt opp av organisasjonen i praksis. Oppbygging, implementering og vedlikehold av et vel fungerende internkontrollsystem tar nødvendigvis en del tid og ressurser første gang man gjør dette.

Store og ressurssterke virksomheter burde ha både forutsetninger og tradisjon for systemrettet tenking. Erfaringene fra tilsynsvirksomheten tyder imidlertid ikke på noen sammenheng mellom virksomhetens størrelse og hvorvidt man har etablert et internkontrollsystem. Det avgjørende er hvilke kunnskaper og holdninger ledelsen i virksomhetene faktisk har i forhold til dette arbeidet.

Datatilsynet minner imidlertid at etablering av et internkontrollsystem er et lovpålagt krav, som virksomhetene ikke lenger kan nedprioritere eller sette helt til side.

Manglende systematikk
Når det gjelder informasjonssikkerhet, har de fleste virksomheter etablert sikkerhetstiltak, men det viser seg å være en manglende systematikk også i dette arbeidet. God sikkerhet forutsetter en systematisk prosess. Hva virksomheten anser å være en tilfredsstillende informasjonssikkerhet skal fastlegges, risiko skal kartlegges og nødvendige tiltak skal gjennomføres. Mangel i forhold til å etablere struktur og innhold i denne del av internkontrollsystemet er fortsatt fremtredende.

Dårlig sikkerhet ved elektronisk samhandling
Samhandlingen mellom publikum/kunder og offentlige og private virksomheter skjer naturlig nok i økende grad ved hjelp av elektroniske hjelpemidler. Publikum forventer at man skal gis muligheten til å kommunisere via Internett og e-post, om man ønsker det. Virksomhetene på sin side ser på dette som en mulighet til både å gi bedre service og å effektivisere kundedialogen. Datatilsynet erfarer imidlertid at den infrastrukturen som bygges opp for den elektroniske samhandlingen ofte ikke er god nok. Mange virksomheter benytter dårlig sikrede e-postløsninger og tilbyr løsninger på Internett med en utilstrekkelig grad av sikkerhet.

Publikum har stort sett tillit til at virksomheter de oppfatter som seriøse og skikkelige, også ivaretar sikkerheten i de elektroniske løsningene de oppfordrer publikum til å benytte seg av. Brukerne vil derfor ikke reservere seg mot å kommunisere også sensitive personopplysninger, dersom de ikke tydelig advares mot det. I den grad ellers ansvarlige virksomheter tilbyr løsninger som reelt sett er lite sikre, bidrar dette til at publikum heller ikke i andre sammenhenger stiller spørsmål ved sikkerheten i løsningene.

Bildet er imidlertid ikke entydig negativt. Datatilsynet har gjennom sin tilsynsvirksomhet også sett løsninger hvor informasjonssikkerheten virkelig er tatt på alvor, samtidig som hensynet til kostnader, effektivitet og brukervennlighet er ivaretatt.

Nasjonal satsing nødvendig
Erfaringene Datatilsynet har høstet de siste årene understreker behovet for en nasjonal satsning for å etablere en tilfredstillende infrastruktur for trygg samhandling via elektroniske medier. Moderniseringsministeren har i den sammenhengen tatt viktige initiativ for å fremme elektroniske signaturer.

Brudd på sletteplikten
Personopplysninger som ikke lenger er nødvendige for formålet med registreringen skal slettes. De gjennomførte tilsynene viser imidlertid at brudd på sletteplikten er fremtredende. Problemet synes ikke å være knyttet til noen spesiell sektor, men er gjennomgående.

Virksomhetene har i liten grad fastsatt retningslinjer og tilhørende rutiner for sletting av overskuddsinformasjon. Inntrykket er at mange velger å fortsatt lagre personopplysninger selv om man er klar over disse egentlig skulle vært slettet. Det kan ikke utelukkes at virksomhetene rett og slett vurderer det slik at kostnadene ved fortsatt oppbevaring av personopplysninger er lavere enn kostnadene ved å ha rutiner for gjennomgang og sletting.

Man lagrer også for det tilfelle at man, av årsaker man ikke overskuer i dag, kanskje likevel en gang i fremtiden kan dra nytte av personopplysningene.

Publikums rett til innsyn
I følge personopplysningsloven skal den behandlingsansvarlige bistå den registrerte med å gi innsyn i hvilke personopplysninger som er lagret, hva de skal brukes til, og hvor de er hentet fra.

Virksomhetene forteller at de registrerte i liten grad krever innsyn under henvisning til personopplysningsloven. Innen offentlig forvaltning er innsynsretten i praksis langt på vei også ivaretatt av offentlighetslov, forvaltningslov og særlovgivningen. I privat sektor oppfattes det å gi innsyn i registrerte opplysninger av mange virksomheter som en naturlig del av kundeservice og dialog. Datatilsynet vil likevel minne om at den behandlingsansvarlige må sørge for å ha retningslinjer for ivaretakelsen av den registrertes innsynsrett etter personopplysningsloven. Ikke minst er det også viktig at reglene gjøres kjent for de av organisasjonens medarbeidere som møter publikum.

Personvern - hemsko for utvikling?
Personvern ser ut til å komme under stadig sterkere press ved avveiningen mot andre hensyn. Krav til rasjonalitet og effektivitet er stikkord i denne sammenhengen. Virksomheter, i økende grad også innen offentlig sektor, tar ikke tilstrekkelig hensyn til personvernet. Enkelte unnlater også helt å vurdere konsekvensene for personvernet når nye løsninger og tiltak etableres. Flere aktører gir også direkte uttrykk for at hensynet til personvern oppleves som en hemsko i utviklingen. Gjennom tilsynsvirksomheten ble det for eksempel avdekket at enkelte medisinske forskere rett og slett hadde valgt å ikke forholde seg til konsesjonsvilkårene fra Datatilsynet. Dette kan være signal om en svekket forståelse og respekt for intensjonene bak personvernlovgivingen.

Datatilsynet erfarer også i økende grad at tilsynsobjektene markerer uenighet i forhold til de vedtak som tilsynet fatter i forbindelse med tilsynsvirksomheten. Vedtakene blir påklaget til Personvernnemnda. Årsaken til dette kan dels ligge i at det er blitt gjennomført langt flere tilsyn enn tidligere, samtidig som Datatilsynet er tydeligere i sin fortolkning av regelverket enn når personopplysningsloven var helt ny. Problemstillinger som har kommet opp i forbindelse med tilsynsaktivitetene, kan derfor ha ligget latent i lang tid.

Behandlingen av klagene i Personvernnemnda bidrar i alle tilfeller til klargjøring og presedens for tilsvarende saker som dukker opp senere.

Internasjonaliseringen gir utfordringer
Datatilsynet erfarer i økende grad utfordringer når det gjelder det å føre tilsyn med selskaper som har aktivitet i flere land og hvor den behandlingsansvarlige har sitt hovedsete utenfor landets grenser. Dette gjelder selv om selskapene er etablert innenfor EØS-området, hvor EUs personverndirektiv gjelder. I prinsippet skal slike tilsyn ivaretas ved en koordinering mellom tilsynsmyndighetene i respektive land. En slik koordinering fører imidlertid til et betydelig merarbeid og byr ofte på praktiske problemer. Blant annet er det store variasjoner landene i mellom når det gjelder omfang og organisering av den operative tilsynsvirksomheten. Datatilsynet er i dialog omkring dette med øvrige land, særlig de nordiske.

7.2 STØRRE TILSYNSPROSJEKTER

Datatilsynet valgte i 2004 å organisere noe av tilsynsaktiviteten som større prosjekter. Denne organiseringen ble valgt for sektorer hvor det ble vurdert som viktig sette inn ressurser for en ekstra grundig, og dermed ressurskrevende, kartlegging. Det ble gjennomført prosjektbaserte tilsyn innen følgende områder:

- Krisesentre
- Elektronisk kommunikasjon innen helsesektoren
- Trygdeetaten
- Medisinsk forskning

Tilsynsprosjektet om medisinsk forskning blir omtalt under temadelen senere i årsmeldingen. Det ble også gjennomført et forprosjekt når det gjelder behandling av personopplysninger innen idretten. Dette prosjektet vil bli fulgt videre opp i 2005.

Krisesentrene

Krisesentrene var opprinnelig etablert med lokal frivillig arbeidsinnsats og deres virksomhet har aldri vært lovregulert. Dette har gitt utfordringer, blant annet i forhold til taushetsplikten. Forhold av svært personlig art kan lett eksponeres i lokalsamfunnet. Konsesjonene, som i sin tid ble utstedt med hjemmel i den tidligere personregisterloven, fulgte derfor en svært restriktiv praksis. Krisesentrene fikk kun registrere navn og adresse på brukerne, og da i første rekke for omadressering av post.

Mye har endret seg siden de første krisesentrene dukket opp på første halvdel av 1980-tallet. Personopplysningsloven har erstattet den tidligere personregisterloven. Samtidig har mange krisesentre utviklet seg til å yte flere tjenester enn kun å fungere som et tilfluktssted for mishandlede kvinner.

Datatilsynet organiserte derfor i 2004 et tilsynsprosjekt overfor krisesentrene. Først ble det sendt ut et kartleggingsskjema til samtlige 50 krisesentre. Etter å ha mottatt tilbakemeldinger fra 39 sentre, ble fem valgt ut for stedlige tilsynsbesøk.

Det er særlig tre spørsmål Datatilsynet har vært opptatt av i prosjektet:

- retten til anonymt opphold
- taushetsplikt/utlevering av opplysninger,
- registrering av opplysninger om tredjeperson

Retten til anonymt opphold

Retten til å oppholde seg anonymt på krisesenteret har lenge vært et viktig prinsipp for Datatilsynet. Et flertall av krisesentrene svarte i kartleggingen at kvinnene blir gitt mulighet til å oppholde seg anonymt. Tilsynsbesøkene avdekket imidlertid at det bare var ett av fem krisesentre som ga en *reell* mulighet til anonymt opphold. Det ble imidlertid ikke foretatt identitetssjekk ved noen av sentrene. Etter dialog med krisesentrene ser Datatilsynet at det kan være gode grunner for at kvinnen skal oppgi sitt navn under oppholdet. Primært er dette knyttet til ivaretakelse av kvinnens egen sikkerhet, for eksempel ved akutte sykdomssituasjoner, evakuering og lignende. Dette behovet er imidlertid mindre for dagbrukere enn beboere.

Utlevering av opplysninger

Fordi krisesentrene ikke er regulert av særlover, er samtykke til behandling av personopplysninger helt grunnleggende. Samtykkekravet vil som hovedregel gjelde også ved utlevering av opplysninger til barnevernet.

De aller fleste krisesentrene oppgir å ha som hovedregel at kvinnens samtykke innhentes før barnevernet eventuelt kontaktes. Hovedregelen fravikes dersom situasjonen vurderes til å være svært alvorlig med hensyn til barnets liv og helse. Datatilsynet er tilfreds med at lederne ved krisesentrene synes å ha et meget bevisst forhold til denne problemstillingen.

Ved utveksling av opplysninger til andre institusjoner og etater ser krisesentrene gjennomgående ut til å være påpasselige med å innhente samtykke til utvekslingen. For lagring av opplysninger til bruk for eventuell senere rettssak, og til bruk under oppholdet, synes det imidlertid ikke å foreligge tilfredsstillende samtykkeerklæringer.

Registrering av opplysninger om tredjepersoner
I tillegg til opplysninger om kvinnen registreres også opplysninger om øvrige familiemedlemmer, i første rekke barn. Barne- og familiedepartementet har dessuten utarbeidet relativt detaljerte skjemaer som i utgangspunktet ikke skal være knyttet til kvinnens, eller tredjepersons, identitet. Datatilsynet ser det imidlertid som bekymringsfullt at skjemaene for beboere og dagbrukere gir informasjon også om overgriper, og at disse opplysningene oppbevares sammen med opplysninger om kvinnen.

Videre oppfølging
Med bakgrunn i kartleggingen, og de stedlige tilsynene, har Datatilsynet utarbeidet et utkast til retningslinjer for krisesentrene. De tar utgangspunkt i hvordan Datatilsynet mener at personopplysningsloven bør tolkes og anvendes i forhold til krisesentrene. Retningslinjene er sendt til berørte instanser for uttalelse. De vil deretter bli formidlet i en endelig form til samtlige krisesentre.

Elektronisk kommunikasjon i primærhelsetjenesten
Høsten 2004 gjennomførte Datatilsynet et tilsynsprosjekt som satte fokus på elektronisk kommunikasjon i primærhelsetjenesten. Prosjektet var en direkte videreføring av den løpende tilsynsaktiviteten som Datatilsynet har hatt mot helsesektoren siden 2002. Målet med prosjektet var å kartlegge noen av de utfordringene som primærhelsetjenesten møter ved å ta i bruk elektronisk kommunikasjon mot helseforetakene og øvrige instanser innen helsesektoren, og i dialog med sine pasienter. Den mer generelle etterlevelsen av regelverket med hensyn til internkontroll og informasjonssikkerhet ble også kontrollert.

Det ble gjennomført ti tilsyn som ledd i prosjektet. Fem stedlige og fire brevlige tilsyn var rettet mot legekontorer, og ett stedlig tilsyn hos mot helseforetak. Det ble også holdt møter med to leverandører av programvare for elektronisk kommunikasjon.

Tilsynene viste at ansvarsforholdene var rimelig avklarte når det gjelder legekontorenes oppkopling mot de regionale helsenettene. I forhold til leverandørene av programvare for elektronisk kommunikasjon hadde legekontorene imidlertid mindre oversikt og klarhet i hvem som har ansvar for hva. Datatilsynet konstaterte også at det var en del uklarhet i forhold til utveksling av meldinger mellom legekontorene og andre aktører innen helsevesenet.

Erfaringene fra tilsynene tyder på at primærhelsetjenesten i svært liten grad har etablert en tilfredsstillende internkontroll når det gjelder sin behandling av helseopplysninger. Syv av ni legekontorer fikk derfor varsel om pålegg grunnet manglende etterlevelse av helseregisterlovens bestemmelser om internkontroll, mens åtte av ni fikk pålegg som følge av manglende etterlevelse av sikkerhetsbestemmelsene.

Også helseforetaket fikk pålegg om å rette opp manglende etterlevelse av bestemmelsene om internkontroll og informasjonssikkerhet.

Betryggende i Trygdeetaten
Trygdetaten omfatter Rikstrygdeverket, 500 enheter på fylkes og kommunenivå, og har om lag 9 000 tilsatte. Trygdeetaten har sensitive personopplysninger om nær sagt alle landets innbyggere. Datatilsynet ønsket derfor å få bedre oversikt over trygdeetatens håndtering av personopplysninger - særlig hvorvidt vilkårene for de ulike behandlingene av personopplysninger er oppfylt, hvordan den registrertes rettigheter ivaretas, og om opplysningene sikres godt nok. Tilsynet fokuserte på internkontrollsystemet og implementeringen av dette.

Det ble gjennomført tilsyn hos Rikstrygdeverket sentralt, ved to fylkestrygdekontorer og to lokale trygdekontor. Selv om dette har vært det mest omfattende tilsynsprosjektet Datatilsynet har utført i en og samme behandlingsansvarlige virksomhet, er likevel ikke alle etatens behandlinger av personopplysninger kartlagt. Til det er omfanget av trygdeetatens virksomhet for stort.

Resultatet av tilsynet var oppløftende og ga et positivt inntrykk av Trygdeetaten. Rutinene for håndtering av personopplysninger i virksomheten virket totalt sett å være meget gode, og var tydelig forankret i beslutninger fra ledelsen. Det fremstod som viktig for ledelsen og virksomheten som helhet at personopplysninger behandles korrekt og forsvarlig. Det ser ut til at Trygdeetaten har lagt til grunn at godt personvern er en forutsetning for at etaten kan oppnå ønsket tillit i befolkningen.

Selv om Datatilsynet kunne konstatere at trygdeetatens behandling av personopplysninger i all hovedsak skjer i samsvar med regelverket, ble det avdekket enkelte avvik. Det er behov for ytterligere utvikling av rutinene knyttet til situasjoner der medlemmer ber om innsyn i opplysninger om seg selv. Rikstrygdeverket må også klargjøre lagringsbehovet for opplysninger om misbruk av trygdemidler når mistanken senere frafalles. Det må blant annet etableres rutiner for sletting i samsvar med dette. Videre må Rikstrygdeverket videreutvikle rutinene i internkontrollsystemet, slik at man har enda bedre sikkerhet for at avvik fra fastlagte rutiner blir håndtert av riktig nivå i organisasjonen.

7.3 KORT OM ØVRIGE TILSYN

Her nevnes kort noen av de øvrige tilsynene som ble gjennomført i 2004, men som ikke omtales nærmere i temadelen senere i årsmeldingen.

Detaljhandel/fordelskort
Datatilsynet gjennomførte tilsyn mot to aktører som benytter såkalte fordelskort. Den som benytter et slikt kort får et utbytte, beregnet ut fra hva vedkommende kjøper hos kjeden. Kunden på sin side aksepterer at opplysninger som kortnummer, tidspunkt og beløp

overføres til et sentralt kunderegister. Disse opplysningene benyttes blant annet til markedsføring og statistikk.

Det er tilsynets oppfatning at aktørene er opptatt av personvern, og at kunnskapen om personopplysningsloven er god. Dette skyldes nok for en stor del at bransjen er avhengig av tillit fra medlemmene, og at et brudd på personopplysningsloven kan få foretningsmessige følger.

Internettleverandører
Datatilsynets hovedfokus ved tilsyn mot leverandører av internett-tilgang for private var å kontrollere virksomhetenes praksis med hensyn til lagring og sletting av personopplysninger, utlevering av disse, samt forvaltning av e-post kontoer for sine kunder.

Det ble ikke avdekket at det foretas registrering av hvilke sider internettbrukerne besøker, eller hvilken adferd brukerne har ved oppkobling mot Internett. Slik logging ville ifølge internettleverandørene dessuten ha vært svært ressurskrevende å gjennomføre.

Noen av internettleverandørene ga til kjenne en liberal praksis med utlevering av trafikkdata til politiet. Det ble sjelden bedt om formell kjennelse før materialet ble overlevert til politiet.

Datatilsynet påpekte ovenfor flere av virksomhetene at sikring av kundenes e-post ikke var tilfredstillende. Unødvendig mange ansatte hadde etter Datatilsynets mening muligheter for å tilegne seg kundenes brukernavn og passord. Leverandørene må beskytte passordfilene bedre, for eksempel ved at disse krypteres. Datatilsynet ser på ovennevnte som et midlertidig problem, da struktur for elektronisk identifisering og digitale signaturer er i ferd med å utvikles. Slike løsninger vil trolig overta for det tradisjonelle brukernavnet og passordet.

7.4 STYRINGSSVIKT I ORGANISASJONEN?
Trygdeetaten har vist at det lar seg gjøre å innføre et vel fungerende internkontrollsystem. Man må da spørre seg: Hvorfor har Trygdeetaten fått det til, mens en systematisk tilnærming til internkontroll er nærmest fraværende i mange av de andre virksomhetene Datatilsynet har ført kontroll med?

Hos mange virksomheter oppfattes det ikke som naturlig eller viktig å etablere et strukturert system for styring av virksomheten. Selv i store virksomheter kan Datatilsynet konstatere at det er en manglende kompetanse i forhold til å etablere enhetlige systemer. Styringen av virksomheten foregår etter helt andre mekanismer enn hva regelverket forutsetter. Å ha en systematisk tilnærming til internkontroll, som i utstrakt grad bygger på samme konsept som system for kvalitetssikring, føles derfor fjernt for mange. I andre virksomheter kan kompetansen være tilstede, men man setter ikke på dagsorden å etterleve offentlig regelverk.

Moderne regelverksutvikling er tuftet på forutsetningen om et strukturert pliktsubjekt. Den ansvarlige forutsettes å ta ansvar og handle. Dette innebærer å sørge for at noe konkret skjer i virksomheten. Ingen tilsynsorganer forventer at virksomhetens øverste leder selv skal gjennomføre de pålagte pliktene. Den ansvarlige skal imidlertid sørge for å utløse

handling. Ofte delegeres store deler av arbeidet med tilpasning til regelverket til mellomledere i virksomheten. Dette kan være både en hensiktsmessig og riktig strategi, men det fritar imidlertid ikke den øverste ledelse for sitt ansvar og plikt til oppfølging. Det system som bygges opp i linjeorganisasjonen må tillegges den makt og autoritet som et ledelsessystem krever. Dette forutsetter tilstedeværelse og fokus fra virksomhetens øverste ledelse.

For øverste leder handler altså spørsmålet i stor grad om å delegere oppgaver eller plikter, forvisse seg om fremdrift, bemyndige i samsvar med internkontrollsystemet og sørge for en systematisk oppfølging og periodisk gjennomgang. Virksomhetens størrelse vil være av stor betydning for hvordan dette løses i praksis.

Datatilsynet konstaterer i mange av sine tilsyn at den øverste lederen ikke har tatt det ansvaret som regelverket forutsetter. Virksomhetens etterlevelse av regelverk vil da ofte være basert på initiativ fra linjeledelsen. I noen tilfeller kan dette gi et tilfredstillende resultat, men i de fleste tilfeller mangler den autoriteten som internkontrollen forutsetter.

Lederskap handler fremfor alt om å ta ansvar, vise vei og sette standard i forhold til hvordan virksomheten skal opptre. Internkontrollsystemet er et verktøy i utøvelsen av dette lederskapet.

8 TEMAER 2004

8.1 DIREKTE MARKEDSFØRING

Over en million reserverte
Ved utgangen av året hadde 1 036 296 personer registrert seg i reservasjonsregisteret i Brønnøysund. Registeret ble opprettet 1. januar 2001 for at privatpersoner skulle kunne reservere seg mot telefonsalg og adressert reklame. Siden den gang har det vært en stadig økende tilstrømning av personer som ønsker slik reservasjon. Tallet på reserverte er nær doblet bare i løpet av det siste året. Av alle reserverte har 99 prosent reservert seg mot telefonsalg, 88 prosent vil ikke bli kontaktet av humanitære og samfunnsnyttige organisasjoner, mens 56 prosent ikke ønsker å motta adressert reklame i posten.

Tabellen nedenfor gir oversikt over utviklingen i antall som har reservert seg i det sentrale reservasjonsregisteret siden det ble opprettet i 2001 og frem til årsskiftet 2004. Tallene viser det samlede antallet registrerte ved utgangen av det enkelte 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 et stort antall misfornøyde med måten reservasjonsordningen fungerer på. Dette til sammen antyder at man bør se nærmere på hele ordningen. Bare i løpet av 2004 mottok Datatilsynet omkring 1 800 klager fra folk som hadde reservert seg, men som likevel ble oppringt av selgere.

Henvendelsene til Datatilsynet viser at det er ulike grunner til at folk mottar uønskede markedsføringshenvendelser. Det kan være at enkeltpersoner er registrert i forskjellige registre med ulike variasjoner i navnet, de har fått ny adresse, de får henvendelser i navn av å være en juridisk person, eller markedsførerne følger ikke reglene med vask mot det sentrale reservasjonsregisteret godt nok.

På bakgrunn av dette vil Datatilsynet se nærmere på reservasjonsordningen. En av ideene som har vært luftet i den forbindelse er at den direkte markedsføringen kan baseres på forhåndssamtykke og ikke reservasjon. Det vil altså si at man må foreta en aktiv handling for å få markedsføringshenvendelser, i motsetning til i dag der man selv aktivt må be om å ikke få det.

Endringer i markedsføringsloven?
Datatilsynet har hatt forslag til endringer i markedsføringslovens § 2 b om forbud mot uanmodet e-postreklame og lignende til høring. I sin høringsuttalelse ga tilsynet full tilslutning til at fysiske personer generelt bør dekkes av kravet om forhåndssamtykke ved direkte markedsføring. Også juridiske personer bør få en viss form for beskyttelse mot direkte markedsføring. Ukentlig mottar tilsynet henvendelser fra næringsdrivende som er oppgitt over mengden av direkte markedsføring som de ikke får stoppet. Særlig små enkeltmannsforetak føler dette som et stort problem.

Tips en venn
I høringsuttalelsen kommenterte Datatilsynet også behovet for en rettslig avklaring når det gjelder "tips en venn"- funksjoner. Disse har blant annet vært brukt i reklamekampanjer. Et av problemene er at det på denne måten skjer en spredning av personopplysninger som den enkelte selv ikke har kontroll over. Det må i hvert fall være klare begrensninger hva gjelder bruk av den oppgitte informasjon utover å oppfylle den oppgave vennen har akseptert. Tilsynet er likevel skeptisk til ordningen som helhet, da den rokker ved det grunnleggende personvernrettslige prinsipp om at alle skal ha kontroll over egne personopplysninger. Mister man denne kontrollen, mister man til en viss grad muligheten til å benytte seg av de rettigheter personopplysningsloven tillegger den enkelte, særlig når det gjelder innsyn, retting og sletting. Dette nettopp fordi man ikke vet hvor ens egne personopplysninger tar veien.

Tipsdatabase for mulig brudd på reservasjonsretten
Datatilsynet har opprettet en tipsdatabase for internt bruk. Klager fra publikum som hevder at navngitte virksomheter ikke respekterer reservasjonsretten, registreres fortløpende. Ordningen gir dermed en god mulighet til å følge opp de virksomhetene som det særlig klages over, for eksempel ved avlegge virksomhetene et tilsynsbesøk.

Med bakgrunn av den systematiske registreringen innkalte Datatilsynet ledelsen hos en direkte markedsfører til møte, med krav om forklaring på hvorfor tilsynet hadde mottatt så mange klager rettet mot nettopp denne virksomheten. Metoden viste seg å være meget effektiv, idet det etter møtet ikke er kommet flere klager på den aktøren.

Adresselister fra Posten
Posten Norge AS har et register over de fleste privatpersoner boende i Norge; Postmottakersystemet (PMS). En registrering i Postmottakersystemet er nødvendig for distribusjon av post, og skjer ved innrapportering fra postbud, gjennom meldinger om adresseendringer og gjennom datavask mot Folkeregisteret.

Posten henvendte seg til Datatilsynet da de ønsket å leie ut adresselister fra dette registeret. Adresselistene skulle ikke inneholde personer som er reservert i det sentrale reservasjonsregisteret i Brønnøysund, personer under 15 år, personer med hemmelig adresse eller døde personer. Datatilsynet ga Posten Norge lov til å bruke adresselister over privatpersoner til å korrigere opplysninger i andre lister (listevask). Imidlertid avslo Datatilsynet at Posten skulle kunne leie ut adresselistene. Avslaget ble påklaget til Personvernnemnda.

Personvernnemnda fant, i likhet med Datatilsynet, at utleie av adresselistene er uforenelig med det opprinnelige formålet; å drive postformidling. Formålet med Postens adresseregister er at post skal kunne fordeles til riktig mottaker. Formålet med utleie av listene er derimot videreformidling av adresseopplysninger til andre aktører som ønsker å betale for å bruke postens lister. Nemnda viser også spesielt til forarbeidene til personopplysningsloven, som understreker at hensynet til privatlivets fred skal gis betydelig vekt i avveiningen mot kommersielle interesser. Datatilsynets vedtak ble derfor opprettholdt.

8.2 OFFENTLIG FORVALTNING

Datatilsynet har i løpet av året mottatt en rekke høringer som reiser sentrale spørsmål om offentlig sektors behandling av personopplysninger. Felles for mange av initiativene er ønsket om å få til en mer kostnadseffektiv og brukerrettet offentlig forvaltning, i tråd med regjeringens moderniseringsprogram. Noen av de foreslåtte tiltakene innebærer lagring av store mengder personopplysninger i sentrale databaser, eventuelt at det etableres portaler for utveksling av personopplysninger forvaltningen imellom. Eksempler på dette er Moderniseringsdepartementets planer om en felles offentlig it-arkitektur og etablering av en database med grunndata for det offentlige til bruk av ulike forvaltningsorganer. Videre Helse- og omsorgsdepartementets "Norsk pasientregister" og Utdanningsdepartementets sentrale elevregister knyttet til nasjonale prøver.

Det effektive ikke alltid det riktige

Det er naturlig, og i de fleste sammenhenger også riktig, at man også i offentlig sektor tar i bruk ny informasjonsteknologi for å effektivisere og rasjonalisere sine saksbehandlingsprosesser og samhandling med publikum.

Imidlertid vil Datatilsynet minne om at stat og kommune ikke *ensidig* kan legge vekt på idealer fra privat sektor og etablere løsninger som synes hensiktsmessige ut fra rene effektivitetshensyn. Selv om offentlige etater, i likhet med privat sektor, driver utstrakt tjenesteyting, utøver det offentlige i tillegg også en betydelig grad av makt- og myndighetsutøvelse. Det offentlige må derfor, i tillegg til økonomisk rasjonalitet, også legge vekt på hensyn som rettssikkerhet, personvern og medvirkning for alle deler av befolkningen. Det er i siste instans opp til de øverste politiske myndigheter å avveie rene effektivitetshensyn opp mot slike grunnleggende rettigheter.

Sentrale databaser
Datatilsynet ser med bekymring på en utvikling mot store sentrale databaser med personopplysninger. Ut fra personvern- og rettssikkerhetshensyn kan det i mange sammenhenger faktisk være hensiktsmessig at personopplysninger fortsatt lagres på forskjellige steder i forvaltningen og at manglende standardisering forhindrer "fri flyt" av opplysningene. Det at det krever en del ressurser å samle inn og sammenstille personopplysninger fra ulike kilder kan også bidra til mindre misbruk. Menneskelige "portvakter", som stiller spørsmål ved hvorvidt det er riktig og nødvendig å gi ut personopplysningene, kan også redusere unødig spredning. Dersom man fjerner disse hindringene ved etablering av nye og mer effektive løsninger, må det i stedet bygges inn andre mekanismer som reduserer potensialet for at personopplysninger spres unødig eller misbrukes.

All erfaring tilsier dessuten at etableringen av store databaser med godt strukturerte personopplysninger raskt fører til et press for at opplysningene også skal taes i bruk til helt andre formål enn hva de opprinnelig ble innsamlet for.

Felles it-arkitektur og felles grunndata
Moderniseringsdepartementet sendte høsten 2004 ut to rapporter til høring, *"Forprosjektrapport om arkitektur for elektronisk samhandling i offentlig sektor"* og rapporten *"Persondatautveksling i Norge"*. Begge rapportene berører hvordan det offentlige bedre kan utveksle og benytte persondata. Rapportene har imidlertid en så overlappende og uoversiktlig tematikk at det var vanskelig for Datatilsynet å ta stilling til innholdet i disse. Rapportene er lite konkrete med hensyn til mål, analyser, tiltak og konsekvenser. Vurderinger med hensyn til personvern og informasjonssikkerhet er nærmest helt fraværende. Man har stort sett nøyd seg med å gå rett på lettvinte konklusjoner om at fordelene ville overstige de mulige ulempene for personvernet, eller at slike spørsmål var det andre prosjekter som tar hånd om. Lov og regelverk, herunder personvernlovgivningen, blir i den ene rapporten omtalt som "hindringer" for de nye og effektive løsningene som søkes etablert. Dette kan være uttrykk for en manglende forståelse for de hensynene og veloverveide vurderingene som ligger bak dagens personvernlovgivning i Norge og Europa for øvrig.

Maktforskyvning
Rapportene tar til orde for å få til mer gjenbruk og en mer effektiv utnyttelse av forskjellige typer grunndata på tvers av forvaltningen. En betydelig del av den informasjonen som skal utveksles vil naturlig nok være personopplysninger. Det at offentlige myndigheter får en enklere tilgang til stadig større mengde opplysninger om den enkelte borger, uten å være i direkte kontakt med vedkommende, kan isolert sett bidra til en svært effektiv forvaltning. Imidlertid kan det også bidra til en forsterket maktforskyvning fra den enkelte borger til myndighetene.

"Min side"
Moderniseringsdepartementet skal etablere en felles inngangsdør til offentlige tjenester på Internett i løpet av sommeren 2005. Gjennom "Min side" skal borgerne kunne få tilgang til digitale tjenester uavhengig av hvilken sektor eller forvaltningsnivå som tilbyr tjenestene.

Innsyn gir bedre personvern
Etableringen av "Min side" kan gjøre det lettere for den enkelte å kontrollere hvilke personopplysninger som ulike statlige og kommunale etater har registrert om vedkommende. Det er også mulig å etablere løsninger som varsler den berørte når ulike forvaltningsorganer utveksler opplysninger om vedkommende. Bedre muligheter for innsyn vil bidra til økt kvalitet i de personopplysningene som forvaltningsorganene benytter seg av, ved at feil i opplysningene oppdages og rettes, og overskuddsinformasjon slettes. På denne måten kan "Min side" bidra til, ikke bare en mer effektiv og brukervennlig forvaltning, men også til et bedre personvern. Dette forutsetter imidlertid at hensynene til personvern og informasjonssikkerhet taes inn som sentrale premisser allerede tidlig i planleggingen.

Ulike brukere - ulike forutsetninger
Når det offentlige skal etablere løsninger hvor man oppfordrer alle til å ta i bruk dataverktøy i sin dialog med forvaltningen må det også etableres sikkerhetsløsninger som tar høyde for at brukerne har høyst ulike forutsetninger for å bidra til oppfyllelse av den samlede informasjonssikkerheten ved bruk av tjenestene. Det er en kjensgjerning at mange private databrukere i liten grad tar i bruk helt elementære sikkerhetsløsninger, eksempelvis viruskontroll, brannmur, passord og annen konfigurasjonskontroll. Og, i enda mindre grad, elektronisk signatur og kryptering som i dag er nødvendig for sikker kommunikasjon. Mange er også fortsatt avhengig av å benytte offentlig tilgjengelige PCer for eksempel på biblioteker, skoler og internettkafeer.

Datatilsynet har derfor overfor Moderniseringsministeren pekt på behovet for at det foretas sikkerhetsvurderinger og tilpasninger av løsningen også med tanke på de store variasjonene med hensyn til sluttbrukernes dataverktøy, kompetanse og mulighet til å ivareta eget personvern. Ved bruk av dagens nettbankløsninger er det i første rekke bankene selv som tar konsekvensene ved misbruk. Brukerne lider derfor i liten grad tap dersom de ikke selv har utvist grov uaktsomhet. Ved etablering av en felles portal, hvor mange personopplysninger gjøres tilgjengelig, må det tilsvarende avklares hvem som skal ta ansvaret ved misbruk og hvem som skal bære kostnadene når noe går galt. Det kan vise seg vanskelig å sette en prislapp på den byrde borgeren må bære dersom personopplysninger skulle komme på avveie eller bli misbrukt.

Sikkerhetsnivåer og klargjøring av ansvar
Å få til en sikker identifisering av brukeren vil være helt avgjørende. Dersom det skal benyttes én portal med sentral pålogging må sikkerhetsnivået dimensjoneres i forhold til det til enhver tid mest sensitive materialet som tilbys, og det samlede omfanget av personopplysninger som kan hentes ut via portalen.

Moderniseringsdepartementet har nedsatt en prosjektgruppe som skal komme fram til løsninger for sikker kommunikasjon mellom publikum og forvaltningen. Viktige aktører i denne prosessen har vært de store offentlige etatene som har utstrakt samhandling med publikum. Datatilsynet har kun vært observatør i arbeidet. Tilsynet konstaterer at de offentlige etatene kommuniserer ulike behov med hensyn til hva som skal regnes som tilstrekkelig sikker kommunikasjon. Det må imidlertid være hensynet til brukerne som er avgjørende for hvilken løsning som velges. Datatilsynet mener at det bør etableres én enhetlig løsning som kan gi tilfredsstillende kommunikasjon mellom alle parter og nivåer. Dette også ut fra en samfunnsøkonomisk vurdering.

Før løsningen blir satt i drift må det også være avklart hvem som skal være behandlingsansvarlige etter personopplysningsloven for de ulike elementer av datagrunnlaget som presenteres i portalen, og hvem som skal være behandlingsansvarlig for den samlede løsningen. De behandlingsansvarlige vil være selvstendig ansvarlige for å forankre elementene i en sikkerhetsstrategi. Gjennomførte risikovurderinger må også dokumentere en samlet forsvarlig sikkerhet i alle ledd av løsningen.

Skoleporten og nasjonale prøver
Utdanningsdepartementet har, i forbindelse med nasjonale prøver, etablert et sentralt register som lagrer karakterer, navn og fødselsnummer for alle skoleelever i Norge. Datatilsynet fikk utover høsten 2004 henvendelser fra mange lærere som var bekymret for denne sentrale registreringen og den tilhørende profilbyggingen. I følge nettstedet "skoleporten.no" skal profilen følge eleven og brukes til å gi tilpasset opplæring.

Datatilsynet ser det som uheldig at forskriftsbestemmelsen som pålegger den sentrale innrapporteringen ikke var forelagt Datatilsynet til uttalelse. Tilsynet bad derfor Utdanningsdepartementet om en redegjørelse for hvilke vurderinger som ligger til grunn for å knytte karakteropplysningene til navn og fødselsnummer. Over tid kan disse profilene bli meget omfattende, og innebære personvernrisiko for den enkelte elev. Man kan heller ikke forvente at barn kan ivareta sine rettigheter etter loven på samme måte som voksne.

Datatilsynet har i oppfølgende møter med Utdanningsdepartementet uttrykt sin fortsatte skepsis til den løsningen som er valgt. Utdanningsdepartementet vil som følge av dette ta løsningen opp til ny vurdering, og var ved årsskiftet fortsatt i dialog med Datatilsynet om dette.

Ny lov om utdanningsstøtte
Datatilsynet stiller seg kritisk til den foreslåtte bestemmelsen om innhenting av personopplysninger i forslaget til ny Lov om utdanningsstøtte. I stedet for å innhente opplysninger ved samtykke fra søkeren selv, foreslås det at Statens lånekasse med hjemmel i lov skal kunne innhente en rekke opplysninger fra andre.

Tilsynet har forståelse for at man søker å etablere mer effektive og kostnadsbesparende tiltak for administrasjon av utdanningsstøtten. På den annen side er det vesentlig at lånsøkere i størst mulig grad selv bidrar med opplysninger som er relevante. En administrasjon av rettigheter som i stor grad baserer seg på innhenting av opplysninger fra andre, vil kunne føre til at den registrerte mister oversikten over hvilke opplysninger som er lagt til grunn for behandlingen. Innhenting av opplysninger fra andre krever i tillegg høy kvalitet og pålitelighet.

Tilsynet er også kritisk til forslaget om å gi en vid lovhjemmel til å kunne innhente opplysninger også om tredjepersoner.

Samordning av arbeidsmarkedsetaten, trygdeetaten og sosialtjenesten
Rattsø-utvalget la sommeren 2004 frem sitt forslag om en samordning av arbeidsmarkedsetaten, trygdeetaten og sosialtjenesten. Utvalgets anbefaling innebærer en løsning der det organiseres en ny, statlig etat for arbeid og inntekt, og en ny statlig etat for pensjoner samt stønader og refusjoner i forbindelse med nedsatt helse, pluss en rekke andre

ytelser knyttet til barn. Utvalget foreslår at kommunen beholder ansvaret for å yte sosialhjelp.

Deler av forslaget vil innebærer store personvernmessige konsekvenser for den enkelte. En sentralisert og stor ansamling av til dels meget sensitive personopplysninger gir et økt potensiale for misbruk. Svært mye kunnskap om det enkelte menneske vil kunne bli tilgjengelig for førstelinjetjenesten. Forslaget kan også føre til et stort press mot taushetsplikten mellom fagområdene og internt i etatene.

Utvalget ønsker at man skal ha en stor grad av organisatorisk fleksibilitet. Det anbefalte forslaget legger derfor opp til at førstelinjetjenesten skal kunne arbeide på tvers av formelle etatsgrenser. De skal kunne håndtere opplysninger fra mennesker som søker hjelp både når det gjelder pensjonsspørsmål, refusjon av utgifter for sin nedsatte helse, og spørsmål om manglende inntekt ved langvarig sykdom.

Datatilsynet mener at forslaget om en slik førstelinjetjeneste ikke er tilrådelig, spesielt om det legges opp til at den enkelte saksbehandler skal få tilgang til svært omfattende, og kanskje også sensitiv informasjon om innbyggerne i kommunen.

Taushetsbestemmelsene bør etter Datatilsynets oppfatning ikke strekkes lenger enn nødvendig. Den enkelte saksbehandler bør ikke gis tilgang til flere opplysninger enn vedkommende faktisk trenger for å løse sin oppgave. Selv om den enkelte saksbehandler har taushetsplikt også overfor saksbehandlere i samme etat, har organiseringen av arbeidet mye å si for om personopplysninger spres eller ikke. Mindre etater med noe mer spesialiserte oppgaver vil medføre mindre spredning.

Datatilsynet anbefaler at man bruker de muligheter som ny IT-teknologi gir, til å etablere interne tilgangsbegrensninger. Slike begrensninger i systemene kan sikre at saksbehandlerne kun får tilgang til de opplysningene de trenger for å løse sine konkrete oppgaver. En uthuling av taushetsplikten vil kunne gi etatene lav tillit i befolkningen.

Datatilsynet er for øvrig ikke enig i Rattsø-utvalgets fremstilling av at personvern og rettssikkerhet ”setter unødige hindringer for et samarbeid mellom offentlige etater til brukerens beste”. Regelverket på personvernområdet er nært knyttet opp til internasjonale konvensjoner som Norge er forpliktet til å følge.

Supplerende stønad for personer med kort botid i Norge
I utkast til Lov om supplerande stønad for personar med kort butid i Norge foreslås det at trygdekontorene skal gis en svært vid adgang til å kontrollere rettighetshaverne etter loven. I realiteten gis Trygdeetaten mulighet til å innhente alle typer opplysninger fra alle offentlige instanser. Den foreslåtte loven vil innebære en oppheving av taushetsplikten i en rekke andre særlover. Datatilsynet er skeptisk til en slik oppheving uten at det er vurdert hva taushetsplikten og diskresjonshensyn representerer av verdi i den enkelte særlov. Trygdeetaten vil, dersom lovforslaget gjennomføres, også få tilført mye overskuddsinformasjon.

8.3 HELSE OG FORSKNING

Kan vi som pasienter stole på at opplysninger vi gir legen behandles i fortrolighet? Gjennom store, sentrale registre føres nå oversikt over nær sagt all kontakt med

helsevesenet. Opplysningene i journalene kan også i mange tilfeller leses av andre helsearbeidere og kontorpersonell, uten særlig etterkontroll av at oppslaget var berettiget.

Datatilsynet merker også en tendens til at man for forskning og administrasjon ønsker å ha stadig større og mer overgripende datasamlinger med svært mange opplysninger om hver enkelt, gjerne på identitet, slik at den enkelte kan følges gjennom flere år.

Dårligere personvern med nytt Norsk pasientregister
Sosial- og helsedirektoratet foreslo i 2004 å gjøre Norsk pasientregister om til et register knyttet til identitet. Dette er Datatilsynet sterkt i mot. I høringsuttalelsen påpekte Datatilsynet på at et personentydig Norsk pasientregister, med sentralisert kartlegging av den enkelte norske borgers helsetilstand og bruk av sykehus fra fødsel til død, vil ha negative personvernkonsekvenser for nær sagt alle i Norge.

Det foreslåtte Norsk pasientregister er et nøkkelregister. Ved bruk av noen få opplysninger herfra kan en identifisere hver enkelt av oss i de fleste andre helseregistre – uavhengig av om registrene i utgangspunktet er avidentifiserte eller pseudonyme. Når man ser de eksisterende helseregistrene i sammenheng med det foreslåtte pasientregisteret, blir den samlede kartleggingen bortimot altomfattende.

Datatilsynet ser Norsk pasientregister som så personverntruende at tilsynet heller ikke anbefaler en løsning med et pseudonymt register.

Allerede i dag eksisterer et Norsk pasientregister av mindre omfang. Registeret har konsesjon fra Datatilsynet med vilkår om at navn og personnummer skal slettes. Helse- og omsorgsdepartementet ønsker å lagre flere opplysninger i registeret, og søkte i 2004 om konsesjon for en utvidelse. Datatilsynet mener det ikke er heldig å fremme konsesjonssøknad om utvidelse samtidig som forslag om registerets fremtidige utforming er til offentlig høring.

Lovfesting av Forsvarets helseregister
Datatilsynet var i sin høringsuttalelse svært kritisk til at Forsvarets helseregister skulle lovfestes slik forslag til lov om personell i forsvaret la til grunn. Forslaget var etter Datatilsynets mening utilstrekkelig begrunnet. Formålet med registeret ble utvidet i forhold til tidligere, og den foreslåtte bestemmelsen fremstod nærmest som en blankofullmakt til å forskriftsfeste det registeret Forsvaret til enhver tid måtte ønske seg. Man vurderte ikke personvernulempene noe sted i utkastet, til tross for at det ble hevdet at en slik gjennomgang er viktig.

Etter høringsrunden kom man frem til at det er hensiktsmessig å hjemle Forsvarets helseregister i helseregisterloven. Registeret blir dermed underlagt de samme reglene som andre sentrale personidentifiserbare helseregistre, og også underlagt de samme rettssikkerhets- og personvernskrankene. Det er vedtatt av Stortinget at Forsvarets helseregister hjemles i helseregisterloven § 8. Lovendringen trådte i kraft fra 1. januar 2005.

Landsomfattende helseundersøkelser og kvalitetsregistre
Datatilsynet ga i slutten av 2003 og begynnelsen av 2004 konsesjoner til en rekke av de store helseundersøkelsene. Blant annet Helseundersøkelsen i Nord-Trøndelag (HUNT), Tromsøundersøkelsen og Osloundersøkelsen ble tildelt konsesjoner for mange av sine

prosjekter. Disse konsesjonene er i stor grad bygget over samme lest. Datatilsynet aksepterte en videreføring av samtykket som opprinnelig er innhentet, til tross for at det ikke er tilfredsstillende i forhold til de krav som stilles i dagens lovverk. Det ble imidlertid stilt vilkår for hvilke sammenhenger dataene kan benyttes i, og når man må innhente nytt samtykke og gi ny informasjon til de registrerte. Konsesjonen dekker ikke all bruk av dataene. I enkelte tilfeller krever bruk av disse dataene at det også søkes om ny konsesjon fra Datatilsynet. Dette er spesielt aktuelt dersom dataene skal utleveres til bruk i et prosjekt i regi av andre enn konsesjonsinnehaveren.

Kreftregisteret fikk flere nye konsesjoner. Noen av Kreftregisterets prosjekter har etter Datatilsynets oppfatning ikke kunnet dokumentere at de tilfredsstiller grunnleggende krav i helseregisterloven og personopplysningsloven. I fire av prosjektene har Datatilsynet gitt konsesjon med vilkår om at det må innhentes nytt samtykke for videre behandling av de registrerte data. Disse fire vedtakene er påklaget av Kreftregisteret.

I 2004 ble det også gitt nye konsesjoner til blant annet Nasjonalt leddproteseregister, Nasjonalt MS-register, Nasjonalt Korsbåndregister og Nasjonalt hjertestansregister.

Stor saksmengde gir bedre avklart praksis
Datatilsynet har behandlet en stor mengde saker på helse- og forskningsområdet etter at helseregisterloven og personopplysningsloven trådte i kraft i henholdsvis 2002 og 2001. Saksmengden har gitt et godt grunnlag for etablering av en mer ensartet praksis.

Flere avgjørelser i Personvernnemnda det siste året har videre klargjort tilsynets praksis og trukket opp viktige prinsipper for anvendelse av lovverket, spesielt forholdet til hvilket behandlingsgrunnlag ulike forskningsprosjekt kan hjemles i.

Overordnede prinsipper
Samtykke er utgangspunktet, men følgende argumenter kan vektlegges for å avvike fra utgangspunktet:

- innhenting av samtykke vil føre til lav deltagelse, og dette reduserer undersøkelsens verdi
- informasjon og reservasjonsadgang til den registrerte reduserer ulempene
- om undersøkelsen ikke medfører innhenting av nye opplysninger, anses ulempen å være mindre for de registrerte
- de registrertes antatte interesse for at forskningsprosjektet finner sted

Tilføring av nye opplysninger i sentrale forskriftsbaserte helseregistre må hjemles i forskrift. Datatilsynet har ikke myndighet til å gi konsesjon som utvider forskriftsbestemmelser.

Nedslående funn innen helseforskning
Er behandlingen helseopplysningene får innen forskningen betryggende? Etter å ha ført tilsyn med 50 forskningsprosjekter kunne ikke Datatilsynet se mange lyspunkter.

Datatilsynet satte ned en prosjektgruppe som gjennomførte tilsyn med 50 forskningsprosjekter våren 2004. Det ble ført tilsyn med 26 virksomheter innenfor ulike helseforetak, læresteder, forskningsinstitusjoner, samt legemiddelprodusenter. Prosjektet

avdekket flere forhold som Datatilsynet ser alvorlig på. Tilsynet fant brudd på konsesjonsvilkår, ulovlig oppbevaring av sensitive personopplysninger, fravær av internkontroll og manglende oversikt over ansvarsplassering. Det er utarbeidet en egen rapport som redegjør for funn og tendenser i forbindelse med prosjektet. Rapporten er tilgjengelig på Datatilsynets hjemmeside.

Brudd på konsesjonsvilkår
Datatilsynet har valgt å stille konsesjonsvilkår knyttet til gjennomføringen av prosjekter for å få dem innenfor lovens rammer, snarere enn å avslå konsesjonssøknaden fullstendig. Konsesjonsvilkårene er dermed et viktig verktøy som også kommer forskere til gode.

Av de 17 prosjektene som hadde konsesjon, hadde 11 ikke fulgt konsesjonsvilkårene, uten at forskerne kunne gi noen god forklaring på dette. At konsesjonsvilkårene synes å bli etterlevd i bare seks av 17 prosjekter er et nedslående resultat.

Ulovlig oppbevaring av sensitive personopplysninger
I 15 av 33 kontrollerte prosjekter fant Datatilsynet at man ikke hadde gyldig hjemmelsgrunnlag i helseregisterloven og personopplysningsloven. For flere av prosjektene betyr det at forskeren ensidig har endret premissene for prosjektet uten at deltakeren er informert. Dette innebærer at samtykket ikke lenger er gyldig.

Lav sikkerhet og brudd på sletteplikt
Også når det gjelder den praktiske sikringen av opplysningene var resultatet nedslående. Av 31 relevante prosjekter betrakter Datatilsynet kun 17 til å være utført praktisk forsvarlig. Åtte prosjekter var utført delvis forsvarlig, mens hele seks ikke var forsvarlig utført.

Tilsynene viste også at det jevnt over var en dårlig ivaretakelse av sletteplikten. Med en gjennomgående mangel på internkontroll hos de behandlingsansvarlige er det grunn til å tro at det foreligger store mørketall på området.

Brudd på konsesjonsplikt
I tilsynsprosjektet er det i liten grad gjort forsøk på å avdekke om det finnes forskningsprosjekter som ikke er lagt frem for Datatilsynet eller personvernombudet. Det ble likevel avdekket to konsesjonspliktige forskningsprosjekter som det ikke er søkt om konsesjon for etter helseregisterloven og personopplysningsloven.

Mangel på internkontroll
Virksomheter som behandler personopplysninger skal ha et system for internkontroll for å sikre at pliktene etter personopplysningsloven og helseregisterloven blir overholdt. Rutinene skal sikre at de registrertes rettigheter som bl.a. retten til innsyn, informasjon, retting og sletting blir ivaretatt.

Funn fra tilsynene viste at det nærmest var et totalt fravær av internkontroll. Kun én av 29 virksomheter kunne dokumentere et tilnærmet fullstendig implementert internkontrollsystem.

Datatilsynet fulgte opp med fem tilsyn med utvalgte forskningsprosjekter høsten 2004, og har valgt ut forskning som et område for tilsyn også i 2005.

Høring om forskriftsendring for forskning
Datatilsynet sendte høsten 2004 ut et høringsforslag om å utvide unntaket fra konsesjonsplikt for forskning (personopplysningsforskriftens § 7-27). Systemet med meldeplikt foreslås opprettholdt som hovedregel. Det skal etter forslaget i større utstrekning legges vekt på etterkontroll i form av tilsyn. Høringsnotatet inneholder to alternative forslag til forskriftstekst. Innholdsmessig er forslagene ment å være like. Det første alternativet åpner for en relativt stor grad av skjønnsmessig vurdering fra forskerens side, mens det andre i større grad er konkretiserende.

Bakgrunnen for forslaget til endring er at Datatilsynet har sett at forhåndskontrollen ikke har hatt den ønskede virkningen i alle sammenhenger. Tilsynet mener at større fokus på etterkontroll vil kunne ha et større personvernmessig potensial. Høringsfristen var 31. desember 2004.

Forenkling av melde- og søknadsprosedyrer ved medisinsk forskning
Datatilsynet har sittet i en arbeidsgruppe, oppnevnt av Helsedepartementet i januar 2004, som vurderte forenkling og effektivisering av melde- og søknadsprosedyrer ved medisinsk forskning. Arbeidsgruppen bestod av deltakere fra Sosial- og helsedirektoratet, Helsedepartementet, Den nasjonale forskningsetiske komité for medisin og Datatilsynet. Arbeidsgruppen gjennomgikk eksisterende skjemaer og søknadsprosedyrer og foreslo alternative måter å forenkle og effektivisere utfylling og behandling av søknader og meldinger. Hensikten var å vurdere mulighetene for forenklinger innenfor dagens regel- og rammeverk i påvente av Nylennautvalgets innstilling.

Arbeidet resulterte i at det er blitt etablert en oversiktlig forskningsportal på De forskningsetiske komiteers hjemmeside (se www.etikkom.no/REK/forskerportal) Portalen skal hjelpe forskere til å få en rask oversikt over hvilke melde- og søknadsprosedyrer de må gjennomgå for å starte et forskningsprosjekt. Det er dessuten utarbeidet en felles mal med momenter den enkelte forsker må igjennom ved utformingen av et informasjonsskriv.

8.4 INTERNETT
Publisering av personopplysninger på Internett reguleres som hovedregel av personopplysningsloven. Hvilke begrensninger gjelder når enkeltpersoner omtales på Internett?

Ytringsfrihet og personvern på Internett
Forholdet mellom ytringsfrihet og personvern på Internett ble satt på spissen i 2004. Et nettsted hadde lagt ut informasjon om en rekke enkeltpersoner som hadde arbeidet med barnevernsaker. Nettstedet omtalte personene i til dels sterkt kritiske ordelag, og kom med påstander om rettsstridig behandling. Datatilsynet fikk en rekke klager og henvendelser fra berørte parter, publikum og presse om saken.

Datatilsynet vurderte om bruken av personopplysninger på Internettsiden ble regulert av personopplysningsloven, eller om den kom inn under unntaket i loven for journalistiske, herunder opinionsdannende formål. Datatilsynet kom frem til at klagene måtte avvises. Begrunnelsen var at selv om behandlingen av personopplysninger på Internettsiden isolert sett krenket personvernet, kunne det totalt sett trolig sies å utgjøre samfunnskritikk. Det

var uklart om ytringene skulle anses som opinionsdannende eller ikke. Avvisningsvedtaket er påklaget til Moderniseringsdepartementet.

Vedtakene om avvisning av klagene i denne saken er underbygd med at det kreves en klar hjemmel i lov for inngrep i grunnleggende rettigheter (her i ytringsfriheten). Dette er i tråd med det såkalte *legalitetsprinsippet*. Personopplysningsloven gir, etter Datatilsynets oppfatning, ikke tilstrekkelig hjemmel for inngrep. Saken reiser prinsipielle spørsmål om hvor langt Datatilsynet, i personvernets navn, kan gå i å drive sensur av ytringer på Internett. Dette spørsmålet må avklares når personopplysningsloven skal etterkontrolleres i 2005.

I 2004 ble også aksjonærlistene til selskapet The five percent community (T5PC) publisert av media. Flere journalister og enkeltpersoner tok kontakt og lurte på om dette var i strid med personopplysningsloven. Datatilsynet mente at listen åpenbart var publisert til journalistiske formål, og at den dermed ikke var omfattet av personopplysningsloven.

Barn og unge på Internett
Datatilsynet tok i 2004 stilling til om foreldre til barn under 15 år kan kreve sletting av personopplysninger om barnet på Internett. Saken gjaldt nettstedet "deiligst.no". Barnets foresatte hadde i denne saken kontaktet innehaveren av siden og krevd bilder og andre personopplysninger slettet. Innehaveren av "deiligst.no" nektet å slette opplysningene uten at den som krevde sletting først legitimerte seg. Datatilsynet konkluderte med at foreldrene til barnet har samtykkekompetanse i slike tilfeller, og at retten til sletting kan utøves uten å måtte involvere barnet. Nettstedet ble pålagt å slette opplysningene og bildene.

Datatilsynet vil følge opp Internettsider av liknende karakter i 2005.

Publisering av festbilder på Internett
Stadig flere utesteder legger ut bilder av gjester på sine Internettsider. Bildene publiseres i markedsføringsøyemed, og ofte uten samtykke fra gjestene. Datatilsynet har gjort flere av utestedene oppmerksom på at slik publisering som hovedregel krever samtykke. Dette er et krav både i personopplysningsloven og i åndsverkslovens § 45, bokstav c. Kun informasjon om at bilder blir tatt og publisert er ikke nok til å oppfylle lovkravet om samtykke.

Datatilsynet gjennomførte i desember 2004 en kartlegging av hvor mange utesteder som publiserer bilder av gjestene. Over 90 Internettsider administrert av ulike utesteder ble undersøkt. Omlag 20 av disse publiserte personidentifiserende bilder. Tilsynet vil følge opp de alvorligste sakene, og sikre at publiseringen skjer i tråd med regelverket.

Publisering av saksdokumenter på Internett
Stadig flere forvaltningsorganer publiserer offentlige saksdokumenter i fulltekst på Internett på eget initiativ. Publiseringen begrunnes med hensynet til bedre service og økt tilgjengelighet, både for pressen og allmennheten for øvrig.

I en lovfortolkning fastslo Justisdepartementets lovavdeling sommeren 2004 at forvaltningen må forholde seg til personopplysningslovens krav når saksdokumenter publiseres på Internett etter eget initiativ. Dette innebærer at forvaltningen må ha hjemmel for publiseringen, primært samtykke fra den omtalte, når dokumentene inneholder flere personopplysninger enn personnavn og hvilken sakstype det er snakk om. Hvis dokumentet inneholder andre personopplysninger, for eksempel fødselsnummer, personlig økonomisk situasjon, utdanning og arbeidserfaring, må disse opplysningene sladdes, med mindre den det gjelder samtykker i at opplysningene publiseres .

Datatilsynet har gitt varsel om pålegg til flere kommuner som publiserte dokumenter i strid med regelverket. Tilsynet vil fortsette med å følge utviklingen på dette området nøye.

8.5 SAMFERDSELSSEKTOREN
I meldingsåret har det vært store og prinsipielle saker innen samferdselssektoren. En sak som har vært under behandling hele året, og som ennå ikke har kommet til en løsning, er Statens vegvesen sitt prøveprosjekt med helautomatiske bomstasjoner i Tønsberg, Bergen (og, senere viste det seg også, Gjesdal i Rogaland). Det har også blitt foretatt en kartlegging av samferdselsektoren, herunder telekommunikasjon. Formålet var å skaffe en oversikt over registreringsomfanget av personopplysninger og i hvilken grad den enkelte har rett og en reell mulighet til å kunne ferdes uten å legge igjen spor. Som et ledd i denne kartleggingen ble det gjennomført flere tilsyn.

Rett til sporfri ferdsel?
Personvern er vanskelig å definere. Hva som oppfattes som krenkende for en person kan oppleves helt annerledes for en annen. Retten til selv å kunne bestemme over egne opplysninger er derfor et av de helt sentrale personvernprinsippene. For at selvbestemmelse skal ha et virkelig innhold må den enkelte imidlertid stå overfor reelle valg med hensyn til om man skal la andre få tilgang til, og behandle personopplysninger om seg i ulike sammenhenger.

Retten til anonym ferdsel er ikke uttrykkelig slått fast i norsk lovgivning. En slik rett kan likevel utledes av de grunnleggende rettigheter i blant annet menneskerettskonvensjonens artikkel åtte og av EUs personverndirektiv. Her heter det at enkeltpersoners grunnleggende rettigheter og friheter må respekteres, særlig retten til privatlivets fred. I både personverndirektivet og i den norske personopplysningsloven er den enkeltes selvbestemmelsesrett et av grunnprinsippene – fortrinnsvis uttrykt ved avgivelse av et frivillig, informert og uttrykkelig samtykke til behandling av personopplysninger.

Gjelder ikke ubetinget
Retten til anonym ferdsel gjelder selvsagt ikke ubetinget. Det finnes både internasjonale og nasjonale regler som begrenser den enkeltes mulighet til å reise uten å måtte gi fra seg personopplysninger. Dette gjelder for eksempel identifikasjonskontroll og registrering av personer som ønsker adgang til et geografisk område, eller å reise med bestemte

transportmidler. Det finnes derfor bestemmelser om at alle passasjerer på skip som reiser over 20 nautiske mil skal registreres med navn, alder og kjønn. Opplysningene skal være tilgjengelige for redningstjenesten og andre relevante myndigheter i forbindelse med redningsarbeide.

Må tilrettelegg for sporfrie løsninger
Den grunnleggende retten det er for den enkelte å kunne ferdes fritt i det norske samfunnet uten å legge igjen elektroniske spor, forutsetter at aktørene innen samferdselssektoren må etablere sporfrie løsninger, med mindre sterke samfunnsmessige interesser skulle tilsi noe annet. Alle som planlegger løsninger som forutsetter registrering av opplysninger om individers bevegelser må derfor begrunne og dokumentere hva det er som gjør det nødvendig å gjøre unntak fra den grunnleggende retten til å kunne ferdes sporfritt.

Personopplysninger innen samferdsel - en kartlegging
Gjennom Nasjonal transportplan og Samferdselsdepartementets IKT-strategi tas det til orde for økt bruk og samordning av informasjons- og kommunikasjonsteknologi innen samferdselssektoren. Det er en uttalt målsetting at økt bruk av IKT skal bidra til bedre sikkerhet, effektivitet og nytte for de reisende. Denne utviklingen kan imidlertid komme i konflikt med personvernhensyn, ettersom økt bruk av IKT ofte også innebærer økt registrering av personopplysninger.

Datatilsynet har, blant annet gjennom forsøkene med helautomatiske bomstasjoner, erfart at personvern i bare liten grad vektlegges når nye løsninger etableres innen samferdselssektoren. Med denne bakgrunnen fant Datatilsynet det derfor nødvendig å gjennomføre en mer systematisk kartlegging av registreringsomfanget innen samferdselssektoren. Kartleggingen tok i første rekke for seg reiser ved bruk av fly og båt, øvrig kollektivferdsel og vegtrafikk. I en mer begrenset grad ble det også gjort kartlegging når det gjelder telesektoren.

Fly og båt
For reisende som benytter fly og båt, registreres det opplysninger som hvem som reiser, kjønn, passasjerkategori, eller aldersgruppe. Dersom kunden ønsker det registreres det også eventuelle preferanser for reisen. Alle disse registreringene, med unntak av preferansene, er lovpålagte og har som formål å ivareta sikkerheten til de reisende, til bruk ved ulykker eller andre hendelser. Omfanget av registrerte opplysninger er lite og de slettes kort tid etter at reisen er gjennomført.

Det ble, som ledd i kartleggingen, gjennomført stedlige tilsyn hos ett flyselskap, to reisebyråer og to ferjeselskaper. Hovedinntrykket er at selskapenes behandling av personopplysninger er i samsvar med bestemmelsene i personopplysningsloven.

Elektronisk billettering for buss og bane
Kartleggingen viste at operatørene innen kollektivtrafikken er i ferd med å gå fra det tradisjonelle billetteringssystemet til elektronisk billettering. Det ønskes innført kompatible systemer, slik at kunden kan bruke samme billett i et større geografisk område, og på sikt i hele landet. Også i en slik sammenheng er det viktig at den enkelte, uten for store økonomiske eller praktiske kostnader, fortsatt skal kunne reise kollektivt uten å legge igjen detaljerte opplysninger om seg og sitt reisemønster. De tanker og løsninger som hittil er blitt presentert for Datatilsynet synes å ivareta dette hensynet.

Strekningsvis automatisk trafikkontroll
Vegmyndighetene benytter kjøretøyenes registreringsnummer til kontroll av trafikk og trafikanter. Dette gjelder for eksempel ved passering av bomstasjoner, fartskontroller og kontroll av kjøre- og hviletid.

Datatilsynet ble under kartleggingsarbeidet gjort kjent med et prøveprosjekt som går ut på strekningsvis automatisk trafikkontroll. Dette innebærer at gjennomsnittsfarten måles mellom to kontrollpunkter. Siden denne typen fartskontroll reiser noen helt sentrale utfordringer i forhold til ivaretakelsen av personvernet, følger Datatilsynet nøye med på prøveprosjektet. Dette skal etter planen testes ut våren 2005, i området rundt Lillehammer.

Helautomatiske bomstasjoner
Datatilsynet ble på slutten av 2002 kontaktet av Statens vegvesen i forbindelse med et prøveprosjekt for helautomatiske bomstasjoner i Tønsberg og Bergen. Vegvesenet la innledningsvis opp til alternative betalingsformer, enten abonnement basert på AutoPass-brikke, eller etterskuddsfakturering basert på videoopptak av bilens registreringsnummer. I tillegg ble det lagt opp til en løsning der trafikanten kan betale kontant hos en agent for bompengeselskapet (for eksempel bensinstasjoner) innen tre dager etter passering. De registrerte passeringsopplysningene blir deretter slettet.

Løsningene innebærer at enhver passering av bomstasjonen blir registrert (blant annet bilens registreringsnummer, tid og sted). Datatilsynet meldte derfor tilbake at det i tillegg må tilbys et alternativ som gjør at det, i likhet med myntautomater eller manuell betjening, fortsatt er mulig å passere bomstasjonene uten å legge igjen personopplysninger. Datatilsynet forutsatte derfor at det, før prøveprosjektet ble igangsatt, måtte etableres et alternativ hvor det reelt sett ikke legges igjen passeringsopplysninger som kan knyttes til trafikanten.

Fortsatt ikke godt nok
For å tilfredsstille kravet om anonymitet etablerte Statens vegvesen en løsning med en AutoPass-brikke som fungerer som et ihendehaverbevis. Trafikanten deponerer på en brikke, og betaler den verdi brikken er ladet med. Ved senere lading av brikken benyttes brikkens identifikasjonsnummer som referanse for betalingen. I motsetning til abonnentsløsningen knyttes denne brikken ikke til et bestemt kjøretøy hos bompengeselskapet. Registrerte passeringsopplysninger kan dermed ikke spores tilbake til bil og trafikant.

Ved oppstart av de helautomatiske bomstasjonene i Tønsberg og Bergen i februar 2004 var det imidlertid mye som tydet på løsningen ikke fungerte slik at dette kunne regnes som et tilfredsstillende sporfritt alternativ. Det ble derfor gjennomført stedlige tilsyn både i Tønsberg og Bergen.

Datatilsynet fant at den løsningen som var valgt langt på vei sikret trafikantene sporfrihet, rent teknisk sett. Likevel var løsningen langt fra tilfredsstillende. Alternativet var betydelig underkommunisert og brikken vanskelig å få tak i. I Tønsberg måtte besøkende til og med passere bomstasjonen for å få tak i brikken på et Securitas-kontor innenfor bomringen. Løsningen ga ikke de trafikantene som besøker området en eller få ganger, en reell mulighet til å passere sporfritt. Anskaffelseskostnadene er også urimelig store for de som bare skal passere noen få ganger, og det tilbys ingen rabatter ved bruk av den anonyme brikken.

Vedtak om konsesjonsplikt
Selv om det ikke behandles sensitive personopplysninger i de helautomatiske bomstasjonene, fattet Datatilsynet høsten 2004 vedtak om at de helautomatiske bomstasjonene skal underlegges konsesjonsplikt. Vilkåret for å kunne gjøre dette, er at behandlingen *åpenbart vil krenke tungtveiende personverninteresser*. Etter Datatilsynets vurdering vil det være en åpenbar krenkelse av tungtveiende personverninteresser dersom det enkelte individ ikke selv kan velge hvorvidt man vil legge igjen spor om hvor man ferdes til hvilke tidspunkt langs norske veier. Med de løsninger som hittil har vært implementert tilbys trafikantene ikke løsninger som innebærer at de har et reelt valg, tatt hensyn til informasjon, tilgjengelighet, kostnader og funksjonell bruk.

Ved meldingsårets slutt var Datatilsynet fortsatt i dialog med Statens vegvesen når det gjelder å finne fram til en akseptabel løsning. Selv om det blir enighet om en teknisk løsning som ivaretar trafikantenes rett til å kunne ferdes sporfritt, vil Datatilsynet likevel innføre konsesjonsplikt for de helautomatiske bomstasjonene. Gjennom vilkår satt i konsesjon kan selskapene få felles regler for blant annet utlevering av personopplysninger, praktisering av innsynsretten og sletting av passeringsopplysningene. Datatilsynet erfarte gjennom sitt kartleggingsarbeide at dette håndteres ulikt i de forskjellige bompengeselskapene. Det er uheldig, tatt i betraktning at trafikanten, som følge av samordning selskapene imellom, kan benytte sin autopassbrikke også i andre bompengeselskaper enn sitt eget. Ensartete behandlingsrutiner vil skape forutberegnlighet for publikum.

Datatilsynet forutsetter at det ikke bygges ut nye helautomatiske bomstasjoner før det foreligger løsninger som gjør at trafikantene fortsatt kan ferdes langs norske veier uten å legge igjen detaljerte og personidentifiserbare passeringsopplysninger.

Mobiltelefon og posisjonering
Norge er på verdenstoppen når det gjelder utbredelse av mobiltelefoner og bruk av tilhørende tjenester. Denne teknologien forutsetter en automatisk utveksling av signaler, som kan gi muligheter til å kartlegge hvor innehaveren av telefonen faktisk befinner seg. Da melder spørsmålet seg straks: Hvor fritt kan disse lokaliseringsdataene brukes?

Et teknisk utgangspunkt
En mobiltelefon trenger trådløs kontakt med basestasjoner plassert på bakken for å kunne brukes. Basestasjonene kan på forespørsel kartlegge hvor telefonsettet fysisk befinner seg. Slike data kalles lokaliseringsdata. Posisjonens nøyaktighet avhenger blant annet av tettheten mellom basestasjonene. I bysentra, hvor basetettheten normalt er stor, kan lokaliseringen, slik den gjøres i dag, angis med inntil hundre meters nøyaktighet. Etter som nettverket bygges ut og moderniseres, kan stedsangivelsen bli stadig mer presis.

Den grunnleggende funksjonen for disse lokaliseringsdataene er å gi informasjon om hvor bæreren av mobilen befinner seg. Siden lokaliseringsdataene kan knyttes til enkeltpersoner (bæreren av mobilen), er de også å betrakte som personopplysninger, og bruken av disse dataene er underlagt personvernlovgivningen. Dette gir føringer for hvor lenge teleoperatørene kan lagre lokaliseringsdataene og hvordan de eventuelt kan utleveres til andre, for eksempel andre selskaper som tilbyr tjenester via mobiltelefon (innholdsleverandører).

Stor kommersiell interesse
Datatilsynet ser en betydelig økt interesse for bruk av lokaliseringsdata i kommersielt øyemed. Flere innholdsleverandører har forlengst lansert tjenester for sporing og gjenfinning av biler, båter og andre verdigjenstander via GSM. Det er for eksempel lansert tjenester som varsler mobilbrukeren om denne nærmer seg fotobokser langs veien, eller når man er i nærheten av en eller annen nærmere spesifisert tjeneste, for eksempel et underholdningstilbud.

Abonnentens egen, frivillige bruk
Når det gjelder kommersielle tjenester som mobiltelefonbæreren selv benytter seg av og har god informasjon om, vil personverntrusselen være relativt liten. Dette forutsetter imidlertid at man med vitende og vilje benytter tjenesten. Et eksempel på dette er den såkalte "buddy –tjenesten", levert av NetCom. Ved å sende en etterspørsel, kan man få en melding tilbake om hvor den etterspurte mobiltelefonbæreren fysisk befinner seg. Forutsetningen er imidlertid at begge har meldt seg på tjenesten, og i den forbindelse har samtykket til utlevering av lokaliseringsdataene. Dersom den etterspurte har meldt seg ut av tjenesten, vil posisjonen ikke lenger kunne utleveres til den som spør. Datatilsynet forutsetter ved slike tjenester at det med jevne mellomrom blir sendt varsel til den som blir lokalisert.

Lokalisere for å kontrollere
Det er imidlertid også flere eksempler på at lokaliseringsdata ønskes tatt i bruk i helt andre sammenhenger. Datatilsynet gav i en konkret sak utrykk for at et forsikringsselskap ikke kan basere seg på samtykke fra forsikringstakere til innhenting av lokaliseringsdata for å avdekke mulig forsikringsbedrageri. Tilsynet begrunnet dette med at et slikt samtykke i realiteten ikke vil være særlig frivillig. Det at forsikringstaker nekter å gi sitt samtykke til utlevering vil lett lede tankene til at vedkommende har noe å skjule. Dessuten ville forsikringsselskapet motta en mengde overskuddsinformasjon som er dem uvedkommende. Forsikringsselskapene bør i stedet overlate til politiet å innhente denne typen materiale.

Det er også lansert tjenester skreddersydd for at foreldre skal kunne lokalisere sine barn. Man kan da definere en sone som barnet er forutsatt å holde seg innenfor. Dersom signalene fra mobilen indikerer at barnet av en eller annen grunn har beveget seg utenfor den tillatte sonen, går et sms-varsel til foreldrene. Man har også tjenester hvor man kan følge med på Internett hvor mobilenheten til enhver tid befinner seg, vist som markører på detaljerte kart. Den samme typen tjeneste kan selvsagt benyttes også overfor andre familiemedlemmer. Ikke minst åpner også lokaliseringsteknologien for at arbeidsgivere kan få til en mest mulig effektiv drift og logistikk ('flåtestyring'). Imidlertid kan også posisjoneringsteknologien tas i bruk for å kontrollere at medarbeiderne til enhver tid er på de steder de, fra arbeidsgivers side, er forutsatt å være.

Hvor skal grensene settes?
De nye lokaliseringstjenestene reiser altså en rekke utfordringer som berører personvernet. Det går selvsagt en grense for hvor langt foreldre kan gå for å spore sine barn, eller for arbeidsgivere å spore sine ansatte. Men hvor skal streken settes? I tiden som kommer vil det bli nødvendig å foreta en rekke slike grenseoppganger, basert på helt konkrete tilfeller. Her vil ikke bare Datatilsynet måtte engasjere seg, men også arbeidstakerorganisasjoner, Arbeidstilsyn, Barneombud og så videre.

Utlevering og samtykke

Selv om begge de to store teleoperatørene i det norske markedet (Telenor og NetCom) naturlig nok selv er innholdsleverandører for mange mobiltelefontjenester, er det også en rekke andre selskaper som tilbyr ulike innholdstjenester basert på mobiltelefoni. Når det gjelder tjenester som forutsetter bruk av lokaliseringsdata, baserer både Telenor og NetCom, seg på at samtykke til utlevering og bruk av disse dataene innhentes via innholdsleverandørene. Det blir avtalefestet at det er innholdsleverandørene som står ansvarlig for at gyldig samtykke er innhentet fra kunden før lokaliseringsdata hentes ut fra teleoperatøren. Hos Telenor kan mobilabonnenten få sperret all utlevering av lokaliseringsdata, også selv om man tidligere har samtykket til slik utlevering via en eller flere innholdsleverandører. Hos NetCom har abonnenten ikke denne muligheten.

Oversiktlighet og enkelhet er en nødvendig forutsetning for at abonnenten skal kunne ha kontroll med opplysninger om seg selv, og hvor de tar veien. Datatilsynet har derfor pålagt begge teleoperatørene om å etablere løsninger som gjør det mulig for mobiltelefonabonnentene både å starte og stoppe muligheten til lokalisering direkte hos teleoperatørene. Mobilabonnenten må selv aktivere lokaliseringstjenesten før den kan tas i bruk.

Datatilsynet har også gjennomført tilsyn overfor to innholdsleverandører som henter lokaliseringsdata fra mobiloperatørene. De benyttet seg av forskjellige fremgangsmåter for innhenting av samtykke fra abonnentene, avhengig av hva slags tjenester de tilbyr. Datatilsynet venter med å følge opp innholdsleverandørene til etter at forholdet til teleoperatørene er avklart.

Kontantkort og trafikkdata
Hos mobiltelefonoperatørene ble det ved gjennomgang av sletterutinene avdekket at tilsynsobjektene oppbevarer trafikkdata knyttet til sine kontantkortkunder i tre til fem måneder. Kontantkort fungerer slik at sluttbrukeren fyller opp en "konto" knyttet til telefonnummeret med en sum penger. Kostnadene trekkes fortløpende fra kontoen etter hvert som kontantkortet benyttes. Teleoperatørene kan derfor ikke vise til faktureringshensyn som begrunnelse for at de lagrer trafikkdataene like lenge for kontantkundene som for øvrige abonnenter. På spørsmål fra Datatilsynet påberopte teleoperatørene seg imidlertid at andre hensyn lå bak den lange lagringstiden, blant annet tekniske forhold og forbrukerhensyn. Tilsynet sitter likevel igjen med et inntrykk av at også trafikkdataene for kontantkortkundene lagres fordi dette er det enkleste for teleoperatørene, rent teknisk og administrativt. Det er lettere å forholde seg til en felles lagringsrutine, enten man fakturerer for tjenesten eller ikke. Datatilsynet stiller seg derfor tvilende til om teleoperatørene har et tilstrekkelig saklig grunnlag for å lagre trafikkdataene fra kontantkort i den grad de gjør i dag, og vil følge opp saken.

8.6 KAMERAOVERVÅKING
Trenden fra tidligere års økning i bruk av kameraovervåking er ytterligere forsterket i 2004. Forbedret kvalitet på opptaksutstyret, økt tilgjengelighet, lavere pris og bredere funksjonalitet, gjør at kameraovervåking av mange blir sett på som et egnet virkemiddel for å forebygge og oppklare hærverk, vold og tyveri.

Dette gjelder både for tradisjonelle enkeltstående kameraer, men også som ledd i mer omfattende byggsikring hvor bruk av kamera utgjør en integrert del av et større overvåkingsanlegg. Det er også stadig mer vanlig at drift av overvåkingssystemet settes

bort til egne vaktselskaper. Dette kan både gjøres slik at vaktselskapet får online-tilgang til bilder eller slik at de kan gå inn og se på et opptak. I tilfeller hvor vaktselskapene har en større kundemasse, vil dette i praksis kunne innebære at disse får en større mulighet til å overvåke enn selv politiet har anledning til.

Det er også en klar tendens til at kameraovervåking tas i bruk på områder hvor dette hittil har vært begrenset. Eksempelvis er det som den klare hovedregel kun offentlige myndigheter/politiet som har adgang til å overvåke offentlige områder. Det er likevel stadig oftere aktører som ønsker å overvåke nettopp disse områdene.

Sentrumsgatene i Stavanger
En sammenslutning av butikkinnehavere i Stavanger iverksatte omfattende kameraovervåking i sentrumsområdet. Kameraene fanget opp egne butikkfasader, men også offentlige områder som vei og fortau utenfor butikkene. Området var merket, men ikke i henhold til personopplysningslovens regler. Det var dermed vanskelig å avdekke hvem som var ansvarlig for overvåkingen. Datatilsynet ga pålegg om at den delen av overvåkingen som går utover en ubetydelig del av gaten/fortauet måtte opphøre. Videre ble det stilt krav til tidsrommet for overvåkingen og til merkingen av området.

NSB og Oslo Sporveier
Et annet eksempel er overvåking i offentlige transportmidler. Datatilsynet gjennomførte et tilsyn hos NSB av et prøveprosjekt med kameraovervåking på to lokale togsett. I tillegg ble det foretatt et tilsyn hos Oslo Sporveier som benytter kameraovervåking på Sporveisbussene. Verken trikker eller T-baner har kameraovervåking ombord.

Formålet med overvåkingen er å oppnå en preventiv effekt og å oppklare hærverk. Sentralt står også sikkerhet overfor ansatte og passasjerer i forbindelse med for eksempel voldsepisoder eller ran. To viktige og tungveiende hensyn må her vurderes opp mot hverandre: På den ene siden står hensynet til ivaretakelse av de ansattes liv og helse i tillegg til passasjerenes behov for trygghet. På den andre står behovet for ikke å være under kontinuerlig overvåking.

På denne bakgrunnen har Datatilsynet varslet både NSB og Sporveiene om at det ikke er akseptabelt å overvåke passasjerområdet, dvs kupeene og bussetene. Saken er ikke endelig avsluttet og Datatilsynet antar at saken vil ende som klagesak for Personvernnemnda.

Ny teknologi
Sammen med den sterke veksten i utbredelsen, er det økt funksjonalitet ved ny teknologi som representerer de største truslene og utfordringene for personvernet. Digitaliseringen av hverdagen gjelder også innen kameraovervåking. Digitale overvåkingssystemer selges over disk til en lav pris, og praktisk talt enhver kan sette opp et overvåkingssystem tilknyttet en PC, og dermed ofte også Internett. Datatilsynet ga i 2004 blant annet en arbeidsgiver varsel om pålegg, etter at han hadde la både lyd og bilde fra overvåkingsutstyr ”live” ut på Internett. Enhver kunne dermed i prinsippet både se og høre de ansatte via nettet.

Ny teknologi medfører en utbredelse hvor den som setter et overvåkingsanlegg i drift, ikke kan forventes å ha nødvendig kjennskap til regelverkets krav vedrørende overvåking og de nye sikkerhetsutfordringene som digitaliseringen innebærer. Tilrettelegging av digitale systemer gir mulighet for at bruken av opplysningene går utover det som anses som

kameraovervåking, nemlig digital bearbeiding. Digital bearbeiding benyttes i dag aktivt i mange systemer for å detektere uønsket atferd i et overvåket område, eksempelvis ved at det går en alarm til vaktpersonalet dersom noen klatrer på et gjerde, eller ved uventede ansamlinger av personer. Enkelte av disse egenskapene realiseres også i analoge overvåkingssystemer.

Gjenkjenningsteknologi er det neste steget. Det finnes i dag gratis programvare som muliggjør pålogging til din personlige PC ved hjelp av ansiktsgjenkjenning. Mer inngripende er det hvis dette settes i system i et overvåkingsanlegg. Det kan virke hensiktsmessig at kjøpmannen blir alarmert dersom en kjent, men uønsket, kunde dukker opp i butikken. Faren er at det moderne kameraovervåkingssystemet kan benyttes stigmatiserende.

Det er ikke vanskelig å se at overgangen til digitale systemer omfatter mer enn hva regelverket betrakter som kameraovervåking. Den som velger å sette opp disse systemene må vurdere om man befinner seg innenfor kategorien kameraovervåking, eller om man gjennom overvåkingen foretar en annen behandling av personopplysninger. Dersom man havner utenfor det tradisjonelle kameraovervåkingsbegrepet, må man sørge for at det foreligger et annet lovgrunnlag for denne behandlingen.

Begrensede utleveringsmuligheter

En konsekvens av økt overvåking er at risikoen øker for at opptak kommer på avveie eller utleveres. Ved at stadig flere områder er overvåket øker også muligheten for at den aktuelle hendelsen fanges opp av et kamera. Videoopptak av ulike hendelser, som ran eller ulykker, vil kunne være av stor interesse for ulike medier ettersom live-opptak antas å ha en betydelig dramatiserende effekt. Etter gjeldende regler forutsetter dette enten at den avbildede samtykker til utleveringen, eller at utleveringsadgangen følger av lov.

Videoen fra Plata

Problemstillingen ble aktualisert sommeren 2004 da Politiets særskilte etterforskningsorgan (SEFO) mente at Oslopolitiet brøt personopplysningsloven da usladdede overvåkingsbilder av narkomane på "Plata" i Oslo ble frigitt og senere vist på NRK. Det vil i slike saker være selve utleveringen av opptakene som er ulovlig etter personopplysningsloven. Det forhold at opptakene senere publiseres i media er unntatt fra personopplysningsloven selv om de aktuelle bildene er fremskaffet på ulovlig vis. Begrensninger i publiseringsadgangen av slikt materiale vil eventuelt følge av annet regelverk, for eksempel Vær Varsom-plakaten.

Overvåking av arbeidsplassen
Kameraovervåking er en særlig belastning på områder hvor ansatte oppholder seg store deler av arbeidstiden. Lovverket oppstiller skjerpede krav til overvåking som gjøres på slike områder. Datatilsynet har likevel mottatt en rekke henvendelser fra ansatte i virksomheter som benytter kameraovervåking. Eksempel på enkeltsaker fra 2004 om overvåking på arbeidsplassen:

Nesset kommune
Datatilsynet ble gjort oppmerksom på at en Nesset kommune benyttet kameraovervåking for å avsløre tyveri fra diverse felleskasser på arbeidsplassen. Kameraovervåkingen var ikke skiltet, men ansatte med tjenstlig adgang til det aktuelle området ble muntlig informert. Datatilsynet konkluderte med at dette ikke tilfredsstilte kravet til nødvendig varsling og at overvåkingen dermed fremsto som skjult. Tilfellet var også et brudd på prinsippet om at overvåking som hovedregel bare skal foretas i preventiv hensikt, og at det kun er politiet som er tillagt oppgaven med å innhente bevis til bruk i straffesaker.

Politiet forfulgte saken på selvstendig grunnlag og utferdiget et forelegg til kommunen på ti tusen kroner for ulovlig overvåking. Kommunen vedtok forelegget.

Bakehuset Kafe
Datatilsynet foretok etterkontroll ved Bakehuset Kafe i Bærum. Kafeen var også blitt kontrollert i 2002. Den gang overvåket arbeidsgiver deler av de ansattes arbeidsområder. Virksomhetens begrunnelse ble den gang akseptert under noe tvil, men forutsatt at overvåkingen ikke skulle være permanent og behovet vurderes løpende.

Etterkontrollen avdekket at virksomheten nå i stedet hadde utvidet overvåkingen slik at den omfattet størstedelen av arbeidslokalene. De ansatte var dermed under permanent overvåking. Datatilsynet påla virksomheten å stanse overvåkingen med unntak av områder hvor behovet for overvåking er godt begrunnet og dokumentert. Vedtaket er anket inn for Personvernnemnda.

Delegasjon av tilsynsansvar
Det er vanskelig å gi noe sikkert anslag over antall kameraovervåkingssystemer i Norge, ettersom meldeplikten til Datatilsynet etterleves i svært begrenset grad. Datatilsynet har mottatt totalt 2 015 meldinger om kameraovervåking. Av disse er 1 006 meldt i 2004. Det er grunn til å anta at det reelle antall overvåkingssystemer er langt større. Av ressursmessige årsaker blir dermed Datatilsynets kontroll med kameraovervåkingen nødvendigvis sporadisk.

Dette er en av grunnene til at Datatilsynet, i samarbeid med Justisdepartementet har fremmet forslag om å overføre ansvar for kontroll og tilsyn med kameraovervåking til de kommuner som ønsker det. Dette vil gjelde kameraovervåking innen kommunens grenser. Slik vil kommunene få et større ansvar for, og mulighet til, å ta del i utviklingen av personvernet innenfor kommunens grenser. En omlegging vil også kunne innebære en ikke ubetydelig økning i det totale antallet tilsyn med aktører som utøver kameraovervåking, i tillegg til å heve den lokale interessen for problemstillingene.

8.7 JUSTISSEKTOREN

I hvor stor grad staten skal ha mulighet til å innskrenke individenes integritet er et helt grunnleggende viktig tema når det gjelder bruk av politimetoder for å oppklare og forebygge kriminalitet. Det er et åpenbart dilemma at de som samfunnet i første rekke ønsker å ramme med nye og utvidede politimetoder, de mest ressurssterke og farlig kriminelle, raskt vil tilpasse seg den nye virkeligheten. På denne måten kommer samfunnet inn i en ond sirkel, der politiet ser behov for å ta i bruk stadig mer inngripende og integritetskrenkende metoder. Datatilsynet er også betenkt over den økende usynliggjøringen av politiet og deres metoder, i en tid hvor de fleste politikere tar til orde for et mer synlig politi.

Politimetodeutvalget

Politimetodeutvalgets rapport *Mellom effektivitet og personvern* (NOU 2004:6) ble lagt frem våren 2004. Juridisk seniorrådgiver i Datatilsynet Guro Slettemark var oppnevnt som utvalgsmedlem. Hun hadde grunnleggende dissenser i forhold til flertallets forslag og var representert i utvalgets mindretall, som også kom med et eget lovforslag. I Datatilsynets senere høringsuttalelse ble det særlig reagert på forslagene om dataavlesing og romkontroll.

Forebygging av kriminell aktivitet innebærer at politiet innleder en form for etterretning før handlingen faktisk finner sted. Forebyggingsarbeidet kan dermed føre til at politiet samler inn informasjon om mennesker som ikke har gjort noe kriminelt, og som kanskje heller ikke vil komme til å gjøre det.

Å forene personvern og politiets behov for nye metoder for forebygging av straffbare handlinger er vanskelig. Metodene som politiet benytter seg av vil i seg selv kunne føre til alvorlige krenkelser av personvernet og andre verdier som er sentrale i en rettsstat.

Dataavlesing –et inngrep i tanken?

Dataavlesing er en svært integritetskrenkende metode. Metoden innebærer at informasjon som ikke er kommunisert kan bli gjenstand for politiets nærmere undersøkelse. Dette kan for eksempel skje ved at politiet installerer en spionprogramvare på vedkommendes datamaskin. Programmet registrerer hvert eneste tastetrykk, også tekst og tall som brukeren senere sletter. Programmet sender alle disse detaljregistreringene fortløpende til politiet. Alt dette foregår uten at eier og bruker av datamaskinen er klar over det.

Ved bruk av denne metoden kommer man i inn på et rettssikkerhetsmessig meget problematisk område. Tanker, assosiasjoner og ønsker, som kanskje aldri engang var tenkt kommunisert til andre, skal bidra til å bevise noens skyld. Da må vi stille oss spørsmålet: Hvem kan egentlig være i stand til å vurdere hvorvidt det ene tankesettet er mer mistenkelig enn det andre?

Et annet grunnleggende problem er de store mulighetene for at også uskyldige blir rammet ved bruk av metoden. Det kan være mange brukere av en datamaskin. Dermed vil også familiemedlemmer, arbeidskollegaer og andre som overhodet ikke har noe med en mulig kriminell handling å gjøre bli utsatt for politiets direkte overvåking.

Datatilsynet mener at behovet for, og konsekvensene av dataavlesing er så mangelfullt utredet at metoden ikke bør aksepteres tatt i bruk.

Også spørsmålet om romkontroll (romavlytting) innebærer mange av de samme problemstillingene som dataavlesing. Datatilsynet ser også her åpenbare problemer i forhold til uskyldige tredjepersoner, og opphopning og bruk av overskuddsinformasjon.

PSTs særlige behov
Politimetodeutvalgets flertall ønsker at også det alminnelige politiet skal få tilgang til de fleste ekstraordinære metodene som foreslås. Datatilsynet er enig med utvalgets mindretall som hevder at Politiets sikkerhetstjeneste (PST) trenger bedre hjemler for sine eksisterende metoder, samt å få lovfestet også nye metoder. Det alminnelige politiet har imidlertid ikke et tilsvarende behov som PST og bør dermed heller ikke gis de samme mulighetene.

Et paradoks
For Datatilsynet er det et paradoks at mens det ropes etter stadig nye og mer inngripende politimetoder for å avdekke alvorlig kriminalitet, kan de kriminelle miljøene i ro og mak lytte til politiets kommunikasjonssamband, for dermed å følge med i hva politiet til enhver tid foretar seg. Datatilsynet kan ikke se at en stadig utvidelse av politiets hjemler er det riktige svaret på behovet for et tryggere samfunn. Det er allment kjent at politiet ikke har tatt i bruk mange av de metodene som de tidligere har bedt om og fått lovhjemlet. Datatilsynet ser også en fare for at de uskyldige overvåkes stadig tettere, mens de kriminelle tilpasser seg og finner nye måter å drive sin virksomhet på.

Hjemler
Datatilsynet er enig med Politimetodeutvalget i at dagens metodebruk bør få klarere lovhjemler. Jo mer inngripende en metode er, jo klarere lovhjemmel bør den ha. Det bør også være forutsigbart i rimelig grad for den enkelte under hvilke omstendigheter man kan risikere å bli utsatt for politiets metodebruk. Behovet for metodebruken må også dokumenteres, slik at man i etterkant kan sjekke om inngrepet var berettiget.

Underretning om bruk av metoder
Prinsippet om underretning er et viktig verktøy for den enkelte til å ivareta sin egen rettssikkerhet. Politiets metodebruk blir mer og mer teknologisk sofistikert, og sjansen for at metodebruken ikke kommer den enkelte til kunnskap gjennom en straffeprosess, vil alltid være tilstede der metoder benyttes i forebyggende øyemed. Grunnleggende prinsipper som rett til innsyn og underretning til de berørte, i det minste i ettertid, må være et vilkår for å tillate metoden. Unntak eller utsettelse av disse rettighetene bør avgjøres av en domstol.

Ny lov om politiregistre
Også forslaget til ny politiregisterlov tar opp sentrale spørsmål om hvordan politiets informasjonstilfang bør reguleres. Ikke minst er det helt sentralt å ta stilling til hvilke rettigheter borgerne skal innrømmes i forhold til å få innsyn i, og kontrollere kvaliteten på den informasjonen politiet samler inn.

Politiregisterutvalgets utredning *Kriminalitetsbekjempelse og personvern* (NOU 2003: 21) ble sendt på høring i meldingsåret. Datatilsynets avdelingsdirektør Knut B. Kaspersen satt som medlem i utvalget. Utvalgets innstilling var enstemmig.

Rettstilstanden når det gjelder personvernlovgivningen på politisektoren er i dag uklar. Datatilsynet har derfor i flere år etterlyst et bedre lovgrunnlag for politiets innsamling, lagring, bruk og utlevering av personopplysninger. Etter Datatilsynets vurdering er

utvalgets utredning og lovforslag godt gjennomarbeidet og personvernet gjennomgående ivaretatt. Datatilsynet hadde likevel noen prinsipielle merknader til utredningen.

Ansvar for behandling av personopplysninger i politiet
Det må være avklart og tydelig presisert hvilket nivå innad i politiet som har ansvar for behandling av personopplysninger. Den som pålegges ansvaret må være godt kjent med, og føle en nærhet til det foreslåtte lovverket. Innenfor politiet er dette ekstra viktig, da de fleste av politiets registre er sentralisert. Datatilsynet mener at politimesteren i det enkelte politidistrikt må tillegges dette ansvaret.

Personvernombud
Datatilsynet har i flere sammenhenger tatt til orde for at det bør utnevnes personvernombud innen politiet. Tilsynet er derfor tilfreds med at utvalget har kommet med forslag om dette. Imidlertid burde ordningen ha blitt tillagt større vekt i forslaget til ny politiregisterlov. Hvert politidistrikt bør ha sitt eget personvernombud. Det kan også vurderes å gi personvernombudet avgjørelsesmyndighet når det gjelder bruk av politimetoder som ikke krever rettens kjennelse.

Individets rettigheter
Rettigheter knyttet til innsyn, retting og sletting av opplysninger som angår en selv, er helt grunnleggende personvernprinsipper. Det er derfor av stor rettssikkerhetsmessig betydning at den berørte gis mulighet til å få kunnskap om at vedkommende er registrert hos politiet. Dette gjelder også selv om man ikke får vite meningsinnholdet, eller om kunnskapen gis først i ettertid. Retten til innsyn, retting og sletting må derfor etter Datatilsynets vurdering gjenspeiles i den nye politiregisterloven.

Datatilsynets rolle
Lovforslaget presiserer Datatilsynets kompetanse i forhold til klagesaker og generelle kontrolloppgaver. En presisering av Datatilsynets oppgaver i forhold til politiet er et skritt i riktig retning. Datatilsynet er imidlertid kritisk til forslaget om at tilsynet skal få tilgang til hva som er registrert om en person, uten at de samme opplysningene skal kunne videreformidles til vedkommende. Det legges i stedet opp til at Datatilsynet må nøye seg med å avgi en erklæring om at politiets behandling av personopplysninger eventuelt er tilfredsstillende. Dette er ingen ønsket situasjon for en institusjon som legger stor vekt på hensynet til den personlige integritet og at den enkelte selv skal kunne kontrollere opplysningene som er registrert om seg. Tilsynsoppgaven vil også bli vanskelig å utøve på en tilfredsstillende måte dersom Datatilsynet ikke kan følge opp eventuelle avdekkede avvik med å gi politiet pålegg. Tilsynshjemmelen blir, sett i denne sammenheng, ufullstendig og lite slagkraftig.

Sikring av politiets nødsamband
I 2001 trådte en lovendring i kraft som førte til at det ikke lenger er ulovlig å lytte på politiets radiosamband. Politidirektoratet orienterte derfor politienhetene om hvordan de skulle forholde seg til bruken av radiosambandet. Det ble særlig pekt på at man fortsatt må forholde seg til taushetsplikten. Det ble oppfordret til bruk av alternative kommunikasjonsmetoder, slik som mobiltelefon eller avlytningssikkert (kryptert) samband.

I kjølvannet av denne lovendringen har det oppstått en ny problemstilling ved at kommunikasjonen fra politisambandet også er blitt videreformidlet og lagt ut på Internett. Personopplysninger blir dermed gjort tilgjengelig for en ubegrenset krets av personer. Politidirektoratet mente at en slik videreformidling under enhver omstendighet er kritikkverdig, og oppfordret Justisdepartementet, Post- og Teletilsynet og Datatilsynet om å vurdere saken nærmere.

Brudd på taushetsplikt
Datatilsynet kom til at videreformidlingen er i strid med personopplysningsloven. Tilsynet deler også Politidirektoratets oppfatning av at formidling av informasjon som andre kan ta del i, er brudd på politiets taushetsplikt. Det ble derfor gitt pålegg til politiet om at personopplysninger ikke skal kommuniseres over det åpne radiosambandet. Datatilsynet er for øvrig tilfreds med Stortingets beslutning om å etablere et nytt nødsamband. Dette ser ut til å kunne oppfylle de krav som Datatilsynet har stilt.

DNA og biologisk materiale
DNA-profiler har blitt et stadig viktigere bevis i straffesaker. På grunn av ny kunnskap og bedret teknologi er det mulig å få ut stadig mer informasjon, ikke bare om de personene som biomaterialet er hentet fra, men også om deres slektninger. Disse nye mulighetene stiller samfunnet overfor store etiske og personvernmessige utfordringer.

Regjeringen har derfor nedsatt et utvalg for å vurdere om adgangen til å ta DNA-prøver skal utvides, for eksempel slik at adgangen blir den samme som for fingeravtrykk. I tillegg skal utvalget vurdere om det skal åpnes for å registrere DNA-profiler i flere typer av saker og hvorvidt siktelse skal være et tilstrekkelig vilkår for å registrere vedkommendes DNA-profil. I dag kreves rettskraftig domfellelse. Utvalget skal også vurdere eventuelle endringer i saksbehandlingsreglene for registrering og søk i DNA-registeret.

Datatilsynets direktør er oppnevnt som utvalgsmedlem. Utvalget skal sluttføre sitt arbeid innen utgangen av 2005.

Politiets tilgang til biobanker
Interessant fra et personvernperspektiv er også en lovtolkningssak fra Justisdepartementet som konkluderer med at politiet ikke uten videre skal ha tilgang til biologisk materiale som ligger lagret i biobankene. Tolkningen gjelder biologisk materiale lagret med hjemmel i biobankloven, det vil hovedsakelig si prøver tatt i behandlings- eller forskningsøyemed. Justisdepartementets lovavdeling understreker at bruk av biologisk materiale er omfattet av strenge vilkår i biobankloven, og kan ikke se at det er lovgrunnlag for regulær tilgang til biologisk materiale for å identifisere personer i forbindelse med straffesaker. Kun unntaksvis, i tilfeller der politiet kan påberope seg nødrett, kan det være aktuelt å kreve tilgang på materialet, selv om det i utgangspunktet er i strid med loven. Lovavdelingen understreker imidlertid at det skal mye til før nødrett kan hjemle handlinger som er i strid med en klar lovbestemmelse.

En slik situasjon mente Datatilsynet forelå helt på slutten av meldingsåret. Det ble i forbindelse med flomkatastrofen i Asia gitt tillatelse til at biologisk materiale fra mor og barn-undersøkelsene kunne benyttes til identifikasjon av ofre etter flomkatastrofen i Asia.

Nye mobile fartsmålere i politiet
Politiets data- og materiellteneste kontaktet Datatilsynet for å få en vurdering av et prøveprosjekt der nye mobile fartsmålere med nummergjenkjenning er under uttesting. Datatilsynet har gitt politiet tilbakemelding om at det nye systemet må vurderes opp mot politiets hjemler for å drive fartskontroll. Datatilsynet setter spørsmålstegn ved om det i vegtrafikkloven er et tilstrekkelig hjemmelsgrunnlag for bruk av den nye typen målerutstyr. Dette må avklares før utstyret eventuelt taes i bruk.

Formålet må være utvetydig
Utstyret vil kunne anvendes for to ulike formål nemlig fartskontroller og nummergjenkjenning. Ved fartskontroller vil funksjonen nummergjenkjenning være en del av kontrollen. Nummergjenkjenningen vil imidlertid også kunne anvendes som en separat funksjon, for eksempel i forbindelse med ettersøking av bestemte kjøretøy. Dersom politiet ønsker å ta i bruk utstyret til begge formål, må det også foreligge et hjemmelsgrunnlag som dekker begge de ulike formålene.

Utstyret inkluderer også en digital billedfunksjon. Denne vil ikke falle inn under personopplysningslovens bestemmelser om kameraovervåking. Hjemmelsgrunnlaget for denne billedtakingen må derfor søkes i annet regelverk.

Risikomomenter
Tendensen til at politiets utstyr i økende utstrekning blir mobilt, stiller andre og helt nye krav både til både lovgivning og informasjonssikkerhet. Personvernhensyn og kravet til forutberegnelighet for den enkelte må alltid være sentrale elementer ved innføring av nye systemer. Klare lovhjemler må derfor være et minimumskrav.

Nummergjenkjenningsfunksjonen innebærer et stort overvåknings- og misbrukspotensiale. Dette gjelder i forhold til hvilke registre systemet kan kobles opp mot, men også ved at bruker av utstyret systematisk kan spore kjøretøyer ved å utplassere dette på flere steder. En generell risiko som følger enhver anskaffelse av teknisk mer avansert utstyr er dessuten at de nye mulighetene i seg selv vil øke bruken av utstyret. Samtidig vil det bli et press for å kunne ta utstyret i bruk for andre formål enn hva det opprinnelig ble anskaffet for.

Saken ble ikke endelig avklaret i meldingsåret.

Sikkerhetsklarering
En arbeidsgruppe nedsatt av Forsvarsdepartementet foreslo blant annet lovhjemmel for bruk av lyd- og bildeopptak i forbindelse med sikkerhetsklarering. Datatilsynet mener at søkere for sikkerhetsklarering bør kunne få innsyn i slike opptak av sikkerhetssamtaler. I sin høringsuttalelse etterlyste Datatilsynet også en drøftelse av kvaliteten i de registrene som sjekkes ved sikkerhetsklarering.

Forslagene arbeidsgruppen la frem kom som et resultat av at Stortingets EOS-uvalg har satt søkelyset på rettssikkerheten til den enkelte som søker sikkerhetsklarering. Utvalget uttrykte at det må stilles strenge krav til saksbehandlingen, og ønsket særlig bedrede innsynsmuligheter.

Opptak av sikkerhetssamtale
Opptak av sikkerhetssamtaler er begrunnet med rettssikkerhetshensyn. Likevel kom

arbeidsgruppen til at innsyn i opptakene ikke skulle gis. Datatilsynet støtter ikke dette synspunktet. Innsyn i opplysninger som angår en selv er en viktig rettsikkerhetsgaranti. I dette tilfellet er opplysningene opptak av hva man faktisk har sagt og gjort. Datatilsynet ser det som underlig at man velger å begrunne et tiltak med hensyn til rettssikkerhet, samtidig som man eliminerer et svært viktig aspekt nettopp ved rettssikkerheten.

Hvor korrekte er registrene?
Når en sikkerhetsklarering vurderes, konsulteres en rekke registre for å finne opplysninger om søkeren. Arbeidsgruppen drøftet kun spørsmålet om disse registrenes kvalitet i saker der det kan være aktuelt å nekte klarering på grunn av økonomiske forhold. Dette begrunnes med at kredittopplysningsbyråenes registre ikke alltid er oppdatert. Problemet med manglende kvalitet kan imidlertid være like utbredt i de andre registrene som benyttes i klareringssaker.

Kvalitetsnivået i kredittopplysningsforetakenes registre er godt kjent. Årsaken er den åpne bruken av registrene, og at det gis gjenpart til den registrerte. Feil er dermed relativt lette å oppdage. Opplysninger i politiets registre er imidlertid skjult for vedkommende. Man har dermed ikke de samme mekanismene for å få verifisert opplysningene. Denne situasjonen gjør det viktig å kvalitetssjekke også opplysninger av ikke-økonomisk karakter som benyttes i en klareringssak.

Underretning til berørte
Datatilsynet er også opptatt av at det skal gis underretning til søkere som har blitt sikkerhetsklarert.

Lagringsplikt for tele- og internettrafikk?
Å pålegge teleoperatørene en lagringsplikt for trafikkdata har lenge vært et omdiskutert tema både i Norge og ellers i Europa. Terrorangrepet i Madrid utløste et nytt politisk press på EU-nivå om å avklare forholdene rundt slik datalagring. På EU-toppmøtet i mars 2004, ble det besluttet at et forslag om dette skal utarbeides og vedtas senest juni 2005. Storbritannia, Sverige, Irland og Frankrike kom senere med et forslag til rammevedtak. Dette ble i desember 2004 drøftet av EU's justisministre. Forslaget innebærer at data fra "allment tilgjengelige kommunikasjonstjenester" skal lagres i 12-36 måneder. Forslaget innskrenker seg dermed ikke til telefoni. Også datatrafikk inngår, det vil si opplysninger om hvilke nettsteder du har besøkt og til hvilke adresser du har sendt e-post. I tillegg handler det ikke bare om bruke tele- og trafikkdataene til å oppklare, men også til å forebygge kriminalitet.

Forslaget til rammevedtaket gjelder det såkalte tredjepillars-samarbeidet, (Justis- og sikkerhetsområdet i EU). Det omfattes dermed ikke av EØS-samarbeidet. Likevel må det, dersom forslaget går igjennom, forventes et sterkt press også på norske myndigheter for å innordne seg det samme regelverket. Også flertallet i politimetodeutvalget foreslo at politiloven skal få bestemmelser om lagringsplikt. Datatilsynet gikk i sin høringsuttalelse mot dette forslaget. Tilsynet ser behov for å utrede spørsmålet nærmere og etterspør en re-oppnevning av Datakrimutvalget. Dette utvalget hadde, i motsetning til Politimetodeutvalget, i sitt mandat å vurdere spørsmålet om lagringsplikt.

Brudd på menneskerettighetene

Det er et grunnleggende personvernprinsipp at opplysninger som er ment å skulle brukes for ett formål, ikke skal brukes til andre formål. Når formålet er oppfylt, skal opplysningene slettes.

Lagring av trafikkdata ut over det som er nødvendig for gjennomføring av tjenesten, vil bety at det lagres mange trivielle opplysninger om mange abonnenter. Store mengder informasjon om en hel befolknings bruk av elektronisk kommunikasjon vil bli lagret, for at en liten del som gjør noe kriminelt skal kunne etterforskes mer effektivt. Dette rokker ved den grunnleggende rett det er å kunne bevege seg fritt uten at man blir iakttatt.

De europeiske datatilsynsmyndighetene har derfor, gjennom sitt samarbeidsorgan "artikkel 29-gruppen", rettet en skarp kritikk mot forslaget om lagringsplikt. I en felles kunngjøring hevder tilsynsmyndighetene at hele forslaget strider mot den europeiske menneskerettskonvensjonens artikkel 8, hvor det heter: *"Enhver har rett til beskyttelse for sitt privatliv og familieliv, sitt hjem og sin korrespondanse".*

Amerikanernes krav om utlevering av passasjeropplysninger
Saken ble utførlig omtalt i årsmeldingen for 2003. Amerikanernes krav ble innfridd ved en Kommisjonsbeslutning i 2004. De europeiske datatilsynsmyndighetene har utformet retningslinjer for å sikre at passasjerene gis tilstrekkelig informasjon om hvilke opplysninger som blir overført til amerikanerne og hva de skal brukes til. For Norges del vil kommisjonsbeslutningen bli en del av norsk regelverk, med mindre Norge reserverer seg mot beslutningen. I et brev til Justisdepartementets lovavdeling har Datatilsynet tatt til orde for en slik reservasjon.

Politisamarbeid over landegrensene
Innen EU har det vært stor aktivitet i forhold til økt samarbeid mellom medlemslandenes politimyndigheter. Etter terroranslaget i Madrid i mars 2004, er det kommet en rekke forslag fra EU om effektivisering og tettere samarbeid mellom politimyndighetene. I et personvernperspektiv ligger de største utfordringene i ønsket om økt utveksling av personopplysninger over landegrensene. På det politioperative, administrative og politiske plan i Norge, er interessen meget stor for et tett samarbeid med EU. Dette er en bekymringsfull utvikling både ut i fra grunnleggende demokratiske og personvernmessige hensyn.

For Norges vedkommende har det vist seg relativt enkelt å få delta i det operative samarbeidet mer eller mindre på lik linje med EU-landene ved inngåelse av samarbeidsavtaler. Når det kommer til de organer som skal sikre individenes rettigheter og føre kontroll med politisamarbeidet, har Norge imidlertid ikke blitt innrømmet deltagelse. Et godt eksempel på dette er Europol-samarbeidet, der Norge ikke deltar i det felles tilsynsorganet Joint Supervisory Body (JSB). Datatilsynet har også tidligere uttrykt bekymring over dette.

Schengen informasjonssystem
JSA er det felles tilsynsorgan for Schengen informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengenområdet, eller er straffedømt i et av medlemslandene. Datatilsynet møter med en fast observatør. JSA hadde i 2004 et høyere aktivitetsnivå enn vanlig. Dette skyldes hovedsakelig generelt stor aktivitet innen Schengensamarbeidet. JSA

har i tillegg hatt fellesmøter med tilsynsorganet for Europol, og tilsvarende når det gjelder tollssamarbeidet.

JSA har særlig hatt fokus på personvernutfordringene i forhold til forslag om utvidelse av Schengen informasjonssystem (SIS). I mai avga JSA en offentlig uttalelse om utviklingen. JSA stiller seg kritiske til at flere etater skal få tilgang til opplysningene som er registrert i SIS. Dette øker faren for at opplysningene vil bli brukt til andre formål enn de opprinnelig var innsamlet for. JSA er også bekymret for det presset som hele tiden er der for å innta nye kategorier av opplysninger i Schengen informasjonssystem. Det advares mot en utvikling der selve formålet med systemet ikke lenger er retningsgivende for hvilke opplysninger som kan registreres. I stedet legger man vekt på hvilke muligheter som finnes til å legge inn nye kategorier av opplysninger. Biometriske data er et eksempel på nye kategorier som ønskes registrert.

Samarbeidsavtale med Eurojust
Datatilsynet er i en viss utstrekning blitt rådført i forbindelse med forhandlinger om inngåelse av samarbeidsavtale med Eurojust (samarbeid på påtalesiden innen EU). Som et viktig premiss for Stortingets behandling av spørsmålet om avtaleinngåelse, er Datatilsynet opptatt av at det foretas nødvendige avklaringer rundt individenes rettigheter, herunder at norske borgere sikres et like godt personvern som EUs borgere. En annen utfordring er at personopplysningsloven har et svært begrenset virkeområde. Denne kan derfor ikke anvendes som sikkerhet for ivaretakelse av individenes rettigheter i forbindelse med Eurojust.

8.8 ARBEIDSLIV

I likhet med tidligere år er problemstillinger knyttet til personvern i arbeidslivet et av de områdene hvor Datatilsynet mottar flest henvendelser fra publikum. Henvendelsene fordeler seg jevnt mellom arbeidsgiver- og arbeidstakersiden og dreier seg i stor grad om arbeidsgivers innsyn i e-post og internettlogger, kontroll av telefonbruk, kameraovervåking og opptak av telefonsamtaler. Siden mange av henvendelser også dreier seg om forhold som ligger i grenselandet mellom personopplysningsloven og arbeidsmiljøloven har Datatilsynet etablert en nærmere dialog med Direktoratet for arbeidstilsynet. De to tilsynsetatene utveksler informasjon om aktuelle saker, blant annet om bruk av vandelsattester, rusmiddelkontroll og ulike typer arbeidsmiljøundersøkelser.

Felles nordisk tilsynsprosjekt
Det nordiske Datatilsynssjefsmøtet besluttet i 2003 at det skulle gjennomføres et samnordisk tilsynsprosjekt for å se nærmere på behandling av personopplysninger i tilsettingsprosesser. Det ble for Norges del gjennomført tilsyn mot vaktselskapene Falck Norge AS og Securitas AS. I tillegg også mot teknologikonsernet Nokia Norge.

Manglende sletting av personopplysninger
Et trekk som gikk igjen i de tre kontrollerte virksomhetene var at det manglet retningslinjer for ivaretakelse den enkeltes rett til innsyn i registrerte opplysninger. Det forelå heller ikke tilfredsstillende rutiner for retting og sletting av personopplysninger. Alle de tre selskapene oppbevarte opplysninger i personalmappene som skulle ha vært slettet. Hos begge vaktselskapene lå også tidligere innhentede politiattester fortsatt lagret i personalmappene. Dette strider mot lov om strafferegistrering og kravene til sletting i personopplysningsloven. Formålet med politiattesten er oppfylt så snart det er godtgjort at

den tilsatte har tilfredsstillende vandel. Politiattesten skal deretter makuleres. Av andre opplysninger som burde vært slettet var blant annet svært gamle advarsler og sykmeldinger. De tre virksomhetene fikk pålegg om å gjennomgå personalmappene for å slette unødige personopplysninger. De ble også pålagt å utforme skriftlige rutiner for innsyn, retting og sletting.

Securitas har anket pålegget om å makulere tidligere innhentede politiattester inn for Personvernnemnda.

Egenerklæring om vandel
Vaktselskapene har gjennom Lov om vaktvirksomhet med forskrift hjemmel til å innhente politiattest. Attesten viser om søkeren tidligere har vært straffet eller bøtelagt, eller om vedkommende er under etterforskning.

Securitas innhentet i tillegg egenerklæringer om vandel. Her ble søkerne bedt om å redegjøre for forhold som går ut over de opplysningene som fremgår av politiattesten.

Dette er en tendens Datatilsynet har sett også hos arbeidsgivere i andre bransjer, som ikke har anledning til å innhente politiattest. I mangel av nødvendig lovhjemmel ber arbeidsgiver jobbsøkere og ansatte om at de i stedet fyller ut egenerklæringer om vandel, for eksempel om vedkommende noen gang har vært mistenkt eller anklaget for mulige straffbare forhold. Innhenting av denne typen egenerklæringer innebærer etter Datatilsynets vurdering en omgåelse av lovgivers intensjoner med å begrense tilgangen til vandelsopplysninger.

Datatilsynet påla Securitas å avvikle ordningen med å innhente egenerklæring om vandel.

Egenerklæring om helse
Securitas benyttet også en meget omfattende egenerklæring om helse, hvor søkeren ble bedt om å oppgi opplysninger om blant annet syn, hjerteproblemer og kondisjon.

Datatilsynet ga vaktselskapet pålegg om å avslutte innhentingen av helseopplysninger via egenerklæring. Etter å ha vært i en etterfølgende dialog med Securitas har Datatilsynet omgjort vedtaket, slik at enkelte relevante helseopplysninger nå anses lovlig innhentet, forutsatt at arbeidstaker samtykker til dette. Dette gjelder blant annet opplysninger om hørsel, syn og fargesans. I tillegg også opplysninger om sykdomstilstander som kan gjøre den ansatte uskikket til å utføre enkelte arbeidsoppgaver innen vaktvirksomheten.

Ikke samtykke for rusmiddeltesting
Securitas hadde også etablert et system for rusmiddeltesting av sine ansatte, basert på samtykke. Datatilsynet mener imidlertid at arbeidsgivers styringsrett og samtykke fra de ansatte ikke er et tilstrekkelig hjemmelsgrunnlag for å kunne gjennomføre rusmiddeltester. Selv om Datatilsynet må utvise forsiktighet med å overprøve et gitt samtykke, er det ikke tvil om at mange arbeidstakere føler seg forpliktet til å si ja til denne typen inngrep. Konsekvensen av å ikke gi samtykke til rusmiddeltesting vil lett være at man heller ikke får jobb.

Tatt i betraktning den inngripende karakter som rusmiddeltesting innebærer, og den manglende maktbalanse det er mellom arbeidsgiver og arbeidstaker, mener Datatilsynet at det er lovgiver som må avgjøre hvilke bransjer og arbeidsforhold som gjør det nødvendig

med rusmiddelkontroller. Både formålsbestemmelsene i personopplysningsloven, hensynet til menneskerettighetene og legalitetshensyn tilsier en restriktiv holdning.

Selv om vaktselskapet hevder at kundene og allmennheten forventer en særskilt kontroll av sikkerhetspersonellet, mener Datatilsynet at Securitas ikke har dokumentert et større behov for rusmiddeltesting enn hva andre arbeidsgivere kan påberope seg. Personer som på grunn av rusproblemer ikke er egnet til å arbeide i vaktselskapene må fanges opp på annen måte.

Vedtaket er påklaget til Personvernnemnda.

Ny arbeidslivslov
Arbeidslivslovsutvalget leverte våren 2004 en svært omfattende utredning.

Formålet med utredningen var å få til en forbedring og forenkling av gjeldende arbeidsmiljølov. Når det gjelder de delene av utredningen som omtaler kontroll og overvåkning i arbeidslivet kan Datatilsynet imidlertid ikke se at de foreslåtte endringene bidrar til verken forbedring eller forenkling.

Bestemmelsene i forslaget gir kun generelle overordnede prinsipper, som allerede finnes i personopplysningsloven. Forslagene vil ikke gi de presiseringer som Datatilsynet har sett behov for når det gjelder bruk av personopplysninger i arbeidslivet. Etter Datatilsynets oppfatning hører denne typen presiseringer og konkretiseringer hjemme i forskriften til personopplysningsloven, og ikke ny arbeidslivslov. Det er uheldig når regelverk som gjelder bruk av personopplysninger blir spredt utover i lovverket. Det er upedagogisk og lite hensiktsmessig at behandling av personopplysninger i personalmapper skal følge reglene i personopplysningsloven, mens opplysninger knyttet til ansattes e-post skal reguleres i ny arbeidslivslov.

Utvalget legger stor vekt på bruk av samtykke som grunnlag for kontroll av ansatte. Både i EUs personverndirektiv og i vår egen personopplysningslov er samtykke et sentralt utgangspunkt for å kunne behandle personopplysninger. Innen arbeidslivet knytter det seg imidlertid vesentlige begrensninger til et slikt samtykke. I mange situasjoner vil den ansatte ikke stå overfor et reelt valg når det gjelder å gi sitt samtykke eller ikke. Skal et samtykke være reelt må det være frivillig. Arbeidstaker må også senere, uten at det fører til negative konsekvenser, kunne trekke sitt samtykke tilbake.

Datatilsynet er imidlertid tilfreds med at utvalget ikke legger opp til samtykke som behandlingsgrunnlag for helseundersøkelser og lignende.

Tillitsvalgte får innsyn i lønnsopplysninger
I 2001 avgjorde Datatilsynet at arbeidsgiver ikke, uten samtykke fra arbeidstaker, kunne utlevere lønnsopplysninger til tillitsvalgte om uorganiserte eller organiserte i andre arbeidstakerorganisasjoner i forkant av lønnsforhandlingene. Det var bare få unntak fra regelen, blant annet ved spørsmål om brudd på det såkalte ufravikelighetsprinsippet, eller saker som angår likestillingsloven.

Etter at det kom fram nye momenter fra Landsorganisasjonen vurderte Datatilsynet saken på nytt i 2004.

Datatilsynets vurdering

I de fleste tilfellene er det tilstrekkelig for tillitsvalgte å få opplysninger om ansattes lønn på gruppenivå i forbindelse med lønnsforhandlingene. Så lenge kategoriseringen, det være seg stilling, organisasjonstilhørighet, eller kjønn inneholder opplysninger om fem eller flere personer, vil opplysningene ikke omfattes av personopplysningsloven.

Når det dreier seg om færre enn fem personer kan enkeltpersoner være indirekte identifiserbare og personopplysningsloven gjelder. Etter Datatilsynets nye vurdering kan de tillitsvalgte likevel få tilgang til lønnsopplysninger om færre enn fem personer. Den tillitsvalgte må imidlertid da underskrive en taushetserklæring.

Til grunn for Datatilsynets endrede oppfatning er også hensynet til forskjellen mellom offentlig og privat sektor på grunn av reglene i offentlighetsloven.

Personlighet i pannen
En sak som dukket opp helt i slutten av meldingsåret illustrerer at Datatilsynet enkelte ganger må stille spørsmål ved arbeidsgivers respekt for den ansattes personlige integritet, selv om personopplysninger ikke direkte blir behandlet.

For å bedre kommunikasjonen internt i et selskapet Transocean oppfordres de ansatte til å ta en personlighetstest. På bakgrunn av testen blir arbeidstaker så kategorisert i en til to av fire forhåndsdefinerte kategorier, symbolisert gjennom fire ulike dyrearter og farger. En klistrelapp som viser hvilken kategori den ansatte tilhører festes deretter på vedkommendes hjelm eller kontordør. På denne måten skal det synliggjøres for alle hva slags karaktertrekk vedkommende har. Dette skal lette kommunikasjonen medarbeiderne imellom.

Etter forespørsel fra Datatilsynet hevder selskapet at gjennomføring av testen er frivillig. De ansatte utfører testen på egen hånd og finner selv ut hvilken kategori de tilhører. De detaljerte testresultatene blir heller ikke oppbevart. Det skjer dermed ingen behandling av personopplysninger, slik personopplysningsloven definerer det.

Datatilsynet mener likevel at tiltaket, slik det er gjennomført, kan krenke den enkeltes personlige integritet. Arbeidstaker vil lett oppleve press i retning av å måtte gjennomføre testen, for deretter å feste klistremerket som signaliserer personlighet på hjelmen. Dette vil lett kunne virke stigmatiserende, også om man, som en av få, skulle nekte å la seg merke på denne måten.

Datatilsynet mener at det bør være mulig å skape bevissthet om viktigheten av god kommunikasjon mellom mennesker på en arbeidsplass på mindre potensielt krenkende måter.

Vedlegg 1:

RETTSSIKKERHET 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 er 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 rettssikkerhet. Begrepet har imidlertid fått et upresist innhold. I dag blir begrepet rettsikkerhet benyttet i to betydninger. Rettssikkerhet 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 rettssikkerhetsbegrepet 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 rettssikkerhetsbegrepet 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

utrykk for demokratiet, borgerne styrer seg selv gjennom valg. Lovskravet er også en forutsetning for forutsigbarhet.

Rettssikkerhet 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 rettssikkerhet. 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 ivaretatt 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 avveiingen 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.

Vedlegg 2: Oversikt over gjennomførte tilsyn 2004

Saksnr.	Tilsynsobjekt	Poststed	Bransje/sektor
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 Norge AS	Oslo	Arbeidsliv
2004/0310	Securitas AS	Oslo	Arbeidsliv
2004/0573	Peppes Pizza AS	Sandvika	Arbeidsliv
2004/0553	NorgesGruppen ASA	Oslo	Detaljhandel
2004/0552	COOP-kjeden	Oslo	Detaljhandel
2002/0768	Bakevarehuset AS	Asker	Kameraovervåking
2004/1505	Hydro Texaco	Bergen	Kameraovervåking
2004/1504	Bergen Storsenter	Bergen	Kameraovervåking
2004/0380	Sandviken Dagligvare	Bergen	Kameraovervåking
2004/1547	Terje Høili	Fredrikstad	Kameraovervåking
2004/1370	Torvbyen	Fredrikstad	Kameraovervåking
2004/1368	Hydro Texaco	Fredrikstad	Kameraovervåking
2004/1320	Narvesen Gardermoen	Gardermoen	Kameraovervåking
2004/1626	Mosaiske trossamfunn	Oslo	Kameraovervåking
2004/1566	ICA Norge AS v/Rimi Østbanehallen	Oslo	Kameraovervåking
2004/1538	XXL sport & villmark, Storgata	Oslo	Kameraovervåking
2004/1377	Elkjøp Stormarked	Oslo	Kameraovervåking
2004/0915	Oslo Sporveier	Oslo	Kameraovervåking
2004/0894	NSB Persontog AS	Oslo	Kameraovervåking
2004/0866	Profilhuset Meny-Ultra	Oslo	Kameraovervåking
2004/0865	Statoil Detaljist v/Skedsmo	Oslo	Kameraovervåking
2004/0864	Steen og Strøm Norge AS	Oslo	Kameraovervåking
2004/0862	Rimi Norge	Oslo	Kameraovervåking
2004/0861	Esso Tiger AS	Oslo	Kameraovervåking
2003/1104	Car Park (Oslo City)	Oslo	Kameraovervåking
2004/1475	Nygaten Vel	Stavanger	Kameraovervåking
2004/1410	Stavanger Storsenter	Stavanger	Kameraovervåking
2004/0863	Nille AS v/stovner senter	Ytre Enebakk	Kameraovervåking
2004/1328	it:solutions	Bergen	Internettrelatert
2004/0523	BGNett AS	Bergen	Internettrelatert
2004/0521	Telenor internett AS - Privatmarked	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	Markedsførere
2004/0027	Bonnier DM AS	Oslo	Markedsførere
2004/1282	Klæbu Legesenter	Klæbu	Primærhelsetjeneste
2004/1284	Kvaløysletta legekontor	Kvaløysletta	Primærhelsetjeneste
2004/1281	Nermo Legesenter	Mo i Rana	Primærhelsetjeneste
2004/1283	Skåla legekontor	Skåla	Primærhelsetjeneste

2004/0355	Fjelstrup legeservice	Stavanger	Primærhelsetjeneste
2004/1276	Utsikten Legesenter	Tromsø	Primærhelsetjeneste
2004/1275	Nordbyen Legesenter	Tromsø	Primærhelsetjeneste
2004/1279	Risvollan Legesenter	Trondheim	Primærhelsetjeneste
2004/1280	Vikhammer Legekontor	Vikhammar	Primærhelsetjeneste
2004/1277	Ytteren Legesenter	Ytteren	Primærhelsetjeneste
2004/1018	Krisesenteret i Fredrikstad	Fredrikstad	Ideelle organisasjoner
2004/1020	Krisesenteret i Hamar	Hamar	Ideelle organisasjoner
2004/1291	Redningsselskapet	Høvik	Ideelle organisasjoner
2004/1290	Landsforeningen til støtte for krybbedød	Oslo	Ideelle organisasjoner
2004/1021	Krisesenteret i Oslo	Oslo	Ideelle organisasjoner
2004/1019	Krisesenteret i Sarpsborg	Sarpsborg	Ideelle organisasjoner
2004/0906	Krisesenteret i Tromsø	Tromsø	Ideelle organisasjoner
2004/1373	Stena Line Norge AS	Oslo	Reisevirksomhet
2004/1367	Skandinavisk reisefeber AS	Oslo	Reisevirksomhet
2004/1363	Color Line	Oslo	Reisevirksomhet
2004/1362	Mytravel Norway (ving)	Oslo	Reisevirksomhet
2004/1376	Widerøes Flyveselskap	Sandvika	Reisevirksomhet
2004/1574	Helse Vest RHF	Bergen	Større helseforetak
2004/1575	Helse Nord RHF	Harstad	Større helseforetak
2004/1451	Helse SØR RHF	Kristiansand	Større helseforetak
2004/1278	Helgelandssykehuset HF (Mo i Rana)	Mo i Rana	Større helseforetak
2004/1573	Helse Øst RHF	Oslo	Større helseforetak
2004/1576	Helse Midt-Norge RHF	Trondheim	Større helseforetak
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	Fylkestrygdekontor i Akershus	Oslo	Trygd
2004/1274	Trygdekontor i Oslo	Oslo	Trygd
2004/1274	Fylkestrygdekontor i Sør-trøndelag	Trondheim	Trygd
2004/1274	Trygdekontor i Trondheim	Trondheim	Trygd
2004/1491	Universitetet i Bergen	Bergen	Forskning
2004/1490	Universitetet i Bergen	Bergen	Forskning
2004/1489	Universitetet i Bergen	Bergen	Forskning
2004/1488	Universitetet i Bergen	Bergen	Forskning
2004/1487	Universitetet i Bergen	Bergen	Forskning
2004/1484	Universitet i Bergen	Bergen	Forskning
2004/0763	Universitetet i Bergen	Bergen	Forskning
2004/0665	Haraldsplass Diakonale Sykehus AS	Bergen	Forskning
2004/0528	Helse Bergen HF	Bergen	Forskning
2004/0345	Helse Bergen, Haukeland (barneleukemi)	Bergen	Forskning
2004/0344	Helse Bergen, Haukeland (prosjekt)	Bergen	Forskning
2004/0343	Helse Bergen, Haukeland(kreft)	Bergen	Forskning
2004/0338	Helse Bergen, Haukeland (Ernæring)	Bergen	Forskning
2004/0333	Helse Bergen HF	Bergen	Forskning
2004/0757	Nordlandsforskning	Bodø	Forskning
2004/0760	Helse Finnmark	Hammerfest	Forskning
2004/0337	Akershus Universitetssykehus HF	Nordbyhagen	Forskning

2004/1183	Radiumhospitalet	Oslo	Forskning
2004/1155	Eli Lilly Norge AS	Oslo	Forskning
2004/1080	Universitetet i Oslo	Oslo	Forskning
2004/0759	Universitetet i Oslo	Oslo	Forskning
2004/0758	Universitetet i Oslo	Oslo	Forskning
2004/0754	Universitetet i Oslo	Oslo	Forskning
2004/0645	Aker universitetssykehus - Prosjekt II	Oslo	Forskning
2004/0644	Aker universitetssykehus - Prosjekt I	Oslo	Forskning
2004/0638	Rikshospitalet	Oslo	Forskning
2004/0603	Radiumhospitalet	Oslo	Forskning
2004/0362	Eli Lilly Norge AS	Oslo	Forskning
2004/0361	GlaxoSmithKlein II	Oslo	Forskning
2004/0360	SIRUS IV	Oslo	Forskning
2004/0359	SIRUS III	Oslo	Forskning
2004/0358	SIRUS II	Oslo	Forskning
2004/0357	Eli Lilly Norge AS	Oslo	Forskning
2004/0356	Aker sykehus - Generell	Oslo	Forskning
2004/0354	Rikshospitalet	Oslo	Forskning
2004/0351	SIRUS	Oslo	Forskning
2004/0350	Universitetet i Oslo	Oslo	Forskning
2004/0349	Universitetet i Oslo	Oslo	Forskning
2004/0348	Universitetet i Oslo	Oslo	Forskning
2004/0346	Rikshospitalet	Oslo	Forskning
2004/0340	Ullevål Universitetssykehus HF	Oslo	Forskning
2004/0339	Ullevål Universitetssykehus HF	Oslo	Forskning
2004/0335	Det norske Radiumhospital HF	Oslo	Forskning
2004/0334	Ullevål Universitetssykeshus HF	Oslo	Forskning
2004/0332	GlaxoSmithKlein	Oslo	Forskning
2004/0331	AstraZeneca	Oslo	Forskning
2004/0330	Novartis	Oslo	Forskning
2004/0329	Genova AS	Oslo	Forskning
2004/0328	Sirus	Oslo	Forskning
2003/1080	Universitetet i Oslo	Oslo	Forskning
2004/0762	Høgskolen i Telemark	Porsgrunn	Forskning
2004/1066	Høgskolen i Savanger	Stavanger	Forskning
2004/0365	Høgskolen i Stavanger	Stavanger	Forskning
2004/0364	Høgskolen i Stavanger	Stavanger	Forskning
2004/0363	Høgskolen i Savanger	Stavanger	Forskning
2004/1034	Universitetet iTromsø (prosjekt 3)	Tromsø	Forskning
2004/1033	Universitet i Tromsø (prosjekt 2)	Tromsø	Forskning
2004/0764	Universitetssykehuset i Nordland	Tromsø	Forskning
2004/0635	Tromsø universitet - generell	Tromsø	Forskning
2004/0367	Universitet i Tromsø	Tromsø	Forskning
2004/0366	Tromsø universitet (prosjekt 1)	Tromsø	Forskning
2004/0704	SINTEF Unimed prosjekt I	Trondheim	Forskning
2004/0703	SINTEF Unimed prosjekt II	Trondheim	Forskning
2004/0702	SINTEF Unimed prosjekt III	Trondheim	Forskning
2004/0557	NTNU - Prosjekt IV	Trondheim	Forskning
2004/0556	NTNU - Prosjekt III	Trondheim	Forskning
2004/0555	NTNU - Prosjekt II	Trondheim	Forskning
2004/0554	NTNU - Prosjekt I	Trondheim	Forskning
2004/0543	St. Olav - Prosjekt V	Trondheim	Forskning

2004/0541	St. Olav - Prosjekt IV	Trondheim	Forskning
2004/0536	St.Olav - Prosjekt III	Trondheim	Forskning
2004/0535	St. Olav - Prosjekt II	Trondheim	Forskning
2004/0534	St. Olav - prosjekt I	Trondheim	Forskning
2004/0342	St. Olavs Hospital HF	Trondheim	Forskning
2004/0341	NTNU	Trondheim	Forskning
2004/0352	Sykehuset innlandet HF Tynset	Tynset	Forskning
2004/0353	Kompetansesenteret for Sikkerhets-, fengsels-, og rettspsykiatri	Oslo	Forskning