Datatilsynet

Datatilsynets årsmelding 2006

Årsmelding R07/01

20.02.2007

Manus til stortingsmelding om Datatilsynets virksomhet, jf personopplysningslovens § 42.

Oversendt Fornyings- og administrasjonsdepartementet.

20. februar 2007.

Datatilsynet

Gateadresse: Tollbugata 3, Oslo

Postadresse: postboks 8177, dep

0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50

Innholdsfortegnelse

DEL I

1 Om Datatilsynet

Datatilsynet ble etablert 1. januar 1980 i samsvar med den daværende personregisterloven vedtatt i 1978.

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 Fornyings- og administrasjonsdepartementet. 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 avgir sin egen årsmelding.

Datatilsynets oppgaver

Som en følge av at personopplysningsloven den 1. januar 2001 kom i stedet for den tidligere personregisterloven, ble hovedtyngden av Datatilsynets arbeide flyttet fra forhåndskontroll til etterfølgende kontroll. Dette i form av tilsynsarbeid, informasjon og oppfølging av brudd på regelverket.

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

Den økonomiske rammen for Datatilsynet var i 2006 på 24 778 000 kroner. To millioner var øremerket en ekstra kommunikasjonssatsing knyttet til oppfølging av Personvernundersøkelsen som ble gjennomført i 2005.

Lønnskostnadene til Datatilsynet utgjør 65,5 prosent av den totale bevilgning.

Ut over dette er budsjettet bundet opp i mer eller mindre faste kostnader som husleie, drift, inventar/utstyr og nødvendig reisevirksomhet til tilsyn og deltagelse i internasjonale samarbeidsorganer. Datatilsynet har således de senere år hatt lite handlingsrom til å sette inn økonomiske ressurser til tiltak som ikke direkte knytter seg til juridisk saksbehandling eller tilsynsvirksomhet. De to millionene som ble bevilget til en ekstra kommunikasjonsinnsats i 2006, og som er fulgt opp som er fulgt opp også i 2007-budsjettet, har derfor vært et meget motiverende og positivt bidrag. Den ekstra satsingen gjør det mulig for Datatilsynet å iverksette helt nye kommunikasjonstiltak som skaper oppmerksomhet og gir befolkningen en kunnskap som gjør den enkelte bedre i stand til å selv å kunne ivareta eget personvern og respektere andres.

Organisasjon

Datatilsynet var i 2006 bemannet med 32 årsverk, som fordeler seg slik:

- Direktøren
- Juridisk avdeling: 12 medarbeidere
- Tilsyn- og sikkerhetsavdelingen 5 medarbeidere
- Administrasjonsavdelingen 7 medarbeidere
- Informasjonsavdelingen 7 medarbeidere. 4 av disse er jurister knyttet til Datatilsynet juridiske svartjeneste, Frontservice. Frontservice betjener henvendelser pr telefon og e-post ved siden av ordinær saksbehandling.

Datatilsynet vurderer kjønnssammensettingen fortløpende og søker å ta hensyn til å rekruttere i forhold til denne om kvalifikasjonene ellers er like. Tre kvinner har i virksomhetsåret hatt svangerskapspermisjon og tre menn er tilsatt i vikariater/engasjement.

Datatilsynet har som mål å arbeide aktivt for at etaten til enhver tid gir kvinner og menn like arbeidsforhold og like muligheter til karriereutvikling og faglig utvikling. Gjennomsnittsalderen i Datatilsynet er for tiden 42 år for menn og 37 år for kvinner.

Tre medarbeidere sluttet i virksomhetsåret.

Datatilsynet ønsker å stimulere til et kulturelt og kompetansemessig mangfold i staben. Videre tilrettelegges det for en personalpolitikk som skal virke motiverende, og hindre utstøting av personer med nedsatt funksjonsevne. Datatilsynet er knyttet til avtalen om inkluderende arbeidsliv. Fokus i 2006 har vært tiltak som forebygger belastningslidelser. Dette har vært tiltak knyttet til trening, ergonomisk veiledning og instruksjon om hensiktsmessig arbeidsteknikk.

3 Saksbehandling

Det ble journalført 6 431 dokumenter i meldingsåret. Av disse var 3 744 innkomne og 2 530 utgående brev fra Datatilsynet. Dette representerer en nedgang på 234 journalførte dokumenter i forhold til året før. Fortsatt utgjør helserelaterte saker, og da særlig knyttet til forskningsprosjekter, den betydeligste delen av saksmengden. I løpet av 2007 vil det, som et resultat av Nylennautvalgets arbeid, komme en ny forskningslov. Denne vil gripe direkte inn i Datatilsynets saksbehandling. Omfanget vil avhenge av i hvilken grad Datatilsynet blir tillagt myndighet etter den nye forskningsloven.

Det er også i dette meldingsåret gått med mye saksbehandlingsressurser knyttet til personvern innen arbeidslivet. Dette skyldes naturlig nok de store e-postsakene fra 2005 (Vinmonopol, Redningsselskapet og forlaget Bazar) som Datatilsynet fortsatt arbeidet med. Det ble også nedlagt betydelig arbeid i forbindelse med de nye biometriske passene og konsesjon i forbindelse med et advokatkontors antipiratarbeid. Innen samferdselssektoren stod arbeidet med EFC-direktivet sentralt. Dette direktivet var den bakenforliggende årsak til at representanten Sponheim (V) sendte et dokument 8:forslag til Stortinget med forslag om å pålegge Regjeringen å gi en melding til Stortinget om personvernmessige aspekter ved overvåking i samferdselssektoren.

Konsesjonsplikten

Plikten til å søke konsesjon gjelder i all hovedsak for behandling av sensitive personopplysninger, blant annet opplysninger om helse, rase, religiøs oppfatning, politisk tilknytning, straffbare handlinger og seksuell atferd. Datatilsynet kan likevel bestemme at også andre behandlinger av personopplysninger skal være konsesjonspliktige, så fremt behandlingen åpenbart vil krenke tungtveiende personverninteresser.

Det ble i meldingsåret gitt 225 konsesjoner, hvorav størstedelen ble gitt til forskningsprosjekter.

Av andre kan nevnes konsesjon til selskaper som driver helautomatiske bomstasjoner, private barneverninstitusjoner og til advokatfirmaet Simonsen for sin virksomhet som antipiratbyrå.

Meldeplikten

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

I 2006 kom det inn 3 019 nye meldinger om behandling av personopplysninger mot 2 953 året før. Totalt er det nå 8 954 meldinger i meldingsdatabasen. Dette utgjør en nedgang på ca. 2 400 fra året før. 5 518 meldinger ble slettet fra databasen i 2006, fordi de var ”gått ut på dato”. Tallene tyder på at mange virksomheter ikke overholder meldeplikten. Dette antas i særlig grad å gjelde kameraovervåking.

Klagesaker til Personvernnemnda

I meldingsåret oversendte Datatilsynet 13 saker til Personvernnemnda for videre klagesaksbehandling. Dette gjaldt:

- Klage på personopplysninger lagt ut på Internett av en privatperson
- Klage på Stavanger Aftenblad vedrørende krenkelse av personvernet på Internett
- Klage på pålegg om opphør av KLPs praksis om kredittvurdering av potensielle leietakere
- Klage vedrørende installasjon av Microsoft Windows XP
- Klage vedrørende identitetsmisbruk
- Klage på vedtak om opphør av dopingprøver
- Tre klager på bruk av fingeravtrykk i forbindelse med adgangskontroll
- Klage på bruk av fingeravtrykk i forbindelse med timeregistrering for ansatte
- Klage på bruk av fingeravtrykk i tilknytning til pålogging av datasystem
- Klage på utlevering av personopplysninger fra Tilsynsrådet for advokatvirksomhet
- Klage på vedtak om brudd på taushetsplikten knyttet til forsikring.

Resultatet i syv av disse sakene ble meddelt Datatilsynet i meldingsåret. I tillegg mottok Datatilsynet resultatet i ni saker som var sendt inn før 2006.

Av de 16 sakene som ble behandlet og avgjort av Personvernnemnda ble syv av Datatilsynets avgjørelser opprettholdt, og seks ble omgjort. I tre saker ble resultatet materielt stående, men grunnlaget endret.

Den relativt høye andelen avvik fra utfallet av førsteinstansbehandlingen er blitt lagt merke til, både i og utenfor Datatilsynet. Omgjøringenes antall er imidlertid likevel så få at det er vanskelig å finne et mønster som kan sies å karakterisere Datatilsynets og Personvernnemndas ulike tilnærminger til de samme, konkrete personvernspørsmålene som forutsettes regulert av personopplysningsloven.

For Datatilsynet har det fremstilt seg som nærliggende å forklare de hyppige omgjøringene som ulik vektlegging i de to instansene av hensynet til den enkelte borgers interesse på den ene siden, og korporative og samfunnsfelleskapelige interesser på den annen.

Datatilsynets implementering av de endelige avgjørelsene har i to tilfeller støtt på helt spesielle problemer. I forbindelse med passasjertransportørers ønske om kameraovervåking av hele passasjerarealet i buss og tog, påla nemnda Datatilsynet å utferdige konsesjoner for tiltak som Stortinget uttrykkelig har understreket skal være konsesjonsfrie (PVN 2005 - 12 og 13). En årsak til forundring har også vært Personvernnemndas definisjon av begrepet ”personopplysning”, som har fjernet seg markert fra Datatilsynets egen - en forståelse som Datatilsynet også deler med de fleste av sine søsterinstitusjoner i Europa.

Det hender dessuten at språkbruk og formuleringer i Personvernnemndas avgjørelser savner en presisjon og klarhet som gjør dem enkle å bruke som basis for fremtidig saksbehandling. Eksempelvis er det både i og utenfor Datatilsynet usikkerhet om hvorvidt

Personvernnemnda i avgjørelsen av en sak om bruk av biometri (PVN 2006-07) har godkjent en løsning, eller autorisert et spesielt patent, samt hvilke sikkerhetsanalyser som førte nemnda frem til sin konklusjon.

Høringssaker

Datatilsynet mottok i alt 123 høringssaker. Til 85 av disse ble det gitt bemerkninger med materielt innhold. De viktigste sakene er omtalt senere i årsmeldingen.

Lov og forskriftsarbeide

I samarbeid med Justisdepartementet og Fornyings- og administrasjonsdepartementet ble det startet et lovrevisjonsarbeide på personopplysningsloven. Dette arbeidet vil fortsette i 2007. Arbeidet ledes av Justisdepartementets lovavdeling, som er ansvarlig for personopplysningsloven.

Positivt år for personvernombudsordningen

Stadig flere virksomheter oppretter personvernombud. I løpet av 2006 ble det opprettet 43 nye ombud. Ved utgangen av året var det dermed til sammen 63 ombud, som representerer 238 ulike virksomheter.

Denne gledelige utviklingen er en direkte følge av at Datatilsynet har jobbet både mer målrettet, og brukt mer ressurser enn tidligere på å gjøre ordningen kjent for offentlige og private virksomheter. Oppfordringen har vært at virksomhetene bør opprette et ombud internt i virksomheten, eller knytte til seg et eksternt ombud. Datatilsynet har informert om ordningen i foredrag, tilsyn og i diverse møter. Tilsynet besøkte dessuten fem byer, der kommunene i området fikk informasjon om ordningen. Etter å ha fått utfyllende informasjon, har det vist seg å være lettere for virksomheter å ta beslutningen om å opprette ombud.

Også bank og finanssektoren ble spesielt oppfordret om å opprette personvernombud. Som et ledd i dette sendte tilsynet ut et brev til alle landets banker med informasjon om ordningen og invitasjon til å delta på et seminar for potensielle ombud. Interessen var overveldende og 36 virksomheter fra sektoren deltok på seminaret med den følge at åtte banker oppnevnte personvernombud. I tillegg har også enkelte inkassosselskaper gjort det samme.

Videre har seminarer stått i fokus i løpet av året. I tillegg til seminaret for bank- og finanssektoren, er det blitt gjennomført to seminarer for virksomheter som vurderer ordningen. Datatilsynet har dessuten arrangert et opplæringsseminar for nye ombud, i tillegg til det årlige seminaret for samtlige ombud. Erfaringene med seminarene har vært gode, og satsingen vil bli utviklet videre i 2007.

Ut over disse informasjonstiltakene har Datatilsynet utviklet et søknadsskjema som har gjort det lettere å søke om å få opprette et ombud. Videre er det blitt utviklet et eget meldeskjema for ombudene, slik at de enkelt kan føre oversikt over virksomhetens meldinger. Virksomheter med personvernombud er unntatt fra meldeplikten til Datatilsynet, men må melde fra om behandling av personopplysninger til ombudet.

4 Deltakelse i offentlige råd og utvalg

Datatilsynet har som visjon å fremme respekten for det enkelte samfunnsmedlems privatliv, særlig når det gjelder bruk av personopplysninger. For å fremme denne visjonen arbeider Datatilsynet blant annet for å påvirke at nasjonal og internasjonal lovgivning tar hensyn til respekten for privatsfærens betydning for bevaring av menneskerettigheter, demokratiet og rettsstatens institusjoner. Deltakelse i offentlige råd og utvalg en viktig arena i så måte.

I meldingsåret har Datatilsynet deltatt i følgende råd, utvalg eller samarbeidsfora:

Arbeidsgruppe for revisjon av personopplysningslov og personopplysningsforskrift

Personopplysningsloven skal etterkontrolleres. I denne anledning er det nedsatt en arbeidsgruppe som arbeider med problemstillinger knyttet til lovrevisjonen. Gruppen består av representanter fra Justis- og politidepartementet, Fornyings- og Administrasjonsdepartementet og Datatilsynet. Gruppen leverte i meldingsåret et forslag til enkelte endringer i personopplysningsloven, samt en forskrift om innsyn i arbeidstakeres e-post.

Datakrimutvalget

En av datatilsynets jurister er medlem av Datakrimutvalget. Primært har det vært arbeidet med implementering av Cybercrime-konvensjonen i norsk rett.

Arbeidsgruppe for opprettelse av Offentlig Elektronisk Postjournal (OEP)

Gruppen ledes av Fornyings- og Administrasjonsdepartementet. Mandatet er blant annet å kartlegge behovet for utfyllende felles regler for journalføring og kvalitetssikring av offentlig journal, med formål å hindre utilsiktede konsekvenser av at journalen blir allment tilgjengelig over Internett. Arbeidet er ikke avsluttet.

Arbeidsgruppe for utredning av ID-kort for byggenæringen

Datatilsynet var først invitert til å delta i en referansegruppe, men ble etter det første møtet i referansegruppen innlemmet som observatør i arbeidsgruppen, nedsatt av Arbeids- og Inkluderingsdepartementet. Det ble utformet en rapport som ble sendt på høring i 2006. Datatilsynet tok dissens på samtlige forslag i rapporten.

Styringsgruppen for SERTIT

Nasjonal Sikkerhetsmyndighet (NSM) er ansvarlig for sertifiseringsordningen for informasjonssikkerhet når det gjelder IT-utstyr og systemer. Datatilsynet har de siste årene deltatt i styringsgruppen for arbeidet. Formålet med deltakelsen er å fremme sertifiseringsordningen, slik at denne kan få praktisk anvendelse for de som er underlagt sikkerhetsbestemmelsene i personopplysningsloven. Datatilsynet har valg å avvikle videre engasjement i gruppen.

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. Formålet med rådet 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.

Bransjenorm for helsesektoren

Sosial- og Helsedirektoratet har vært initiativtaker til et større prosjekt hvor formålet har vært å utvikle en bransjenorm for helsesektoren. Normen skal bidra til å harmonisere nivået i helsesektoren når det gjelder informasjonssikkerhet. Gjennomførte tilsyn har avdekket et stort behov for et felles løft. Datatilsynet har bistått med råd og veiledning ved utforming av normen. Arbeidet ble avsluttet september 2006. En styringsgruppe har overtatt ansvaret for forvaltning av normen. Arbeidet består nå i å få en hensiktsmessig spredning og implementering av normen i sektoren. Dette skaper store utfordringer gitt sammensetningen av små, mellomstore og store aktører. Datatilsynet deltar som observatør i styringsgruppen.

KIS - Koordineringsutvalget for informasjonssikkerhet

Utvalget består av representanter for sju departementer, Statsministerens kontor og ni direktorater. Opprettelsen av koordineringsutvalget er et ledd i gjennomføringen av 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 og sørge for samordning av tilsynspraksis. Utvalget skal også drøfte aktuelle risiko- og sårbarhetsspørsmål og bidra til koordinering av informasjonstiltak og beredskapsplanlegging Mye av arbeidet i KIS delegeres til arbeidsgrupper. Datatilsynet har prioritert å være aktiv i disse arbeidsgruppene.

SARI – Samordning av regelverk innen informasjonssikkerhet

Gruppen er opprettet av koordineringsutvalget. Alle myndigheter som regulerer informasjonssikkerhet sitter i denne gruppen. Siktemål er regelverksforenkling innen regulering av informasjonssikkerhet.

KOBI – begrepsapparat innen regulering av informasjonssikkerhet

Koordineringsutvalget opprettet KOBI som en ny gruppe i 2006. Alle myndigheter som regulerer informasjonssikkerhet sitter i denne gruppen. Siktemålet er å lage en metode for klassifisering av informasjon, ut fra behov for beskyttelse.

Koordineringsutvalget for E-forvaltning

Utvalget skal arbeide med samordning mellom de forskjellige offentlige organer for å realisere planen E-2009. Møtene, som ledes av Fornyings- og administrasjonsministeren holder fokus på målformuleringene i nevnte plan og hvordan de enkelte aktører kan bidra for å realisere disse.

Arbeidsgruppe for implementering av datalagringsdirektivet

Dette er en interdepartemental gruppe for implementering av datalagringsdirektivet .

Utvalgets mandat er å tilpasse datalagringsdirektivet til norsk lov. Datatilsynet er representert med en observatør i gruppen. I dette arbeidet har Datatilsynet spesielt lagt vekt på avklaring rundt lagringstid, hvor informasjon skal lagres, hvem som skal ha tilgang og terskel for bruk av data.

Ny folkeregisterlov

Folkeregisteret innholder nøkkelopplysninger om alle landets innbyggere. En rekke aktører har tatt til orde for å utvide omfanget av opplysninger som registreres, og å gi lettere tilgang til opplysningene for aktører i privat og offentlig virksomhet. Datatilsynet deltar med en observatør i arbeidet.

Nasjonalt identitetskort, elektronisk signatur og elektronisk identitet

Justisdepartementet har tatt initiativ til å utrede behov for nasjonale identitetskort. Datatilsynet deltar med observatørstatus i en arbeidsgruppe som utreder dette. Datatilsynet har vært opptatt av mange aspekter ved nasjonalt identitetskort. Blant disse er hva som skal inngå av opplysninger i kortet, bruk av RFID teknologi, om det skal etableres et sentralt register, og hvem som i så fall skal få tilgang til dette. Arbeidet som observatør i denne gruppen har krevd betydelig mer ressurser enn det Datatilsynet hadde forutsatt. Dette skyldes i hovedsak at tilsynet har hatt vesentlige merknader til gruppens konklusjoner.

NAFAL

NAFAL er et såkalt ”tilpasningsråd for sivil luftfart”. Hovedtema er implementering av sikkerhetsløsninger på flyplasser. Innen denne tematikken reises en rekke spørsmål i forhold til personvern. Datatilsynet har i 2006 deltatt som observatør på ett møte.

5 Internasjonalt samarbeid

I likhet med deltakelse i norske offentlige råd og utvalg, er også deltakelse på internasjonale møter og arbeidsgrupper en viktig arena for å påvirke lovgivningen på området. Med all respekt er det i dag EU som pensler ut de framtidige personvernrettslige normer og regler. Datatilsynet har derfor valgt å være deltaker i utvalgte arbeidsgrupper under artikkel 29-gruppen. De internasjonale møtene er også en arena for utveksling av synspunkter, som er særdeles viktig for et tilsynsorgan som Datatilsynet å være en del av.

Nedenfor er en oversikt over de internasjonale arbeidsgrupper og råd som Datatilsynet er representert i.

Artikkel 29-gruppen

Den norske personopplysningsloven reflekterer alle de grunnleggende og ufravikelige personvernprinsippene som er nedfelt i EU-direktivet om personvern. Sammen med kollegaer fra de ti søkerlandene til EU-medlemskap, har Datatilsynet deltatt som observatør i arbeidsgruppen opprettet etter direktivets artikkel 29. Gruppen har som oppgave å drive fram koordinering og synkronisering av EU/EØS-landenes nasjonale personvernarbeid, med utgangspunkt i personverndirektiv 46/95. Gruppen har en rådgivende funksjon overfor Kommisjonen og står fritt til å tolke og konkretisere direktivets innhold. I løpet av meldingsåret avholdt gruppen fem to-dagersmøter i Brüssel, i tillegg til det større ”vårmøtet”, som denne gang ble arrangert i Budapest.

Gruppen arbeider ofte med utgangspunkt i dokumenter fra uformelle arbeidsgrupper, der alle medlemslandene kan være med. Uten at det foreligger noe formelt vedtak, er det i praksis akseptert at også observatørland kan tiltre disse gruppene. Datatilsynet har i meldingsåret vært representert i tre slike arbeidsgrupper.

- *Medical Data.* Arbeidsgruppen har hovedfokus på helsejournaler.
- *Identity management.* Arbeidsgruppen tar for seg autentisering og identifisering i den elektroniske verden.
- *Internet task force*. Arbeidsgruppen arbeider med internettrelaterte spørsmål, med vekt på det tekniske. I meldingsåret har gruppen blant annet drøftet personvernmyndighetenes holdning til e-Call (automatisk oppringing av nødsentral fra ulykkessted i trafikken). Gruppen har også hatt kontakt med Google Incorporate for å sette seg inn i selskapets håndtering av personopplysninger ved G-mail og selskapets søkemotor.

Det internasjonale datatilsynsmøtet

Hvert år holdes det en internasjonal konferanse for datatilsynssjefer med deltakere fra hele verden. Konferansen inneholder en åpen del som også andre enn datatilsynssjefene kan delta på. I 2006 ble konferansen holdt i London og Datatilsynet deltok med tre representanter. Hovedtema for konferansen var ”A report on the surveillance society”.

Berlin-gruppen

Den internasjonale arbeidsgruppen for personvern innen telekommunikasjon (Berlin-gruppen) er primært nedsatt for å arbeide med tekniske problemstillinger knyttet til telekommunikasjon, men behandler også andre tekniske problemstillinger. Blant de mest sentrale saker i meldingsåret var:

- Søkemotorenes praksis med hensyn til lagring av søk
- Planlagt bruk av det europeiske satellittsystemet Galileo innen samferdselssektoren
- Bruk av RFID i legitimasjonsdokumenter og betalingskort
- Digitalisert overvåkning: Internett samt kameraovervåkning

En rekke andre tekniske problemstillinger var gjenstand for drøftelser i gruppen. Arbeidet i gruppen gir Datatilsynet viktige bidrag i sitt arbeid med tekniske problemstillinger.

Police Working Party

Gruppen arbeider med spørsmål vedrørende politisamarbeid som faller inn under tredje søyle, det vil si utenfor det indre marked. Datatilsynet er representert med en saksbehandler.

Joint Supervisory Authority

JSA er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). Informasjonssystemet inneholder opplysninger om personer som er ettersøkt, savnet, nektet innreise til Schengenområdet, eller er straffedømt i et av medlemslandene. Normalt avholdes fem møter årlig i Brüssel, og Datatilsynet er representert med ett medlem i gruppen. JSA har også arbeidet med uttalelser i forbindelse med ønsker om utvidelse av SIS. I 2006 ble alle landene oppfordret til å foreta tilsyn etter artikkel 99 i Schengenkonvensjonen.

Internasjonalt saksbehandlermøte

Dette er et internasjonalt samarbeidsforum for saksbehandlere. Det ble avholdt to møter, henholdsvis i Madrid og Athen. Diskusjonene omhandlet blant annet e-governement, e-ticketing, ekomdirektivet, bruk av lydopptak i arbeidslivet, bruk av personopplysninger i finanssektoren og forskjellige løsninger for innføring av personvernombud. Datatilsynet var representert med to saksbehandlere på disse møtene.

Nordisk saksbehandlermøte

Dette er et årlig nordisk forum for saksbehandlere. Møtet ble avholdt i Helsinki og Datatilsynet var representert med tre saksbehandlere. Møtet hadde særlig fokus på kontroll i arbeidslivet, herunder innsyn i e-post, rusmiddelkontroll og telefonkontroll.

Nordisk teknologimøte

Nordisk teknologimøte er opprettet for å skape en god kontakt mellom de teknologiske miljøene hos personvernmyndighetene i de nordiske land. Formålet med møtene er å diskutere aktuelle tekniske problemstillinger, med sikte på å komme frem til en omforent håndhevelse av regelverket. Tema på årets var detaljer rundt gjennomføring av tekniske kontroller, drøftelser rundt bruk av RFID, pass og nasjonale identitetskort, samt helsevesenets bruk av mobile terminaler.

6 Informasjonsvirksomheten

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, frivillige organisasjoner 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.

Selv om Datatilsynet gjennom sin publisering av saker på hjemmesiden, kombinert med en aktiv mediekontakt, oppnår stor grad av synlighet og skaper debatt i mediene, så har disse virkemidlene helt klare begrensninger. Det er vanskelig å skape en reell refleksjon, bevisstgjøring og dermed bygging av kunnskap i målgruppene.

Personvernundersøkelsen fra 2005 viste tydelig at befolkningen på den ene siden har liten kunnskap om egne rettigheter med hensyn til personvern, men stor tillit til at alle de virksomhetene som behandler personopplysinger etterlever lovgivningen. Samtidig viser undersøkelsen blant virksomhetene at man der har liten kunnskap om, og følgelig liten grad av etterlevelse i forhold til de konkrete kravene som stilles i den nye lovgivningen.

Som en oppfølging av personvernundersøkelsen oversendte Datatilsynet i januar 2006 et satsingsforslag ”Kommunikasjon for et bedre personvern” til Fornyings- og administrasjonsdepartementet, FAD.

Datatilsynet er meget tilfreds med at FAD allerede i juni samme år meddelte at det for 2006-budsjettet ble bevilget to millioner kroner ekstra til satsing på kommunikasjonstiltak. Datatilsynets budsjettramme ble også for 2007 øket med to millioner kroner til formålet. Dette har gjort det mulig for Datatilsynet å realisere kommunikasjonsprosjekter som kan gi både befolkningen som rettighetshavere og virksomhetene som plikthavere en øket oppmerksomhet, refleksjon og kunnskap om viktige personvernspørsmål.

Straks etter at Datatilsynet var blitt underrettet om ekstrabevilgningen ble det etablert to forskjellige prosjekter for å følge opp den ekstra kommunikasjonssatsingen.

Ungdom og personvern

I tråd med satsingsforslaget, og føringer i tildelingsbrevet fra Fornyings- og administrasjonsdepartementet, ble ungdom definert som en sentral målgruppe for kommunikasjonstiltakene. Det ble tidlig klart at det ville være hensiktsmessig å utvikle et undervisningsopplegg knyttet til de nye læreplanene i skoleverket, som inneholder kompetansekrav når det gjelder IKT og personvern. Ut fra denne forutsetningen ble det etablert et samarbeid med Utdanningsdirektoratet og Teknologirådet. Begge instansene har bidratt med faglige ressurser inn i prosjektet. I tillegg stilte Utdanningsdirektoratet også med økonomiske midler.

Ungdom har et effektivt ”spamfilter” for autoritær informasjon. De vil helst være i fred og oppdage verden på egenhånd. Undervisningsopplegget ”Det er du som bestemmer” er derfor søkt laget på ungdoms premisser og i deres formdrakt. Budskapet er at de unge i stor grad kan ta kontroll over sine egne opplysninger og at de selv er ansvarlig for å respektere andres rett til privatlivets fred.

Undervisningsopplegget består av et hefte med faktaopplysninger, historier fra virkeligheten og diskusjonsoppgaver. Dessuten er det laget veggplakater til klasserommet, nettstedet www.dubestemmer.no og en multimediepresentasjon med filmsnutter for lærere. Målgruppen er elever i ungdoms- og videregående skole.

Kampanjen ”Du bestemmer” (www.dubestemmer.no) ble for øvrig lansert 29. januar 2007.

Kommunikasjonstiltak overfor virksomhetene

Den nevnte personvernundersøkelsen fra 2005 viser tydelig at man i både private og offentlige virksomheter har liten kunnskap om, og følgelig liten grad av etterlevelse av de konkrete kravene som stilles i personvernlovgivningen. Mange mener at kravene i personopplysningsloven ikke gjelder for dem. Dette gjelder selv om de behandler personopplysninger, og denne behandlingen dermed vil være omfattet av loven. Få av virksomhetene oppgir at de etterlever regelverket i sin helhet. Det påvises spesielt mangler i forhold til kravene om informasjonssikkerhet, internkontroll og informasjon til den som opplysningene gjelder. Hele 74 prosent av virksomhetene mener selv at mangel på kunnskap er hovedårsaken til at personvernlovgivningen ikke blir etterlevd.

Funnene fra personvernundersøkelsen bekrefter Datatilsynets erfaringer gjennom de senere årenes tilsynsvirksomhet. Det er derfor et samlet inntrykk at det er behov for å motivere og legge til rette for økt etterlevelse av personvernlovgivningen ute i virksomhetene, offentlige så vel som private.

Det er derfor etablert et ekstra satsing også overfor virksomhetene som tar sikte på å bevisstgjøre om pliktene etter personvernlovgivningen, motivere, og gi tilstrekkelig kompetanse og veiledning til å etterleve regelverket.

Det utarbeides et nytt og omfattende veiledningsmateriale knyttet til internkontroll, inkludert informasjonssikkerhet. Materialet inkluderer:

- Et motiverende temahefte
- En helhetlig veileder om internkontroll
- Ferdige ”maler” for nødvendige internkontrolldokumenter
- Spesialtilpasset materiale for virksomheter som kun har personopplysninger om egne ansatte og kunder. Det er utarbeidet et ”typeeksempel” som virksomhetene kan redigere og tilpasse sin egen virkelighet.
- Et støtteverktøy som hjelper virksomheten med å kontrollere sin etterlevelse opp mot regelverket.

Kampanjen lanseres februar 2007. Over 2 000 virksomheter kontaktes med tilbud om oppfølging og veiledning, blant annet gjennom seminarer i Trondheim, Bergen og Oslo.

Direkte publikumskontakt

Datatilsynet legger stor vekt å ha god tilgjengelighet og service overfor de enkeltpersoner eller virksomheter som av eget initiativ søker råd og veiledning når det gjelder personvernlovgivningen, enten det dreier seg om rettigheter, plikter eller andre tilgrensede temaer. En betydelig del av ressursene brukes derfor 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 fire 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. I tillegg til å besvare telefoner og e-post, bidrar Frontservice også med vanlig juridisk saksbehandling.

Hvor mange og hvor lenge?

Datatilsynet har registrert 9 163 besvarte telefonhenvendelser i meldingsåret. Dette er noe mindre enn året før. Det er flere årsaker til dette, blant annet:

- Stadig mer og bedre informasjon er å finne på Datatilsynets hjemmeside
- En økende andel sender e-post fremfor å ringe
- Antall henvendelser mht direkte markedsføring er gått markant ned

En del telefoner går også til øvrige saksbehandlere, som ikke fører statistikk over besvarte telefonhenvendelser. Som følge av at den juridiske førstelinjetjenesten tidvis var lite bemannet høsten 2006 er andelen ikke-registrerte telefonbesvarelser blitt noe høyere enn vanlig.

Hva handler henvendelsene om?

I likhet med året før er "Arbeidsliv" fortsatt det temaet det kommer flest henvendelser om. Dette skyldes i første rekke den betydelige oppmerksomheten omkring arbeidsgivers innsyn i e-post, tilsynssakene og utarbeidelse av forskriftsbestemmelser om e-post.

”Informasjonssikkerhet” er også et tema som mange henvender seg til Datatilsynet om. Naturlig nok kommer de aller fleste henvendelsene da fra representanter for plikthaverne, det vil si de ”behandlingsansvarlige” etter personopplysningslovens terminologi. Det har også, blant annet som følge av stor medieoppmerksomhet, vært et økende antall henvendelser relatert til bruk av fødselsnummer.

Tabellen nedenfor viser telefonhenvendelsene fordelt på tema, og hvorvidt innringer opptrer som (eller på vegne av) plikt- eller rettighetshavere.

Tema	Plikt	Rett	Sum	Prosent
Arbeidsliv	703	787	1490	16 %
Forskning	198	22	220	2 %
Fødselsnummer	64	628	692	8 %
Helseforvaltning	118	67	185	2 %
Informasjonssikkerhet	1 233	43	1 276	14 %
Internasjonalt (overføring til utlandet)	168	16	184	2 %
Internett	165	241	406	4 %
Kameraovervåking	425	283	708	8 %
Kunde-/medlemsregister	262	131	393	4 %
Melding/konsesjon	710	42	752	8 %
Reservasjon/DM	70	617	687	7 %
Skole/barnehage	170	61	231	3 %

Sosial/trygd/barnevern	98	84	182	2 %
Økonomi	124	533	657	7 %
Annet	337	763	1056	12 %
Sum	4845	4318	9163	100 %

Det har vært en fortsatt nedgang i henvendelser om direkte markedsføring. Disse utgjorde 7 prosent av telefonhenvendelsene i 2006, mot henholdsvis 10 prosent i 2005 og 18 prosent i 2004.

Besvarelse av e-post

Det er i meldingsåret besvart 3 058 ordinære publikumshenvendelser per e-post. Til sammenlikning var tallet tilsvarende 3 080 året før. Reelt sett har det likevel vært en økning i antallet henvendelser per e-post, idet en større andel enn tidligere er gått inn til journalføring og ordinær saksbehandling. Disse blir dermed registrert i saksbehandlingssystemet, fremfor i tellingen av e-post.

Etter at det ble satt ekstra fokus på oppfølging av innkomne e-post er den gjennomsnittelig svartiden kommet ned i to dager. Ved årsskiftet var det ingen ubesvarte e-posthenvendelser.

Veiledningsmøter om informasjonssikkerhet

Datatilsynet legger vekt på gi råd og veiledning til virksomheter som arbeider med å sikre personopplysninger i samsvar med regelverket. Mye av veiledningen skjer via besvarelse av telefon- og e-posthenvendelser, men i en del saker er veiledning gjennom møter mer hensiktsmessig. Det ble derfor gjennomført ca 70 veiledningsmøter med informasjonssikkerhet som hovedtema. Veiledningsmøtene er ofte knyttet til et 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 har også ønsket dialog for å oppnå en bedre forståelse for regelverkets krav.

Personvernrapporten etterspørres

Som et supplement til den ordinære årsmeldingen for 2005 ble det, i likhet med de to forutgående år, utarbeidet en mer popularisert versjon av årsmeldingen, "Personvernrapporten 2006". Den ble trykket i ni tusen eksemplarer og distribuert til i underkant av fem tusen mottakere. Det er i ettertid kommet inn etterbestillinger av over 3 000 eksemplarer, hvorav flere klassesett til bruk i undervisning. Dette innebærer en tredobling i forhold til året før. Den store økningen i etterspørsel etter Personvernrapporten tyder på at publikasjonen er blitt godt kjent i målgruppene.

www.datatilsynet.no

Datatilsynet legger stor vekt på å bruke nettsiden aktivt. Det ble i meldingsåret publisert 72 egenproduserte nyhetsartikler på forsiden. I tillegg ble det laget to nye temasider med mange artikler i hver, samt bygget opp en bedre side for regelverk.

2 700 personer står på abonnentlisten for nyhetsbrev. Estimert antall daglig besøkende på hjemmesiden er steget fra i underkant av 1 200 i 2006 til mer enn 1 500 i 2007. Hjemmesiden har beholdt sine fem stjerner i Norge.no sin kåring av offentlige nettsteder.

Kurs og foredrag

Foruten de egenarrangerte seminarene i forbindelse med personvernombudsordningen gir Datatilsynet ikke tilbud om kurs eller seminarer i egen regi. Imidlertid er det høyt prioritert å stille opp når noen tar kontakt med ønske om Datatilsynets deltakelse på ulike kurs og seminarer i regi av andre. Det har i meldingsåret vært en betydelig etterspørsel etter foredragsholdere fra Datatilsynet, som stilte opp på hele 157 ulike seminarer og konferanser, mot tilsvarende 92 i 2005 og 70 i 2004.

Mediekontakt

I løpet av 2006 har Datatilsynet besvart 1 425 henvendelser fra mediene, i form av å gi intervjuer og kommentarer til aviser, tv, radio eller internettbaserte medier. Datatilsynet har også vært representert i mange debatter på radio og tv.

Tabellen nedenfor viser antallet registrerte nyhetsoppslag i internettbaserte medier:

	2004	**2005**	**2006**
Ant. medieoppslag	2 189	4 143	3 602

Nedgangen i antall registrerte medieoppslag fra 2005 til 2006 skyldes i første rekke at det høsten 2005 var ekstraordinært mange oppslag som følge av sakene omkring arbeidsgivers innsyn i e-post.

Nyheter som kommer i trykk (fagtidsskrifter og lokale medier) eller på tv/radio, uten at disse samtidig gjøres tilgjengelig på Internett, er ikke med i tallmaterialet.

Saksdokumenter og meroffentlighet

Datatilsynet praktiserer meroffentlighet, og postjournalen er tilgjengelig via den elektroniske postjournalen (EPJ) som administreres av Statskonsult, på vegne av departementer og direktorater. Tjenesten per dato er kun tilgjengelig for redaksjoner og media. Det er i 2006 blitt sendt ut 1 111 til journalister etter bestilling via den elektroniske postjournalen. I tillegg er det sendt ut 544 dokumenter til virksomheter, organisasjoner eller privatpersoner.

7 Tilsyns- og sikkerhetsarbeid

De fleste virksomheter innen offentlig og privat sektor kan underlegges tilsyn etter personopplysningsloven. Datatilsynet gjennomfører, i likhet med de fleste tilsynsorgan, risikobasert tilsynsvirksomhet. Dette innebærer at innsatsen rettes inn mot områder hvor sannsynligheten for, og konsekvensen av, regelverksbrudd er høyest.

Grunnlaget for tilsynsarbeidet ligger i dokumentet "Strategi og metodikk for operativt tilsyn med personopplysningsloven". Denne strategiplanen omtaler Datatilsynets forvaltningsområde som helhet og legger føringer i forhold til operativt tilsyn. Virksomhetsplanen legger føringer for valg av sektorer, bransje og/eller tema. I tillegg er oppfølging av tips og klager fra publikum viktig.

Etter at avvikene er lukket hos den enkelte virksomhet vil Datatilsynet gjerne bidra til at liknende virksomheter unngår å gjøre de samme feilene. Metodene som benyttes er blant annet:

- kontakt med aktuell bransjeforening eller andre bransjeorganer for å drøfte lovforståelse og tolkning, initiere bransjenorm eller publisere fagartikler i medlemsblader.
- kontakt med eierinteressene (for eksempel et departement)
- å beskrive problemer i media, lage veiledninger som legges ut på tilsynets hjemmeside, eller bidra med foredragsvirksomhet
- å starte prosjekter hvor de nye problemstillingene kan gjennomgås.

Generelle funn

Personvernet er under press på nær sagt alle områder hvor det er gjennomført tilsyn i 2006. Når den enkelte beslutningstaker står ovenfor et dilemma hvor personvernet enten hindrer det man ønsker å gjøre, eller krever at man endrer planer, går beslutningen ofte i personvernets disfavør.

Brudd på bestemmelser om informasjonssikkerhet og internkontroll er fortsatt fremtredende. Gjennomgående er få virksomheter i stand til å dokumentere informasjonssikkerheten slik regelverket foreskriver. Videre er det mange virksomheter som ikke har etablert rutiner for behandling av personopplysninger. Mye er derfor overlatt til sedvane i bransjen. I mange bransjer vil dette, på tross av mangelfulle systemer, likevel resultere i en forsvarlig håndtering av opplysningene. Det kan imidlertid ofte være bare gunstige tilfeldigheter som gjør at personopplysninger ikke kommer ut av kontroll.

Det skjer trolig daglig omfattende krenkelser av personvernet som ikke blir stilt under et kritisk lys. Datatilsynet har for eksempel i lang tid har hatt vesentlig bekymring når det gjelder helsesektoren. Kombinasjonen av liberal tilgangskontroll og mangelfull bruk av logger gir liten reell kontroll med hvem som faktisk skaffer seg tilgang til sensitive personopplysninger. Helsesektoren er trolig langt fra enestående i slik sammenheng. De tilsynene som ble gjennomført i finanssektoren avdekket en tilsvarende liberal praksis med tilgang til kontoopplysninger. Utlevering av denne typen personopplysninger til utenforstående kan innebære en betydelig integritetskrenkelse for de som rammes av dette, det være seg kjendiser eller ikke.

Datatilsynet merker seg at respekten for bestemmelser om sletting gjennomgående er liten. Dette gir grunnlag for bekymring når man samtidig vet at terskelen for å registrere

opplysninger er lav. Mange virksomhetsledere synes ikke å ha reflektert over at overskuddsinformasjon og opplysninger som ikke lenger er nødvendige for formålet med registreringen skal slettes. Tvert imot hevder mange at langvarig oppbevaring ”kan være nyttig” for virksomheten, uten at de klarer å begrunne den fortsatte lagringen på en saklig troverdig måte.

Det blir generert betydelig mengder overskuddsinformasjon i ulike systemer. Et eksempel er internettsøkemotorenes lagring av søk og IP-adresse. Dette gjør det mulig å avdekke hvilke søk en bruker har foretatt. IP-adresser som etter hvert blir mer og mer statiske (byttes ikke ut) vil langt på vei kunne knyttes til enkeltindivider. Lagring av både IP-adresse og søk vil raskt kunne falle i kategorien overskuddsinformasjon.

Nedenfor følger en kort presentasjon av funn innen ulike sektorer. Tilsynene innen helse, finans- og justissektorene er trukket inn i den nærmere gjennomgangen i årsmeldingens del to.

Sletting av personopplysninger i rusinstitusjoner

Datatilsynet hadde en antakelse om at det kunne være uklarheter med hensyn til sletting av personopplysninger innen rusomsorgen. Disse institusjonene behandler mange sensitive personopplysninger. Eierforhold, organisering og type tilbud er svært varierende.

Det ble valgt seks private og seks statlige/kommunale rusinstitusjoner. Prosjektet ble gjennomført som en brevkontroll med påfølgende stedlig tilsyn hos to private og to kommunale institusjoner. Formålet var å belyse om sletting av personopplysninger skjedde i tråd med bestemmelsen i personopplysningslovens § 28.

Det ble utformet et brev med totalt 12 spørsmål som tok sikte på å fastslå hvem som er behandlingsansvarlig for behandling av personopplysninger i institusjonen, hvilke lover og bestemmelser som eventuelt gjelder spesielt for denne institusjonen, og hvilke rutiner for sletting som foreligger.

Tilsynspersonalet hadde allerede før prosjektets start forutsett at det ville være stor forskjell i tilnærming til sletting, avhengig av om institusjonene var underlagt arkivloven eller ikke. Svarene gjorde det klart at det også er vesentlig forskjell på institusjonene med ansatt helsepersonell som driver en eller annen form for medisinsk behandling, og de institusjoner som kun driver omsorg eller rehabilitering. For den første gruppen gjelder helsepersonelloven og journalforskriften, som har klare regler for hva som kan slettes og hvordan retting og sletting skal skje. Kunnskapen om bestemmelsene om sletting som følger av personopplysningsloven og helseregisterloven synes å være relativt dårlig. Konkrete rutiner for å håndtere personvernlovverket i den enkelte institusjon mangler i all hovedsak.

Opptak av telefonsamtaler

Prosjektet ble opprettet på bakgrunn av en del henvendelser fra publikum som tydet på at opptak av telefonsamtaler er mer utbredt enn det tilsynet har hatt kunnskap om.

De utvalgte tilsynsobjektene er hentet fra en liste hos bransjeorganisasjonen NORDMA over telemarkedsførere. Det ble sendt ut forespørsel til 33 virksomheter.

Tilsynsmyndigheten mottok svar fra 30 av disse. Rundt halvparten av virksomhetene gjør lydopptak.

Materialet viser en blanding av manuelt initierte opptak (ca. 70 prosent) og automatisk (30 prosent). Noen virksomheter tar opp hele samtaler, mens andre er mer selektive og tar for eksempel kun opp selve avtaleinngåelsen. Et flertall av virksomhetene oppgir behov for dokumentasjon av avtale som viktigste årsak til lydopptak (ca. 70 prosent), mens resterende fordeler seg på kontroll av ansatte, kvalitetskontroll, opplysningskvalitet og kontroll av kundebehandling. Flere virksomheter oppgir mer enn en begrunnelse. Rundt 70 prosent av virksomhetene har innhentet samtykke for behandlingen. Tilsvarende oppgir rundt 80 prosent av virksomhetene at de informerer kundene om at lydopptak blir gjort.

Datatilsynet kartla også rutiner for sletting og utlevering. Det er flere virksomheter som beholder opptak, uavhengig av om avtale inngås eller ikke. Alle oppgir å slette opptak senest etter ett år. Opptak utleveres til motpart i tilfelle konflikt om avtaleinngåelse.

Personprofiler

Personopplysningsloven regulerer bruk av personprofiler. Datatilsynet har hatt ønske om større kunnskap om temaet, og valgte å gjennomføre et prosjekt for å avdekke i hvilken grad bruk av personprofiler representerer et problem, eller ikke. Kartleggingen vil gi et bedre grunnlag for å trekke opp noen grenselinjer når det gjelder bruk av personprofiler.

Foreløpige analyser av materialet tyder på at de fleste av de 20 virksomhetene som ble kartlagt gjør bruk av personprofiler. Det ser imidlertid ut til at få av disse oppfyller regelverkets krav om å innhente samtykke og gi tilstrekkelig informasjon til de berørte.

Private helseforsikringer

Det ble gjennomført en undersøkelse mot private helseforsikringer om var initiert fra artikkel 29-gruppen. Arbeidet med disse tilsynene følger en fremdrift som er utenfor tilsynets kontroll og er i skrivende stund ikke avsluttet. Tilsynene er gjennomført, men analyse av materiale og videre fremdrift er ikke avklart.

Private etterforskere

Datatilsynet ønsket å se nærmere på hvilke rammebetingelser private etterforskere arbeider under. Tidligere tilsyn innenfor arbeidsliv avdekket at slike virksomheter driver aktiviteter som ligger svært tett opp til det arbeidet politiet gjør, uten at hjemmelsgrunnlaget er tilsvarende avklart.

Det er få store firmaer innen bransjen. Tilsynet gjennomførte kontroll hos to aksjeselskaper og ett enkeltmannsforetak. Felles for disse var at bare én person var tilknyttet etterforskning. Det var, etter tilsynets vurdering, stor spredning både i type saker, etterforskningsmetoder og hvor seriøst virksomhetene forholdt seg til håndtering av personopplysninger.

Datatilsynet konkluderte med at etterforskerne var å anse som behandlingsansvarlig. Tilsynsobjektene manglet helt eller delvis dokumentert informasjonssikkerhet og tilstrekkelig internkontroll.

I vedtakene overfor de private etterforskerne ble regelverkets krav til informasjon overfor den registrerte presisert. Dette fører i praksis til at hemmelig overvåking og etterforskning er ulovlig. Det er ingen grunn til å anta at andre private etterforskere på en bedre måte oppfyller lovens krav. Det er stort behov for informasjon til bransjen med hensyn til behandlingsansvar, dokumentasjonsplikt og ikke minst informasjonsplikten.

Et initiativ mot Justisdepartementet for å initiere en lisensordning er aktualisert. Per i dag synes Datatilsynet å være det eneste kontrollorgan overfor bransjen.

Private friskoler

Våren 2006 gjennomførte Datatilsynet tilsyn ved seks friskoler. Flere av skolene hadde internat, og en gjenganger var ønsket om et rusfritt miljø. For å oppnå dette benyttet flere skoler ulike former for rusmiddeltester. Datatilsynet mener at skolene må ha konsesjon for å kunne foreta rustester, men påpeker samtidig at saken bør få en rettslig avklaring. Datatilsynet har derfor spilt inn problemstillingen til Kunnskapsdepartementet i forbindelse med revisjon av friskoleloven.

Videre åpnet flere av skolene for elektroniske søknader, hvor søker må oppgi sitt fødselsnummer. I de fleste tilfeller var ikke skolens internettside tilstrekkelig sikret, og derfor ikke egnet til dette.

Det ble ikke avdekket noen form for kameraovervåking på skolene, eller logging av elevers bruk av Internett. Det ble heller ikke avdekket opptakskriterier i strid med personopplysningsloven.

Private barneverninstitusjoner

Tilsyn ble gjennomført ved i alt syv private barneverninstitusjoner. Disse institusjonene er underlagt konsesjon fra Datatilsynet. Konsesjonsvilkårene blir, etter det tilsynet erfarte, relativt godt etterlevd. Rutiner knyttet til innsyn og informasjon var likevel et unntak fra dette. Enkelte problemer med hensyn til sletting ble også avdekket, men er i etterkant løst gjennom rundskriv fra Barne- og likestillingsdepartementet.

For å få plassert behandlingsansvaret på rett sted, og å få overført erfaringer og konklusjoner også til andre virksomheter i sektoren, vil det bli gjennomført møter med relevante parter.

Kameraovervåking

Når det gjelder kameraovervåking var Datatilsynet i meldingsåret særlig interessert i å se nærmere på digitaliserte overvåkingssystemer, blant annet systemer som overfører bilder til en sentral vaktenhet. Kostnadene ved å starte med kameraovervåking synker stadig, og stadig flere aktører tar metoden i bruk. Datatilsynet antar at dette også fører til at flere enn før setter i gang med ulovlig kameraovervåking.

Det ble gjennomført seks tilsyn med vaktselskaper hvor disse hadde overføring av billedmateriale fra kundene til vaktselskapets alarmsentral. For hvert vaktselskap ble det også gjennomført tilsyn med en kunde som benytter aktuell tjeneste fra selskapet. I tillegg ble det gjennomført to tipsbaserte kontroller.

Av de kontrollerte vaktselskapene betraktet halvparten slike tjenester som et satsningsområde for massemarkedet. De øvrige hadde tjenestene som en spesialtilpasning for enkelte større kunder.

Løsningene tilpasset massemarkedet baserte seg på overføring av, eller tilgang til, billedmateriale ved en utløst alarm, eller ved en avtalt kontroll. Vaktselskapene betraktet det ikke som hensiktsmessig å lagre alt billedmateriale for kundene. Denne type tjenester vil normalt anses som et databehandlerforhold, hvor den behandlingsansvarlige har satt ut hele eller deler av behandlingen til en ekstern part. Bestemmelsen om databehandlere

gjelder imidlertid ikke direkte i forhold til ordinær kameraovervåking (personopplysningslovens kapittel VII).

Personopplysningslovens generelle bestemmelser ble imidlertid lagt til grunn ved tilsynene, og samtlige kontrollerte behandlingsansvarlige (kunder) ble pålagt å etablere databehandleravtaler med vaktselskapene. Vaktselskapene ble på sin side pålagt opphør av sin behandling, med mindre den ble regulert i en databehandleravtale.

Bransjen har gitt signal om at den vil kontrollere de avtalene og rutinene som ligger i sine egne frivillige godkjenningsordninger.

Ett av tilsynene, kameraovervåking i regi av Mandal havnevesen, er trukket ut og drøftes spesielt i årsmeldingens del II.

Arbeidsliv

Det ble gjennomført flere tilsyn mot taxisentraler. Det ble avdekket uklarheter når det gjelder behandlingsansvaret, samt rutiner for håndtering av personopplysninger, inkludert sletting.

To av tilsynene knyttet seg til arbeidsgivers innsyn i elektronisk post. Datatilsynet konkluderte i disse sakene at arbeidsgiver hadde berettiget interesse i å foreta innsyn.

De øvrige tre tilsynene var knyttet til drosjenæringens system for såkalt ”flåtestyring”. Bakgrunnen for tilsynene var at Datatilsynet hadde mottatt en del klager fra lisenshavere som mener at det er en for omfattende overvåking av bilparken. Tilsynet var ved årsskiftet ikke avsluttet.

Ut over dette har det vært ført to tilsyn hvor tema var overvåking av ansatte blant annet ved bruk av ”doomkameraer”. I disse er kameraet skjult i en mørk kuppel som hindrer den overvåkede i å verifisere hvorvidt vedkommende er innen dekningsområdet for kameraet eller ikke. Sakene har preg av uenighet mellom arbeidsgivere og arbeidstakere om hvor mye overvåking arbeidsgiveren har et saklig grunnlag for å kunne utføre.

DEL II

8 Temaer og tendenser i 2006

Datatilsynet vil trekke frem seks tendenser som har vært særlig fremtredende i meldingsåret.

Tendensene er hentet fra erfaringer fra tilsyn og saksbehandling, fra høringsarbeidet, deltakelse i forskjellige arbeids- og styringsgrupper, samt gjennom saker som Datatilsynet er blitt oppmerksom på gjennom medieomtale. Beskrivelsen av tendensene bygger på en grundigere omtale andre steder i årsmeldingen.

8.1 Farvel anonymitet

Muligheten til å være anonym eller benytte alternativer som ikke etterlater spor er i ferd med å forsvinne fra det norske samfunnet. Datatilsynet har observert denne utviklingen over flere år. Årsaken til utviklingen er trolig en blanding av lav bevissthet i befolkningen rundt behovet for anonyme alternativer, og at de som utvikler nye teknologibaserte løsninger ikke legger tilstrekkelig vekt på personvern. I stadig flere sammenhenger forventes vi å identifisere oss eller etterlate elektroniske spor, selv om det ikke kan påvises saklig grunn for registreringen.

Bruk av kontaktløse brikker har satt fortgang i utviklingen. Brukeren trenger ikke å foreta seg noe for å aktivere sporingen. En direkte, kontaktløs kommunikasjon mellom brikke og system gjør registreringen til en enkel jobb, enten det dreier seg om å åpne en dør, eller å identifisere personer.

Brikker som kan fjernavleses innebærer at den enkelte i mindre grad kan vite når vedkommende legger igjen elektroniske spor. Årsaken er at man ikke trenger medvirkning fra den enkelte. Dette vil gjøre det vanskelig folk flest å følge med på hvor omfattende overvåkingspresset er, og hvordan dette utvikler seg.

Slutt på fri ferdsel?

Innen samferdselssektoren bygges det i akselererende grad opp en infrastruktur som gir muligheter for overvåking. Dette skjer innen alle transportformer. Dette kan være ved bruk av kamerateknologi, RFID-brikker (som i Autopass), elektronisk billettering innen offentlig kommunikasjon, flåtestyring, og såkalte ”svarte bokser” i bilene, som løpende registrerer kjøremønsteret. I tillegg er det under planlegging og oppbygging et obligatorisk system for satellittbasert overvåking.

Datatilsynet har registrert at denne utviklingen har kunnet foregå nærmest uten debatt.

Da Personvernnemnda tillot lagring av passeringsopplysninger for ”sporingsfrie brikker” i helautomatiske bomstasjoner, etterlyste den samtidig en debatt om helheten i de tiltakene som innskrenker retten til å kunne ferdes i det norske samfunnet uten å bli registrert og overvåket. Personvernnemnda viser i vedtaket til at den er henvist til å begrense sin saksbehandling til en vurdering av den aktuelle klagen, men oppfordrer til en gjennomgang på området.

Helautomatiske bomstasjoner og nye biometriske pass som kan avleses på avstand er allerede innført, og vil komme til å omfatte alle reisende i årene fremover. Systemene er enten obligatoriske, eller alternativene bortfaller i praksis fordi de blir lite tilgjengelige, eller kostbare for den enkelte å ta i bruk.

Overvåkingssystemer kan misbrukes, og de endrer maktbalansen mellom den enkelte og det offentlige. Datatilsynet er sterkt bekymret for de svake begrunnelsene for lagringen av alle våre bevegelser, og den manglende viljen til å vurdere risikoen ved systemene. Det kan virke som om systemene tas i bruk bare fordi løsningene finnes, og fordi det er effektivt og praktisk for overvåkeren at individene automatisk blir identifisert. De som står bak utviklingen av de nye teknologiske løsningene har i liten eller ingen grad vurdert om fordelene oppveier innhogget i den enkeltes personvern.

Sporingsbrikker er et spesielt kraftig overvåkingsverktøy dersom man kombinerer det med en "klassisk" teknologi som kameraovervåking. Datatilsynet har i meldingsåret sett eksempler på slike kombinerte systemer, blant annet overvåking av båter og havneanlegg i Mandal. Det er tydelig at flere aktører arbeider med forskjellige teknologier i kombinasjon med bruk av kamerasystemer, for bedre å kunne identifisere enkeltpersoner direkte, eller indirekte via kjøretøyer og andre gjenstander.

Elektroniske merking av dømte, demente eller arbeidstakere

Spørsmålet om hjemmesoning med elektronisk merking av dømte voldsforbrytere ble sendt på høring i 2006. Datatilsynet påpekte at forslaget innholder uavklarte spørsmål i forhold til hvor detaljert overvåkingen skal være.

Overvåking av enkelte kriminelle reiser spørsmål om vi ønsker et samfunn der "uønskede" og "vanskelige" grupper av mennesker blir elektronisk merket. Tilsynet antar at dersom man først har valgt å åpne for elektronisk merking av en type kriminelle, har man overskredet en terskel, og neste skritt på veien mot økt bruk av denne type tiltak vil være langt enklere å ta.

Med jevne mellomrom har også spørsmålet om elektronisk merking av sykehjemspasienter dukket opp. Datatilsynet presiserer at merking er et tvangstiltak som må vurderes ut fra helselovgivningen i det enkelte tilfelle. Tilsynet mener imidlertid det er etisk betenkelig om sykehjemmene skulle få anledning til å kompensere for manglende personale og manglende diagnostikk av senildemente, med elektronisk merking av alle pasienter.

Datatilsynet foretok i meldingsåret flere tilsyn for å se på såkalt "flåtestyring", som innebærer en type overvåking og sporing av ansatte gjennom lokalisering av tjenestebiler og mobiltelefoner. Slik sporing av arbeidstakere reiser spørsmål om hvor detaljert og kontinuerlig det er rimelig at en ansatt skal kunne følges av sin arbeidsgiver.

8.2 Voksende databaser og informasjonssamlinger

Gjenbruk, nye formål og evig lagring svekker den enkeltes mulighet til å ivareta eget personvern

Gjenbruk av personopplysninger til nye formål er problematisk for personvernet av flere årsaker. Den registrertes rett til kunnskap om hva opplysningene om ham eller henne skal brukes til står helt sentralt i europeisk personverntenkning. Den registrerte blir informert om ett formål, og danner seg en forståelse av hvordan opplysningene skal brukes. Dersom opplysninger blir benyttet til nye formål, som den registrerte ikke har overskuet, fjerner man muligheten til oversikt. Uten oversikt blir den enkelte fratatt muligheten til å bruke sine øvrige rettigheter etter personvernlovgivningen. Den som har opplysninger får mer makt på bekostning av den registrerte. Forskjellige formål kan også innebære ulike krav til kvalitet og etterrettelighet. Opplysninger som er innsamlet for ett spesifikt formål, er ikke automatisk tilstrekkelige og relevante for alle andre formål.

Datatilsynet har observert at stadig flere aktører ønsker lagring i stadig lengre tid, også av opplysningstyper som tidligere har blitt slettet. Respekten for slettebestemmelsene har gjennomgående vist seg å være liten. Når man samtidig vet at terskelen for å registrere opplysninger er lav, gir dette grunnlag for bekymring. Mange virksomhetsledere hevder at langvarig oppbevaring "kan være nyttig" for virksomheten, men få klarer å gjøre argumentet mer håndgripelig.

Datatilsynet fikk i 2006 også høringssaker der ønsket om videre lagring sto sentralt. Det tidligere overvåkingspolitiet - POTs arkiver ble foreslått lagret videre, med en rett til å komme med tilleggsopplysninger for de registrerte som hadde fått innsyn. Dette ble foreslått til tross for at Stortingets forutsetning var at det skulle være mulig med sletting.

Flere får tilgang til store, overgripende databaser og journalsystemer

I en situasjon der flere og flere store databaser og informasjonssystemer får flere brukere med rett til å logge seg på, lese og bruke personopplysninger, må man ta utfordringen med mulig internt misbruk alvorlig.

I 2006 så Datatilsynet, i samarbeide med Helsetilsynet, på bruken av elektronisk pasientjournal i Helse Bergen HF og ved Akershus Universitetssykehus HF. Tilsynene konkluderte med at pasientjournalene ved disse to helseforetakene ikke var godt nok beskyttet mot intern "snoking" fra ansatte som ikke deltar i behandlingen av pasienten. Datatilsynet og Helsetilsynet mente dette hadde sammenheng med at sykehusene ikke hadde tilpasset journalsystemene til hvordan de faktisk hadde valgt å organisere seg internt.

Datatilsynet mener det er alvorlig at helseforetakene ikke evner å gi tilstrekkelig fortrolighet rundt opplysninger de mottar for å yte helsehjelp. Det er ikke tilstrekkelig at alle som får tilgang til journalene har taushetsplikt. Sykehusene må aktivt sørge for at bare de som deltar i pasientbehandlingen får tilgang.

I meldingsåret dukket også opp spørsmål om taushetsplikten for helsepersonell i det hele tatt beskytter den enkelte pasient mot intern snoking ved helseinstitusjonene. Under etterforskningen av en sak der en leder ved Helgeland sykehus snoket i pasientjournaler, kom politiet frem til at taushetsbestemmelsene ikke var brutt så lenge opplysningene ikke var blitt utlevert til andre. Datatilsynet hevdet at sykehuset likevel hadde et ansvar for å sikre sine systemer, og sykehuset ble ilagt virksomhetsstraff for brudd på plikten til å ha tilstrekkelig informasjonssikring.

Datatilsynet har grunn til å tro at personopplysninger er for dårlig sikret mot intern snoking, ikke bare i sykehus og andre helseinstitusjoner, men generelt i virksomheter hvor store mengder personopplysninger behandles, det være seg i privat som i offentlig sektor. Problemet med internt misbruk får ofte ikke tilstrekkelig oppmerksomhet når man gir store brukergrupper direkte tilgang til mengder av opplysninger. Blant annet påpekte Datatilsynet dette problemet i forbindelse med forslaget om å gi politiet rett til å gå inn i valutaregisteret uten krav om at det bare skjer i forbindelse med etterforskning av konkrete saker.

8.3 Etterforskning i privat regi

De siste årene har Datatilsynet arbeidet med flere vanskelige saker der privat etterforskning har vært i fokus. Private etterforskere har blant annet bistått arbeidsgivere med å undersøke påstått illojalitet fra ansattes side. Blant de metodene som har vært anvendt er gjennomgang av e-poster og filer som ansatte har lagret på arbeidsgivers informasjonssystem.

Musikk og filmbransjen har i lang tid hevdet at de taper store summer på systematiske brudd på Lov om opphavsrett. Det er særlig såkalte fildelingstjenester som har vært fremholdt som kanal for spredning av opphavsrettlig beskyttet materiale. Rettighetshavernes interesseorganisasjoner har ikke vært tilfreds med politiets håndtering av lovbruddene, og har derfor i flere land tatt initiativ til å etterforske slike saker på eget initiativ. I 2006 arbeidet Datatilsynet med spørsmål om konsesjon til et advokatfirma som vil overvåke fildelere på Internett.

Datatilsynet har de siste årene også fått flere henvendelser fra ansatte som føler et ubehag ved at de blir utsatt for "skjulte kunder", det vil si personer som under dekke av å være kunder undersøker servicenivå eller oppførsel på oppdrag fra arbeidsgivere. Arbeidsgiver fremholder slike tiltak som en hensiktsmessig måte å utøve kontroll av kvalitet på egne tjenester, mens ansatte på sin side gjerne kan oppleve et stort ubehag ved dette.

Det er ikke uproblematisk at private aktører skal etterforske lovbrudd eller misligheter uten noen form for fullmakt fra lovgivende myndighet. Politiets kommunikasjonskontroll og etterforskning er regulert i straffeprosessloven. Infiltrasjon og provokasjon er metoder politiet bare kan benytte når kravene i Riksadvokatens retningslinjer er oppfylt. Tilsvarende gir Lov om vaktvirksomhet retningslinjer til vaktselskapene. Prosessreglene som gjelder politiets arbeid garanterer den mistenkte en rekke rettigheter. Regelverket har blitt utviklet gjennom flere år som følge av påvirkning fra instanser som har tydelige roller; Storting, regjering, politi og domstoler. Offentligheten har hatt betydelig innsyn og mulighet til påvirkning av reglene, gjennom høringer, debatter og direkte dialog. Dette er ikke tilfelle når det gjelder privat etterforskning. Derfor setter slik etterforskning personvernet under et særlig press. Når en privat aktør etterforsker, vil den mistenkte være avskåret fra de rettighetene som prosessreglene skal sikre. Datatilsynet har i flere saker også sett at de metodene man har til hensikt å bruke ikke har vært kommunisert godt nok til de personene som er under mistanke. Terskelen for å sette i verk til dels svært inngripende tiltak har vært lav.

8.4 Biometri gir nye utfordringer

Flere og flere aktører ønsker å ta i bruk biometriske løsninger for identifisering eller autentisering. Det kan være til pålogging på PC, avgivelse av fingeravtrykk i stedet for garderobelapp, eller som adgangskontroll, for eksempel til treningsstudioer.

Biometri kan beskrives som kjennetegn som utgår fra kroppen, og som er unike for den registrerte og samtidig permanente eller stabile over tid. Ved å måle disse kjennetegnene kan de benyttes til å gjenkjenne en person eller bekrefte en persons påståtte identitet. De mest kjente formene for biometriske kjennetegn er fingeravtrykk, håndavtrykk og ansiktsform, samt iris- eller netthinneavlesning.

Løsninger som baserer seg på biometri nyter generelt høy tillit i befolkningen med hensyn til presisjon og sikkerhet. Det er derfor spesielt viktig å hindre uriktig bruk av slike verktøy. Når tilliten er høy, kan et eventuelt misbruk få særlig store konsekvenser. Det er viktig å øke bevisstheten om at en løsning som benytter biometri ikke nødvendigvis fører til bedre sikkerhet.

Biometrisk avlesning er som andre tekniske sikkerhetsløsninger, det vil være gode og dårlige løsninger. For eksempel kan dårlige fingeravtrykkslesere akseptere avkuttede fingre og gummihansker påført falske fingeravtrykk. Det vil alltid være et kappløp mellom nye teknologiske løsninger og forsøk på å omgå disse. Det kan være også være mangelfull

identitetskontroll ved innregistrering. Dersom feil person blir registrert i utgangspunktet er løsningen ikke sikker, selv om det benyttes biometri.

I tillegg er det viktig å ha fokus også mot de øvrige sikkerhetstiltak. Man illustrerer dette ofte ved utsagnet: ”At det står en biometrisk avleser på hoveddøren betyr ikke nødvendigvis at rommet innenfor er godt beskyttet dersom bakdøren er ulåst”. Dette gjelder både fysiske løsninger og pålogging til informasjonssystemer. Det er derfor viktig å huske at biometri fremdeles bare er et ledd i en sikkerhetsarkitektur, som ett enkelt ledd i en kjetting.

Den viktigste grunnen til å være varsom med bruk av biometri er at den unikt beskriver individet, og dermed uløselig er knyttet til oss. Om det uforutsette skjer – at et individs biometri blir misbrukt – finnes det ingen muligheter til å ”skifte til ny”. Hvordan et eventuelt misbruk kan gjennomføres er det ikke sikkert at vi ser rekkevidden av i dag.

Datatilsynet vil også advare mot en tendens til at det stadig økende tilbudet av nye og teknologisk fasinerende biometriske løsninger i seg selv fører til at vi som individer i økende grad tvinges til å la oss identifisere, uten at det strengt tatt foreligger et reelt behov.

8.5 Alle under mistanke?

Datatilsynet har i 2006 arbeidet med en rekke saker der man planlegger tiltak som vil berøre en stor gruppe personer, også de som ikke er mistenkt for noe. Motforestillinger mot tiltakene blir gjerne møtt med munnhellet ”de som ikke har noe å skjule, har heller ikke noe å frykte”. Tiltakene gir den enkelte muligheten til å ”bevise” egen uskyld ved å stille seg fullstendig åpen for granskning av blant annet blod, urin, bevegelser og sosiale kontakter.

Innføringen av datalagringsdirektivet står for Datatilsynet som et paradigmeskifte i det norske rettssystemet. Med dette direktivet innfører man et etterforskningsmiddel til bruk for politiet som omfatter hele befolkningen. Det er et breddetiltak, ikke målrettet mot enkeltpersoner eller grupper av personer det hefter en mistanke ved. Opplysninger om all telefonbruk blir lagret: hvem som kontakter hvem til hvilke tidspunkter, hvor vi befinner oss, samt all Internettbruk: hvem som har hvilken IP-adresse til hvilke tidspunkt den akuelle IP-adressen er logget på Internett.

Det er imidlertid ikke bare for politiarbeid og etterforskning man ser denne vridningen mot at den enkelte må bevise sin renhet og uskyld. I 2006 avgjorde Personvernnemnda to klager om anledningen til å teste rus og bruk av doping. De to sakene fikk ulikt resultat.

Securitas fikk ikke anledning til å teste samtlige ansatte med blodprøver eller urinprøver. Personvernnemnda påpekte at det er vanskelig å tenke seg et reelt frivillig samtykke i et arbeidsforhold, og konkluderte med at samtykke ikke er godt nok. Treningssentrene fikk derimot anledning til å inngå avtale med mosjonistene om frivillig deltakelse i et anti-dopingprogram. Som et ledd i dette skal mosjonistene kunne bli tatt ut til tester. Datatilsynets innvending til prosjektet var at et slikt frivillig tiltak vil være lite målrettet, og antakelig bare treffe mosjonister som uansett er dopingfrie. Nemnda mente derimot at disse testene ”bidrar til sunne holdninger og et positivt sosialt press som er til inspirasjon for andre treningssentre.”

Denne typen tiltak er ikke enestående. Datatilsynet har i tidligere årsmeldinger blant annet påpekt presset for å ta i bruk politiattester som ”bevis for uskyld”, i stadig flere sammenhenger. Det er åpenbart at samfunnet har behov for å beskytte seg mot alvorlig kriminalitet, mot at lite egnede personer får visse jobber eller verv, og mot at personer arbeider ruset i jobber som innebærer ansvar for andres liv og helse. Datatilsynet mener

imidlertid at man bør reflektere over mulige konsekvenser av å gå altfor langt i retning av at den enkelte selv i stadig flere sammenhenger forventes å ”bevise” egen renhet og uskyld. Gransking av kroppsvæsker og telefon- og internettbruk vil kanskje kunne avdekke noe, men de samfunnsmessige kostnadene vil kunne være svært store. Kontroll er det tydeligste uttrykk for mangel på tillit.

8.6 Begrepet ”personopplysning” innsnevres

Beskyttelsen av integriteten i Europeisk rettstradisjon er nært knyttet til vernet av personopplysninger. Kjernen i vernet er avhengig av hva begrepet omfatter, og kan lett undergraves dersom begrepets innhold endres.

I personopplysningsloven § 2, nr. 1 er personopplysning definert å være ”opplysninger og vurderinger som kan knyttes til en enkeltperson”. Innholdet i begrepet er nærmere beskrevet i forarbeidene til loven:

> *”Med uttrykket «enkeltperson» menes en person som direkte eller indirekte kan identifiseres, f eks ved hjelp av navn, identifikasjonsnummer eller et annet kjennetegn som er spesielt for personens fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sosiale identitet, jf direktivet artikkel 2 a. Eksempler på personopplysninger kan være opplysninger som foreligger i form av bilde, personens stemme, fingeravtrykk eller genetiske kjennetegn. Hvilket lagringsmedium som benyttes, er uten betydning så lenge identifikasjon er mulig.”*
>
> *”I vurderingen av om personen lar seg identifisere, skal det tas i betraktning alle hjelpemidler som det er rimelig å tro at noen kan komme til å anvende for identifiseringsformål, jf direktivets fortale punkt 26. Det vil dreie seg om en personopplysning selv om det må benyttes en nøkkel - f eks i form av en tallkode - for å knytte forbindelsen mellom opplysningen og den bestemte personen. Krypterte opplysninger kan være personopplysninger slik loven nytter ordet, dersom noen kan gjøre opplysningene lesbare og dermed identifisere personene som opplysningene vedrører.” (Ot.prp. nr. 92, 1998-1999, side 101).*

Personvernnemnda har gjennom flere saker gitt begrepet et annet og snevrere innhold enn det Datatilsynet, og de øvrige Europeiske tilsynsmyndighetene, har lagt til grunn i sin forvaltningspraksis. Integritetsvernet, lovens virkeområde og Datatilsynets mandat er etter dette noe uklart, og vil måtte vurderes grundig i det pågående lovrevisjonsarbeidet.

Personvernnemnda kom frem til overvåkingsbilder på et låst medium ikke er ”personopplysninger” i personopplysningslovens forstand. - Det finnes opplysninger om personer på opptaket, men disse er ennå ikke knyttet til identifiserbare enkeltpersoner, skriver nemnda i vedtakene om kameraovervåking i buss og tog.

Nemndas innstilling til dette spørsmålet kan etter Datatilsynets vurdering tolkes i retning av at opplysninger i svarte bokser ikke vil være beskyttet gjennom personopplysningsloven. I ytterste konsekvens kan det føre til at en virksomhet vil kunne samle store mengder opplysninger om atferd og bevegelser uten å informere, og uten å ta hensyn til sletteregleneе – så lenge opplysningene ligger på et låst medium. Sletteregelen på sju dager vil bare gjelde materiale som er ”tatt ut” av boksen.

Misbrukstrusselen ved langtidslagring av bilder fra kameraovervåking, eller andre personopplysninger, er stor. Datatilsynet ser det derfor som en uheldig utvikling dersom innsamlingen av personopplysninger på låste medier ikke skal omfattes av

personopplysningsloven. At loven eventuelt vil gjelde på et senere tidspunkt vil i liten grad reparere dette.

Datatilsynet vil gjennom sin videre virksomhet søke å avklare realitetene, herunder presedensvirkningen av Personvernnemndas vedtak.

9 Nærmere om utvalgte saksfelter

9.1 Samferdsel

I 2006 er det blitt tydeliggjort at det nå bygges opp en omfattende infrastruktur for overvåking av reisende, både bilister og innen kollektivtrafikken. Dette dreier seg om alt fra overgripende overvåking med satellitter, overvåking ved hjelp av kameraer og radiofrekvensbrikker (som Autopass), til såkalte ”svarte bokser” som sitter i den enkelte bil og registrerer kjøringen.

Denne utviklingen har ikke vært gjenstand for særlig oppmerksomhet, langt mindre politisk debatt.

Måling av gjennomsnittsfart

Norske veimyndigheter har brukt automatisk trafikkontroll (ATK) i mange år. ATK baserer seg på måling av fart i ett målepunkt. Kjører man for fort, blir det tatt et bilde.

Vegdirektoratet og politiet har i 2006 testet måling av gjennomsnittsfart i et prøveprosjekt på E6 nord for Lillehammer. Målingen foregår ved at absolutt alle som passerer et første målepunkt blir tatt bilde av, også de som holder fartsgrensen. Bilen må identifiseres såpass godt at man er sikker på at bildet fra første og andre målepunkt er av samme bil. Bildet tatt ved passering av det første målepunktet blir lagret inntil systemet har sjekket om fører har kjørt for fort. Dersom fartsgrensen er overskredet, overføres opplysningene til politiet for utferdigelse av et eventuelt forelegg. Ved å ta i bruk en systemteknologi som tar bilde av alle biler, er en helt ny infrastruktur for omfattende overvåking blitt etablert.

Satellittovervåking

Mye taler for at vi kommer til å få et EU-basert system for satellittovervåking av biler. EU har flere programmer under planlegging som skal gjøre dette mulig.

Ved hjelp av de globale satellittbaserte posisjoneringssystemene GPS og Galileo vil man kunne posisjonere bilers posisjon. Også bilens hastighet vil dermed kunne overvåkes automatisk.

Norske myndigheter har inngått avtale om satellittposisjonering av biler (e-call). E-call går ut på at alle biler som selges i EU-området fra 2009 skal være utstyrt med satellittposisjonering og kommunikasjon via mobiltelefonnettet som gjør at det sendes informasjon automatisk ved ulykker til nærmeste alarmsentral. Galileo, EUs nye system for satellittposisjonering, har her en sentral rolle.

Merking av biler

Det eksisterer også et EU-program som arbeider med spørsmålet om å gi hver enkelt bil en unik elektronisk avlesbar identitet (Electronic Vehicle Identification - EVI). Det er så vidt Datatilsynet vet ikke bestemt om dette skal være satellittbasert, eller basert på radiofrekvensbrikker, RFID.

Med samme bombrikke gjennom Europa

Også i ordningen for betaling av veiavgifter (Autopass) ligger en overvåkingsmekanisme. Ordningen utvides raskt, og rundt enkelte byer og tettsteder er det etablert helautomatisk bompengeinnkreving som gjør det umulig å passere anonymt. Mynter, som naturlig nok er

et fullverdig anonymt alternativ, kan ikke lenger benyttes i de helautomatiske bomstasjonene.

I 2006 ble det fra norsk side også vedtatt at man skal gå med i en ordning som legger opp til samordning av betalingsløsningene i de europeiske bompengesystemene – enten satelittbasert, eller ved radiofrekvensbrikker, som i Autopass.

Autopassbrikken kan fjernavleses, og det er mulig å overvåke bilenes bevegelsesmønster uten at brukeren er kjent med at det skjer. Også private kan tenkes å fjernavlese brikken, og på denne måten registrere når bestemte biler passerer. Dette kan brukes som varsel når politiet nærmer seg, eller for å kartlegge andre personers bevegelsesmønster etc. For enkelte kan dette være nyttig informasjon for å begå sofistikert kriminalitet.

”Svart boks” i bilen – hvem eier informasjonen?

Det er trolig bare et tidsspørsmål før alle biler produseres med en innebygget ”black box”. Her registreres data om kjøringen, for eksempel hvordan gass, bremser, ratt, blinklys og sikkerhetsbelte benyttes. Normalt er det bare de siste sekundenes kjøring som lagres. Ved en ulykke kan denne informasjonen brukes for å utrede årsaken, og dermed skyldforholdet. Systemet er åpenbart interessant for politi og forsikringsselskap. Imidlertid antar Datatilsynet at mange bilførere ikke vet at denne informasjonen lagres. Hvem som rettmessig er eier av informasjonen, og hvem som skal ha adgang til denne, er i liten grad diskutert.

Hvem vil overvåke bilistene?

Hovedsakelig er det staten og forsikringsselskapene som ønsker å overvåke bilistene. Myndighetenes ønsker er knyttet til overholdelse av trafikkregler, kampen mot kriminalitet, manglende betaling av skatter og avgifter, automatisk ambulansealarm ved ulykker, med mer. Forsikringsselskapene har ønske om å skille høyrisikokunder fra lavrisikokunder, og bruke kunnskapen blant annet til forsikringer basert på nye forretningsmodeller, som for eksempel at kundene betaler en variabel premie basert på faktisk risikoeksponering ("Pay as you drive”). Britiske forsikringsselskaper har allerede innført slike ordninger. Også i Norge har forsikringsselskaper luftet ideen overfor Datatilsynet.

En ”svart boks” sørger for at selskapet har kunnskap om blant annet hvor bilen er, fart, akselerasjon og nedbremsing. Ut fra et sett kriterier fastsatt av selskapet beregnes risikoen bileieren utsetter seg for, og kunden betaler i forhold til den anslåtte risikoen. Dette er informasjon som trolig vil være svært interessant for flere.

Kolumbus – elektronisk billett

Rogaland Kollektivtrafikk sendte ut Kolumbuskortet, et elektronisk reisekort, til samtlige innbyggere over 16 år i Rogaland. Totalt ble det sendt ut over tre hundre tusen kort. Rogaland Kollektivtrafikk er fylkeskommunalt eid, og har som viktigste oppgave å utvikle og styrke det kollektive transporttilbudet i regionen.

Innbyggerne hadde ikke selv bestilt kortet. Rogaland Kollektivtrafikk benyttet seg av folkeregisteropplysninger, oversendt fra Skattedirektoratet, som grunnlag for utsendelsen. Flere rogalendinger oppfattet kortet som uønsket direkte markedsføring, og tok kontakt med Datatilsynet.

Kolumbuskortet inneholder en unik RFID-brikke, slik at hvert enkelt kort kan skilles fra andre. RFID-brikken kan avleses på avstand.

For at innbyggerne ikke skulle kaste Kolumbuskortet, men behandle det som et personlig kort, ble det preget med personnavn. Kortets identifikasjonsnummer var ellers ikke koblet til personen. Datatilsynet skrev til Rogaland Kollektivtrafikk og stilte en rekke spørsmål om tjenesten. Blant annet spurte Datatilsynet om detaljer når det gjaldt lagring av reiseopplysninger, samt sikring av disse.

Tjenesten la opp til at reiseopplysninger skulle lagres så lenge den enkelte var kunde i selskapet. Dette lar seg vanskelig forene med personopplysningslovens krav om sletting, med mindre den enkelte selv samtykker.

Datatilsynet arbeider videre med saken i 2007.

9.2 Justissektoren

9.2.1 Innsynsloven – videre oppbevaring av POTs registre?

Justisdepartementet foreslo i 2006 en ny bestemmelse til innsynsloven. Loven, som gav de registrerte en begrenset rett til innsyn i overvåkingspolitiets arkiver og registre, ble foreslått utbygd med en bestemmelse som gir de som har fått innsyn rett til å supplere opplysningene.

I realiteten tok departementet gjennom høringsbrevet stilling til et langt viktigere spørsmål, nemlig at overvåkingstjenestens materiale skal oppbevares videre.

POTs arkiver ble gransket av Lund-kommisjonen, som avdekket at mange opplysninger var ulovlig innhentet.

Da Stortinget vedtok innsynsloven var det med føringer om å åpne for makulering/sletting: Stortinget bad "…Regjeringen fremme forslag som gir den som er gitt innsyn etter innsynsloven mulighet til å kreve makulering/sletting av uriktige eller ulovlig innhentede opplysninger."

Med høringsbrevet foreslo departementet det motsatte av hva Stortingets vedtak gikk ut på.

Datatilsynet foreslo at departementet skulle utforme et nytt lovforslag som drøftet sakens kjerne – nemlig spørsmålet om sletting eller videre oppbevaring.

Datatilsynet er enig med departementet i at en tolkning av hva som er riktige eller uriktige opplysninger kan være et umulig spørsmål å ta stilling til i de enkelte sakene. Dette bør imidlertid ikke være et argument for videre oppbevaring av opplysningene. Forutsetningene for makulering bør ikke nødvendigvis knytte seg hva som er "uriktige" opplysninger. For eksempel kan man i stedet vurdere hvilke opplysninger PST har bruk for i sin virksomhet i dag. Ettersom det dreier seg om materiale det er gitt innsyn i, er sannsynligheten svært liten for at materialet fortsatt er relevant for PST.

En videre oppbevaring av materialet må baseres på den overvåkede persons samtykke. Tilsynet har forståelse for at det er forskningsmessige interesser knyttet til materialet. Likevel er det sterke grunner som taler for oppbevaring kun etter et aktivt informert samtykke fra den opplysningene gjelder. Etter tilsynets mening er dette den beste måten å håndtere en kritisert epoke i det norske overvåkingspolitiets historie, og samtidig imøtekomme Stortingets vedtak. En videre oppbevaring vil kunne oppfattes som en fortsatt krenkelse av den overvåkedes personvern. Et annet alternativ kunne være å anonymisere materialet og overlevere dette til Riksarkivet. På den måten vil forskningsinteressene i en viss utstrekning kunne ivaretas.

En rett for den registrerte til å supplere "mappen" vil kunne oppfattes som en plikt til å komme med et forsvarsskriv, selv om man kanskje primært ønsker å legge overvåkingshistorien bak seg. Plikten kan være forankret i en følelse av at det som blir stående uimotsagt vil ha en større "sannhetsverdi" enn om man tar til motmæle.

9.2.2 Hjemmesoning og omvendt voldsalarm

Hjemmesoning med elektronisk overvåking

I 2006 sendte Justisdepartementet et forslag på høring som blant annet beskriver et prøveprosjekt med hjemmesoning og elektronisk overvåking. Forslaget kom i forbindelse med tiltak for å få ned soningskøene og for å få et bedre innhold i soningen.

Datatilsynet understreket i høringsuttalelsen at også hjemmesoning med elektronisk overvåking er et inngripende tiltak. Den som skal sone sin straff under slike forhold vil bli kontinuerlig overvåket, samtidig som vedkommendes daglige gjøremål kan utføres mer eller mindre fritt. Den enkeltes følelse av grenser for hva han kan gjøre eller ikke gjøre blir mindre tydelige når man soner hjemme i stedet for i fengsel.

Det er foreslått at Kriminalomsorgen skal innhente samtykke fra andre beboere i samme bolig for at hjemmesoningen skal kunne gjennomføres. Datatilsynet forutsetter at kretsen som skal varsles består av den dømtes familie og eventuelt andre som vedkommende deler husvære med. Dersom informasjon om straffegjennomføringen også skal spres til andre enn denne begrensede kretsen, innebærer det etter Datatilsynets mening en unødvendig spredning av sensitive personopplysninger

Elektronisk merking – "omvendt voldsalarm"

Et forslag om merking av voldsmenn ble også sendt på høring fra Justisdepartementet. Forslaget er ett av en del tiltak med formål å beskytte personer som lever under vold og trusler.

De foreslåtte endringene i straffeloven og straffeprosessloven reiser spørsmål om vi ønsker et samfunn der uønskede eller vanskelige grupper av mennesker blir elektronisk merket. Tilsynet antar at dersom man først har valgt å åpne for elektronisk merking av en type kriminelle, har man overskredet en terskel. Neste skritt på veien mot økt bruk av denne type tiltak vil være langt enklere å ta.

Datatilsynet gjør i sin høringsuttalelse spesielt oppmerksom på at elektronisk merking er et tiltak som i seg selv innebærer et stort inngrep i den enkeltes integritet. Teknologien gjør det mulig å følge en merket person kontinuerlig.

Hvor skal grensene gå for når og hvor man kan overvåke vedkommende? Når vil alarmen bli utløst? Skal alarmen utløses når vedkommende kommer i nærheten av offeret eller i nærheten av forhåndsdefinerte steder, slik at det også blir mulig for den merkede å forutse når han overvåkes? Datatilsynet påpekte i forbindelse med høringsrunden at den aktuelle bestemmelsen i straffeloven manglet en nærmere angivelse av hva som skal vektlegges ved vurderingen av kontaktforbudets geografiske og tidsmessige omfang.

9.2.3 Grooming – forberedelser til overgrep mot barn

Justisdepartementet foreslo i meldingsåret at enkelte forberedelser til seksuelle overgrep mot barn skal kriminaliseres. Forslaget ble fremmet i forbindelse med endringer i straffeloven. Det er prisverdig at man fra politisk hold vil ha virkemidler for å hindre

seksuelle overgrep mot barn, og erkjenner at nye virkemidler må tas i bruk i takt med den teknologiske utviklingen.

I et personvernperspektiv er kriminalisering av forberedelseshandlinger og etterforskning av forberedelse imidlertid ikke uten fallgruver. Hvilke etterforskningsmetoder skal politiet ha til rådighet for å oppnå målet med bestemmelsen?

Å lete etter en gjerningsperson som ikke har forbrutt seg, men som har til hensikt å begå overgrep, kan fort resultere i en type overvåking som også rammer mange uskyldige.

Grooming-bestemmelsen er ikke eksplisitt knyttet til bruk av teknologiske hjelpemidler, men i motivene går det klart frem at man ønsker å utforme en straffebestemmelse som er effektiv i forhold til bruk av Internett og andre elektroniske kommunikasjonsmidler. Den enkeltes privatliv og korrespondanse er gitt en spesiell beskyttelse gjennom den Europeiske menneskerettskonvensjonen, og bestemmelsen vil kunne utfordre dette prinsippet.

Samfunnet bør ha meget gode grunner for å innføre bestemmelser der enkeltpersoners antatte hensikter kan straffes. Datatilsynet etterlyser i høringsuttalelsen dokumentasjon som beskriver omfanget av problemet. Det ble i høringsbrevet vist til endel spørreundersøkelser der barn og unge er blitt spurt om ulike forhold rundt bruk av Internett og andre elektroniske kommunikasjonsmidler. Tilsynet anser ikke dette som tilstrekkelig for å dokumentere behovet.

Slik Datatilsynet ser det, er det største problemet knyttet til barn og unges bruk av elektroniske kommunikasjonskanaler at svært mange foreldre/foresatte ikke har tilstrekkelig kunnskap om hva som faktisk foregår. I så henseende er det på dette området samfunnet bør legge inn hovedressursene, og slik bidra til å forhindre at overgrep skjer.

En aktiv lovgivningspolitikk på dette området kan også ha den virkning at foreldre/foresatte gis et inntrykk av at "noen andre" passer på barnet når det beveger seg i den elektroniske verden. Dette kan igjen bidra til å redusere foresattes nødvendige involvering i barnas bruk av elektronisk kommunikasjon.

9.2.4 IKT/Internett i opplæring for innsatte

Datatilsynet har også uttalt seg om foreslåtte retningslinjer for bruk av IKT/Internett i opplæringen for innsatte i norske fengsler. Et hovedspørsmål i denne sammenheng er hvorfor opplysningene om innsattes bruk av IKT skal lagres sentralt og ikke lokalt ved de enkelte institusjoner. En landsdekkende sentral oversikt over alle innsattes bruk av IKT stiller store krav til sikkerhet og administrasjon av systemet. Datatilsynet stilte spørsmål om hvorvidt en slik ordning er akseptabel. Den vil gi en stor ansamling av personopplysninger, der risikoen for misbruk vil være større enn ved lokal lagring. Det må ligge helt klare føringer for hva opplysningen kan brukes til, og disse må gjøres kjent for brukerne av systemet.

9.2.5 Politiets tilgang til valutaregisteret

Finansdepartementet sendte i januar 2006 et forslag på høring om at politiet skal ha adgang til valutaregisteret også i saker der det ikke er iverksatt etterforskning.

Valutaregisteret inneholder opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge, blant annet om all bruk av norske betalingskort i utlandet. Fra før har politiet, Skatteetaten, toll- og avgiftsetaten, Rikstrygdeverket og Kredittilsynet elektronisk tilgang til opplysningene i registeret. Opplysningene kan

imidlertid bare hentes ut i forbindelse med iverksatt etterforskning, kontrollvirksomhet eller tilsyn.

Etter forslaget skal politiet få full tilgang til valutaregisteret, uten krav om at det er iverksatt etterforskning i en konkret sak. Forslaget vil blant annet medføre at alle norske borgeres befatning med fremmed valuta og bruk av betalingskort i utlandet, vil være tilgjengelig for enhver tjenestemann i politiet. Datatilsynet kan ikke støtte dette.

Svært mange personer er registrert i valutaregisteret uten at de har noen forbindelse med mulig straffbare forhold. Datatilsynet påpekte i sin høringsuttalelse at dersom vilkårene for tilgang utvides, bør gruppen av personer som får tilgang gjøres så liten som mulig. Dersom hvitvaskingsenheten i Økokrim har det største behovet, mener Datatilsynet at det er disse polititjenestemennene som bør få tilgang, og ikke politiet som helhet.

Datatilsynet er overrasket over at det foreslås en utvidet tilgang til valutaregisteret, uten at det utformes spesifiserte kriterier for når politiet kan benytte seg av den utvidete tilgangen. Slik lovbestemmelsen er utformet, fremstår det som at politiet får en generell mulighet til å søke elektronisk i valutaregisteret, etter eget forgodtbefinnende. Det finnes en høyst reell misbruksfare ved at svært mange får vid tilgang til denne typen registre. Datatilsynet så i 2005 eksempler på misbruk av politiets registre, der tilfeldige søk ble foretatt, uten at dette ble forhindret av tilfredsstillende tilgangsbegrensning og kontroll.

9.2.6 Eurodac og VIS – biometriske data for reisende og asylsøkere

Manglende nasjonalt ansvar for Eurodac

Datatilsynet gjennomførte et tilsyn med Eurodac ved Kripos. Tilsynet ble utført som en del av et større prosjekt som er initiert av European Data Protection Supervisor. Eurodac er et hjelpemiddel for å fastsette hvilken medlemsstat som er ansvarlig for behandlingen av en asylsøknad.

I etterkant av tilsynet, og etter oversendelse av varslede pålegg, motsatte Kripos seg at etaten var å betrakte som behandlingsansvarlig for den nasjonale delen av Eurodac. Ansvarsforholdet var ikke avklart ved utgangen av 2006.

Nytt felles europeisk visum-informasjonssystem (VIS)

Arbeids- og inkluderingsdepartementet har ansvaret for implementering av nødvendig regelverk i forbindelse med Norges tilslutning til VIS-systemet. Forslag til endringer i utlendingsloven ble i den forbindelse sendt på høring. Forslag til hjemmel for VIS la opp til registrering, lagring og utveksling av informasjon i forbindelse med behandling av visumsøknader. I Datatilsynets høringsuttalelse ble det etterlyst et klart formål, klarhet i hvem som skal ha tilgang, hvor lenge opplysningene skal lagres og hvem som skal ha ansvaret for den nasjonale delen av VIS.

Visumdatabasen er tenkt opprettet for å ivareta en rekke forhold som er svært vidt beskrevet. VIS skal blant annet forenkle identifikasjon og tilbakesending av ulovlige innvandrere, og forebygge trusler mot de enkelte medlemsstaters ”indre sikkerhet”. De ”rette myndigheter” skal ha tilgang for å ”forhindre, avdekke eller etterforske kriminelle handlinger og terrorisme”.

Begrepene i Rådsforordningen, som lovforslaget bygger på, har en svært vid tolkningsramme. Det er derfor vanskelig å ha et realistisk bilde av hvor mange som faktisk skal ha tilgang til søk i systemet, og hva det skal kunne brukes til.

VIS skal også registrere visumsøkeres biometriske kjennetegn – bilde og fingeravtrykk. En identitet blir imidlertid ikke automatisk mer "sann" når biometriske opplysninger legges til. Opplysningene er aldri mer riktige enn de er i det øyeblikk de registreres inn i systemet. En god nok sikring av opplysningenes korrekthet ved registreringstidspunktet blir derfor særlig viktig.

Datatilsynet etterlyste i høringsuttalelsen en konsekvensvurdering av feilregistrering av uskyldige personer, som blir utsatt for identitetstyveri. Dersom en person med falske identitetspapirer blir innrullert i VIS, vil bruken av biometri medføre et betydelig skadepotensial for den uskyldige personen som er utsatt for identitetstyveriet. En slik konsekvensvurdering må utarbeides før systemet tas i bruk.

Datatilsynet etterlyste videre en klar fastsettelse av hvem som skal ha ansvaret for VIS. Tilsynet har sett at ansvaret for fingeravtrykksdatabasen Eurodac har vært dårlig definert, og at dette har hatt flere uheldige virkninger. Det er en utfordring for den enkelte å orientere seg i forhold til hvilke rettigheter man har og hvor man kan henvende seg for å hevde sine rettigheter. Det har også vært problemer i forhold til feilretting og hvem som skal ha ansvar for at det blir foretatt nødvendige endringer i systemet.

9.2.7 DNA og biologisk materiale

DNA-utvalget avleverte sin utredning og forslag til lov om DNA-register til bruk i strafferettspleien i november 2005. Datatilsynets direktør var representert i utvalget, og dissenterte på enkelte punkter med flertallet i utvalget.

Grunntanken bak DNA-registeret er at nye kriminelle handlinger skal kunne oppklares når DNA-funn fra åstedet kan sammenholdes med profiler fra registeret. Datatilsynet er fornøyd med at forslaget legger opp til at det bare er dømte personer som skal kunne registreres, og ikke personer som bare har vært under mistanke.

Datatilsynet frykter imidlertid at terskelen for å havne i DNA-registeret kan bli svært lav. En dom med strafferamme på seks måneder er nok til å bli registrert. Dette vil også gjelde relativt bagatellmessige forseelser. Dette er stikk i strid med Europarådets anbefaling om at man ikke bør registrere DNA annet enn ved forbrytelser som truer liv og sikkerhet.

Flertallet i DNA-utvalget ønsket at de registrerte profilene aldri skal slettes. Et mindretall foreslo variable sletteregler etter hvor alvorlige forhold den enkelte er dømt for. Datatilsynet støttet mindretallet, men foreslo også en mulighet for å slette opplysninger om unge førstegangsforbrytere dersom de ikke har forbrutt seg på nytt innen en gitt tid, for eksempel to år. Dersom en slik regel kan motivere unge førstegangsforbrytere til å avstå fra å begå ny kriminalitet, må det være bra for både samfunn og individ.

Et samlet DNA-utvalg mente at det ikke skulle være tillatt å forske på data fra DNA-registeret. Helse- og omsorgsdepartementet foreslo likevel en slik adgang. Forslaget var verken begrunnet, eller fulgt opp av en utredning av de personvernmessige ulempene. Datatilsynet påpekte at DNA-prøvene er innsamlet under tvang, og at dette tilsier at det skal mer til enn en enkel dispensasjon for å få tilgang til opplysningene for forskningsformål.

Datatilsynet frarådet i sin høringsuttalelse videre oppbevaring av det biologiske materialet etter at prøven er analysert. Etter analysen bør det biologiske materialet destrueres.

Datatilsynet har sett flere eksempler på at veien er svært kort fra å ha et grunnlagsmateriale liggende, til ønsket om å ta dette i bruk til stadig nye formål.

9.2.8 Tilsyn med Schengen informasjonssystem

Datatilsynet fører tilsyn etter Lov om Schengen informasjonssystem. Disse tilsynene blir normalt initiert av den internasjonale komité JSA, hvor de ulike nasjonale tilsyn er representert. I 2006 ble det satt spesielt fokus på artikkel 99 i direktivet, som omhandler vilkår og rutiner for innlegging av informasjon og retningslinjer for tilgang til opplysningene. Datatilsynet konstaterte en praksis som stort sett var i tråd med regelverket.

9.3 Sektorovergripende saker

9.3.1 Internett

Søkemotorer

De europeiske personvernmyndighetene er bekymret for hvilke opplysninger søkemotorene tar vare på etter et gjennomført søk. Det foreligger påstander om at flere opplysninger, som IP-adresser, søkeord, og hvilket nettsted søkerne går til, lagres nærmest for all ettertid.

Høsten 2006 ble det derfor gjennomført tilsyn mot virksomheter som driver søkemotorer på Internett. Tre virksomheter ble varslet om tilsyn, henholdsvis Sesam - Schibsted Søk AS, Kvasir - Eniro Norge AS og Google. Tilsynene mot de to første virksomhetene ble gjennomført som forutsatt. Det siste tilsynet mot Google viste seg vanskelig å få gjennomført. Datatilsynet har blant annet hatt vanskeligheter med å avklare hvem det er som kan betraktes som behandlingsansvarlig. Google er den desidert mest brukte søkemotoren for norske brukere. Det er derfor viktig at et tilsyn overfor denne internasjonale aktøren blir gjennomført på samme måte som overfor de norske søkemotorene.

Sentralt for tilsynene står spørsmålet om hva som lagres av personopplysninger og når disse personopplysningene slettes. Tilsynene omfatter også at det bringes klarhet i hva slags personopplysninger som innehentes og lagres av søkemotorene for å danne grunnlag for mulige søk.

Nasjonalbibliotekets paradigma-prosjekt

Nasjonalbiblioteket har hatt en midlertidig konsesjon for å samle inn ikke-passordbelagte norsk- og samiskspråklige sider fra Internett. Biblioteket har søkt konsesjon for å kunne videreformidle samlingen.

Pliktavleveringsloven pålegger utgivere, produsenter, trykkerier og importører å avlevere et gitt antall eksemplarer til Nasjonalbiblioteket. Biblioteket har imidlertid hatt problemer med å sikre materiale som bare er publisert på Internett, og har derfor valgt selv å høste inn sidene og lagre dem på egne servere.

Slikt Datatilsynet ser det, er aktørenes egen avlevering til Nasjonalbiblioteket vesensforskjellig fra om Nasjonalbiblioteket selv innhenter informasjonen. I en avleveringssituasjon vil utgiver/produsent ha en bevissthet knyttet til at materialet skal arkiveres for all fremtid. Den samme bevisstheten vil ikke være til stede hos en utgiver som får sitt materiale innhøstet.

For Datatilsynet er hovedproblemstillingen knyttet til personopplysninger og bilder som, av ulike grunner, er fjernet fra Internett. Hvordan skal man forhindre at slike opplysninger dukker opp igjen i en annen sammenheng?

Det er helt grunnleggende for ivaretakelsen av borgernes personvern at retten til sletting av opplysninger på Internett er mest mulig reell. Mange benytter Internett nokså ukritisk når det gjelder publisering av tekst og bilder om seg selv og andre. De selvpålagte skrankene, som redaktører og utgivere tradisjonelt har hatt, er ofte fraværende.

Et annet forhold som også er relatert til fjerning av personopplysninger, er når behandlingsansvarlig/nettstedeier feilaktig og ved uhell publiserer personopplysninger. Et eksempel fra meldingsåret er en kommune som på sin hjemmeside kom i skade for å publisere fødselsnummeret til flere tusen innbyggere. Andre eksempler er publisering av taushetsbelagte opplysninger, eller opplysninger man etter personopplysningsloven skal ha et samtykke for å utlevere. Disse eksemplene viser at en tilgjengeliggjøring av for eksempel kommunenes materiale, som tidligere har vært publisert på Internett, heller ikke er uproblematisk.

Datatilsynet ser at en konsesjon til videreformidling av internettarkivet vil kunne bidra til å undergrave sentrale personvernrettigheter. Det vil kunne oppfattes som en fortsatt krenkelse av personvernet at en statsinstitusjon tar vare på informasjon som er fjernet fra Internett. Datatilsynet erkjenner imidlertid dokumentasjonsverdien i samlingen, og innser at denne vil være nokså verdiløs dersom man ikke kan nyttiggjøre seg den. Tilsynet er i dialog med Nasjonalbiblioteket for å finne en tilfredsstillende løsning.

Fildeling

Under tvil kom Datatilsynet frem til at overvåking av fildelingsnettverkene har grunnlag i personopplysningsloven. Datatilsynet ser imidlertid behov for en politisk avklaring på området.

Et advokatfirma som representerer rettighetshaverne ville registrere kallenavn, IP-adresse, og fillister som viser hvilke musikkspor, filmer eller TV-serier som blir delt via fildelingsnettverk. Hensikten er å skaffe nok opplysninger til å kunne anmelde ulovlig fildeling til politiet, fremme et sivilt søksmål, eller å rette henvendelser til enkelte fildelere via nettleverandørene. Personopplysningene som samles inn vil normalt være avidentifiserte, og videre etterforskning vil måtte foretas av politiet.

Datatilsynet kom under tvil frem til at disse opplysningene kan registreres med grunnlag i personopplysningslovens § 8f. Tilsynet mente videre at advokatfirmaet må ha konsesjon for behandlingen, fordi opplysningene som innhentes er sensitive.

Datatilsynets utfordret musikk- og filmbransjen til å informere publikum om lovlig/ ikke lovlig kopiering og nedlasting av musikk og filmer. Både gjennom egen virksomhet og fra presseoppslag har tilsynet erfart at det er vanskelig for publikum å orientere seg på området.

Etter Datatilsynets mening reiser saken prinsipielle spørsmål som bør få en politisk avklaring. Det er ikke uproblematisk at private aktører skal etterforske lovbrudd uten noen form for fullmakt fra lovgivende myndighet. Politiets kommunikasjonskontroll og etterforskning er regulert i straffeprosessloven. Infiltrasjon og provokasjon er metoder politiet bare kan benytte når kravene i Riksadvokatens retningslinjer er oppfylt. Tilsvarende gir Lov om vaktvirksomhet retningslinjer til vaktselskapene. Advokatfirmaet er ikke underlagt tilsvarende lovgivning og retningslinjer.

Datatilsynet registrerer at både justis- og kulturministeren har kommet med uttalelser knyttet til deling av filer uten lovlig kopieringsgrunnlag. Datatilsynet har oversendt kopi av brevet til Justisdepartementet og Kulturdepartementet. Dette er gjort for å signalisere at det er behov for å endre åndsverkloven dersom det er politisk ønskelig at rettighetshavere skal ha mulighet til å forfølge brudd på denne.

En endring i loven bør i så fall klart angi grensene for hvilke virkemidler rettighetshaverne skal kunne benytte. Datatilsynet mener et slikt tiltak vil bidra til å sikre kravet til forutsigbarhet, både for bransjen og publikum.

Sletting fra Internett

Datatilsynet har i løpet av meldingsåret blitt kontaktet av flere enkeltpersoner som har hatt problemer med å få slettet opplysninger publisert på Internett. Antallet henvendelser fra personer som ber om tilsynets hjelp til å få slettet informasjon er økende. Her er noen eksempler på saker fra meldingsåret.

Videresendt til pornosider

En medarbeider i en offentlig etat kontaktet Datatilsynet. Når han søkte på sitt eget navn på Internett fikk han en mengde treff på internasjonale pornosider. Det viste seg at navnet hans var lagt inn på en rekke sider som ikke hadde annen funksjon enn å sende surferen videre til pornosidene.

Medarbeideren antok at dette var gjort for å sverte navnet hans.

Det har vist seg svært vanskelig å få en slutt på dette. De ansvarlige for hjemmesidene har ikke oppgitt kontaktopplysninger, og sidene er plassert i flere land. Datatilsynet arbeider fortsatt med saken.

TVNOR.no

To jenter ønsket en karriere i mediene. De la inn bilder og informasjon om seg selv på tvnor.no, et nettsted som oppgir at de er "for deg som ønsker en karriere innen TV/filmproduksjon". De fikk ingen tilbud, og ønsket å slette informasjonen. Det viste seg å være svært vanskelig. Oppgitte e-postadresser virket ikke, og det fantes ikke opplysninger om telefonnummer.

Til slutt fikk Datatilsynet sporet opp telefonnummeret til innehaveren via opplysninger om andre selskaper som innehaveren hadde opprettet. Jentenes personopplysninger er nå fjernet.

DNA-analyser på nett

En tenåring søkte på navnet sitt via en søkemotor. På bestemorens hjemmesider fant hun resultatet av sin egen dna-analyse.

Bestemoren hadde tvilt på hvem som var faren til jenta, og hadde i all hemmelighet sendt inn biologisk materiale fra flere slektninger til analyse. Etterpå hadde hun publisert analyseresultatene på Internett, med navn. Barnebarnet ble opprørt, og politianmeldte forholdet. Sidene er nå fjernet.

Sletting fra debattforum på Internett

En person ønsket å få slettet både sine egne leserinnlegg samt motinnlegg andre personer hadde skrevet i et debattforum. I tillegg krevde vedkommende sletting av alle registreringer på sitt navn gjennom søkemotoren Google. Datatilsynet mente at innleggene var ytringer

vernet av ytringsfriheten, og derfor ikke kunne slettes med hjemmel i personopplysningsloven. Personvernnemnda var enig i vurderingen.

Personvernnemnda konkluderte med at debattsider faller inn under personopplysningsloven § 7. Det betyr at innlegg fra klager og andre innlegg som viser til klagers innlegg, samt kommentarer og motinnlegg ikke kan kreves slettet, siden nettstedet representerer virksomhet med opinionsdannende formål.

Personvernnemnda påpekte også at Google indekserer og katalogiserer alle opplysninger som ligger tilgjengelig på Internett. Et debattforum kan neppe påvirke eller hindre slik indeksering, slik klager hevdet.

9.3.2 Biometri

I 2006 fattet Datatilsynet en rekke vedtak om at bruk av fingeravtrykk i forskjellige sammenhenger måtte opphøre. Fem av vedtakene ble klaget inn for Personvernnemnda. Datatilsynets har ikke noe prinsipielt imot bruk av fingeravtrykk eller andre biometriske kjennetegn i enhver situasjon, men tolket formuleringer i personopplysningslovens § 12 slik at adgangen til bruk var meget snever.

Én av de fem klagene ble avgjort av nemnda i meldingsåret. Saken gjelder bruk av fingeravtrykk ved pålogging til datamaskiner i Tysvær kommune. Datamaskinene benyttes til å behandle sensitive personopplysninger, som for eksempel opplysninger om innbyggernes helse. Personvernnemnda ga kommunen medhold i at bruk av fingeravtrykk ved påloggingen var nødvendig for å sikre opplysningene.

Selv om det vil komme flere vedtak fra Personvernnemnda som trolig vil klargjøre den nedre grense for bruk av biometriske løsninger, finner Datatilsynet det riktig å redegjøre nærmere om fordeler og ulemper ved bruk av biometriske kjennetegn.

Hva er biometri?

Biometriske kjennetegn kan beskrives som kjennetegn som utgår fra kroppen, som er unike for den registrerte og samtidig permanente eller stabile over tid. Ved å måle disse kjennetegnene kan de benyttes til å gjenkjenne en person, eller bekrefte en persons påståtte identitet.

De mest kjente formene for biometriske kjennetegn er fingeravtrykk, håndavtrykk og ansiktsform, samt de to øyeteknologiene netthinne- og irisavlesning. I utgangspunktet kan alle målbare og unike egenskaper ved oss benyttes. Dette kan for eksempel være i form av stemmegjenkjenning, DNA, eller hvilken tastefrekvens vi benytter når vi skriver på et tastatur.

Biometri beskrives ofte som ”noe vi er” når det sammenlignes med de tradisjonelle metodene for å gjenkjenne eller bekrefte en persons identitet. De tradisjonelle metodene omfatter ”noe du vet”, for eksempel et passord, og ”noe du har”, for eksempel en kodebrikke.

Biometri har sin egenart, det er uløselig knyttet til kroppen vår, på godt og vondt.

Bruksområder

Biometri, for eksempel i form av fingeravtrykk, er et viktig hjelpemiddel i politiets etterforskning, for å fastslå identitet og knytte gjerningspersoner til et åsted. Biometri kan

imidlertid også benyttes i mer hverdagslige sammenhenger for å bekrefte identitet, for eksempel for å fastslå at en person er medlem i et treningsstudio.

Mange betrakter biometri som en rask, effektiv og sikker løsning for å bekrefte at en person er den hun eller han utgir seg ut for å være. Man trenger ikke ha med seg noe (kort) eller huske noe (kode).

Bruk av biometri kan være et godt bidrag til å utvikle sikre løsninger, men da normalt i kombinasjon med andre metoder for å bekrefte at en person er den han gir seg ut for å være (autentisering). For eksempel kan man benytte det tradisjonelle passordet eller kodekortet, i kombinasjon med en biometrisk løsning. Der kortet kan bli stjålet og koden gitt videre, er biometrien uløselig knyttet til deg. Dersom løsningen og bruken av løsningen er god, vil biometri kunne gi bedre sikkerhet.

Biometri benyttes også i situasjoner der det ikke nødvendigvis er den høye sikkerheten man er på jakt etter. Eksempler her er bruk av fingeravtrykk i stemplingssystemer, for å hindre at ansatte stempler for hverandre, såkalt ”kameratstempling”. Annen bruk kan ha som formål å nettopp gjøre det enkelt for brukeren. Garderobeskap i en svømmehall som åpnes og lukkes ved hjelp av øyegjenkjenning kan være et eksempel på dette.

I 2006 har Datatilsynet fått presentert løsninger for pålogging til informasjonssystemer, fysisk adgangskontroll, timeregistrering, åpning av kasseapparat, ”medlemskort” på treningssentre, ”jakkelapp” på utesteder, og bagasjekontroll på en flyplass. Alle disse baserer seg på bruk av fingeravtrykk.

Fordeler og ulemper

Brukt riktig kan biometri være et godt og effektivt verktøy for sikkerhet. Løsninger som baserer seg på biometri nyter generelt høy tillit i befolkningen, med hensyn til presisjon og sikkerhet. Det er derfor viktig å forhindre uriktig bruk av slike verktøy. Når tilliten til metoden er høy, kan et eventuelt misbruk få store konsekvenser. Det er derfor viktig å øke bevisstheten om at en løsning som benytter biometri ikke nødvendigvis fører til bedre sikkerhet.

To situasjoner er særlig aktuelle:

1. Metoden kan være teknisk svak. Biometrisk avlesning skiller seg i utgangspunktet ikke vesentlig fra andre tekniske sikkerhetsløsninger. Det finnes gode og dårlige løsninger, og det vil være et teknologikappløp mellom sikre løsninger og angrep på disse. Dårlige fingeravtrykkslesere kan for eksempel akseptere avkappede fingre og gummihansker med påmontert falske fingeravtrykk.
2. Mangelfull identitetskontroll ved innregistrering. Dersom feil person blir registrert i utgangspunktet, kan en ikke si at løsningen er sikker, selv om den benytter seg av biometri.

Den viktigste grunnen til å være varsom med bruk av biometri er at biometriske kjennetegn unikt beskriver det enkelte individ, og er uløselig knyttet til oss. En persons biometriske kjennetegn kan ikke skiftes ut. Dersom kriminelle finner metoder for identitetstyveri ved å utnytte svakheter i de biometriske løsningene, vil ofrene for dette bli utsatt for betydelige problemer. Hvordan misbruket kan skje ser vi ikke rekkevidden av i dag.

Biometri kan også være bærer av annen informasjon enn det rent identifiserende. DNA er et åpenbart eksempel på dette. Men også biometrisk avlesning av øynene, ansiktet eller benbygningen kan si noe om helse og etnisk bakgrunn. Vi overskuer ikke i dag hva som på sikt kan utledes av slike målinger.

Innsamling av biometriske opplysninger kan gjennomføres uten at vi selv er klar over det. Vi legger igjen fingeravtrykk overalt hvor vi ferdes. Det samme gjelder hår og spytt. Disse sporene kan kontrolleres i ettertid uten at vi er kjent med det. I andre tilfeller kan biometri behandles i sanntid, eksempelvis ved at ansiktet gjenkjennes i et kameraovervåkingsanlegg, eller at stemmen gjenkjennes.

Summen av opplysninger vi legger igjen, med eller uten den enkeltes bevissthet, kan tegne en tydelig profil av hvem vi er og hvilke preferanser vi har. Det faktum at det er opplysninger som er uløselig knyttet til oss, tilsier at de skal behandles med ekstra varsomhet. Hovedregelen bør være at dersom det finnes alternative og tilnærmet likeverdige løsninger, så bør man velge den løsningen som er minst inngripende i forhold til personvernet.

Biometrisk informasjon lagres normalt i form av en såkalt ”template”. Dette er en kodebasert representasjon av materialet, i stedet for å lagre en hel måling, for eksempel et fullt bilde av fingeravtrykket, med alle dets detaljer. Det er to grunner til at dette har blitt en normal tilnærming å håndtere biometriske data på: For det første er det mindre inngripende for personvernet, og for det andre er en slik representasjon godt egnet for elektronisk behandling.

Datatilsynet anbefaler at man så langt mulig unngår sentral lagring av personopplysninger basert på biometri. Opplysningene bør lagres nærmest mulig brukeren. Brukeren kan for eksempel bære opplysningene med seg på et smartkort, eller de kan lagres i den enkelte avleser, på det enkelte bruksted. Et annet virkemiddel mot misbruk er å gjøre den lagrede informasjonen unik for den enkelte installasjonen. At man er innrullert i en biometrisk løsning bør ikke innebære at det uten videre er mulig å overføre slike opplysningene til et annet system. Man kan forhindre dette ved at templatene krypteres med en unik nøkkel for den enkelte installasjon.

Det er ikke minst også grunn til å være skeptisk til bruk av biometriske løsninger i sammenhenger hvor man hittil ikke har sett noe som helst behov for å identifisere enkeltpersoner.

9.3.3 Pass, nasjonalt identitetskort og elektronisk ID

De tradisjonelle identitetskortene er under rivende utvikling. Vi ser nå en betydelig utrulling av elektroniske identiteter og fjernavlesbare identitetskort. Utviklingen krever bevissthet i forhold til nye trusler og muligheter.

Elektroniske identiteter kan innebære en forbedret sikkerhet på Internett. Datatilsynet ser imidlertid en fare for at utviklingen vil kunne føre med seg større krav om at en må identifisere seg, også for tjenester der det strengt tatt ikke er nødvendig. Identifikasjonsplikt i tilknytning til slike tjenester vil igjen kunne føre til et større overvåkingspress. Siden teknologien er ny for de fleste, må man legge særlig vekt på å informere den enkelte når elektroniske identitetskort utstedes. Den enkelte må få vite hva det innebærer, og hvordan man bør gå frem for å sikre seg.

Fjernavlesing av identitetskort kan være effektivt i mange sammenhenger, men vil samtidig innebære en personvernrisiko. Faren for overdreven spredning av opplysningene blir større når pass og identitetskort blir utstyrt med radiofrekvensbrikker for fjernavlesning. Opplysningene vil kunne leses av den som har avlesningsutstyr, og være i et format der opplysningene lett lar seg legge inn i databaser. Dette vil kunne føre til terskelen for uthenting og lagring av slike data reduseres ytterligere. Den enkelte har ikke nødvendigvis mulighet til å vite når noen har lest av vedkommendes identitetsopplysninger.

Nye pass med biometri og elektronisk fjernavlesing

Datatilsynet er av den oppfatning at sikkerheten i de nye biometriske passene som ble introdusert høsten 2005 er mangelfullt utredet. Dette gjelder særlig i forhold til bruk av kontaktløs brikke.

Ved introduksjon av de nye passene ble lagring av informasjon på brikkene avgrenset til personalia og høykvalitetsbilde av passinnehaver. Det foreligger imidlertid planer om å supplere dette med lagring av fullt fingeravtrykk.

Etter det Datatilsynet erfarer har en rekke andre land foretatt betydelig testing og sikkerhetsvurderinger av den kontaktløse teknologien. I Norge gjenstår fortsatt, etter Datatilsynets vurdering, en tilfredsstillende implementering av sikkerhetsløsninger. Andre land har også gitt langt bedre informasjon til passinnehaverne, enn hva norske myndigheter har gjort.

Av over 240 000 utstedte elektroniske pass har kun fem personer, i følge politiet, bedt om innsyn i den elektroniske brikken. Den mest nærliggende forklaringen er at folk flest rett og slett ikke er klar over at passene inneholder en fjernavlesbar elektronisk brikke, og at de har rett til å kreve innsyn i hvilke opplysninger som ligger lagret i denne.

Gyldighetstiden for norske pass er satt til 10 år. De elektroniske passene som ble produsert i 2005 skal altså være tilstrekkelig sikre også i 2015. Datatilsynet vil minne om at andre land har redusert gyldighetstiden for elektroniske pass ned til fem år, nettopp med den uvisse sikkerheten i den teknologiske løsningen som begrunnelse.

Datatilsynet har ikke avsluttet saken mot Politidirektoratet etter tilsynet som ble gjennomført i tilknytning til utstedelse av de nye passene. Etter Datatilsynets vurdering har Politidirektoratet ikke oppfylt de pålegg som ble gitt, og har derfor henstilt Justisdepartementet å følge opp gjennomføringen av vedtakene. Datatilsynet ønsker i det lengste å unngå en sanksjonering av landets øverste politimyndighet.

Nytt nasjonalt identitetskort

Det er ingen allmenngyldige identitetskort i Norge i dag. De identitetskortene folk flest benytter er laget for spesifikke formål; førerkort for den som har tillatelse til å kjøre bil, pass til bruk ved utlandsreise, bankkort til bruk for banktjenester osv. Selv om disse langt på vei har fungert tilfredsstillende, mener mange at det vil være hensiktsmessig med et nasjonalt identitetskort som kan tjene flere funksjoner. I et slikt kort kan man også legge inn e-ID og elektronisk signatur, for bruk på Internett. En rekke aktører har også tatt til orde for at de tidligere nevnte kortene ikke er sikre nok mot misbruk, og at dette i seg selv er en god begrunnelse for å vurdere innføring av et nasjonalt identitetskort.

Det pågikk i meldingsåret en utredning hvor spørsmålet om opprettelse av et nasjonalt identitetskort ble vurdert. Etter det Datatilsynet erfarer er tanken at dette både vil kunne benyttes som et ordinært identitetskort med bilde, og ha en funksjon for elektronisk

identifikasjon (e-ID), slik at man også kan identifisere seg på Internett. Det er planer om at det nasjonale identitetskortet også skal inneholde en elektronisk fjernavlesningsmulighet (RFID).

Datatilsynet har vært representert med en observatør i gruppen som utreder disse spørsmålene. Datatilsynet er generelt bekymret for hvordan den planlagte kontaktløse brikken vil påvirke individets muligheter for anonymitet. Videre er tilsynet også skeptisk til opprettelse av et sentralt register hvor personalia, bilde og biometriske data skal samles. Hvem som skal gis tilgang til å lese av den kontaktløse brikken, og på hvilke premisser, er også sentrale temaer i diskusjonen.

På kortet er det tenkt plassert en e-ID til bruk på Internett, utstedt av en godkjent virksomhet som fungerer som såkalt ”tiltrodd tredjepart”. Denne utstyrer brikken med diverse sikkerhetsmekanismer, og går god for at den elektroniske IDen identifiserer kortholderen. Dette vil innebære en sikrere løsning enn brukernavn og passord alene. Der løsninger med brukernavn og passord forutsetter at man allerede har en avtale med motparten, får e-ID-brukerne en mulighet til å identifisere seg overfor aktører de tidligere aldri har vært i kontakt med. Løsningen vil også kunne være nyttig der det er behov for å skjerme opplysninger for uvedkommende ved kryptering. Datatilsynet ser i dag at det etableres alt for mange dårlige påloggingsløsninger med brukernavn og passord.

Dersom det nasjonale ID-kortet blir frivillig å ta i bruk, og får en godt fundert sikkerhet, vil det kunne gi befolkningen fordeler også av personvernmessig karakter.

9.3.4 Kameraovervåking

Datatilsynet mener å observere en utvikling der enkeltpersoner i økende grad tar i bruk kameraovervåking i forbindelse med nabokrangler. Det synes som om det å overvåke og dokumentere naboens livsmønster i stadig større grad utgjør et element i uoverensstemmelsene naboer i mellom. Formålet må antas å være todelt, henholdsvis sjikane og dokumentasjon av hendelser. Overvåkingen er gjennomgående ulovlig.

Bruk av overvåkingsutstyr har blitt stadig billigere, og mange ser kanskje på dette som en form for forsikring. Dette gir seg ofte utslag i at folk henger opp kamera på hytter for å se "hvordan været er", men også rettet inn slik at man kan følge med på om det er aktivitet på nabohytta. Videre er det en økende tendens til samarbeid mellom politiet og kommunene når det gjelder overvåking på offentlig steder. Særlig gjelder dette områder hvor mennesker har en tendens til å samles på nattestid i helgene. Formålet med overvåkingen er i hovedsak å avverge kriminelle handlinger og å ha bevismateriale ved en eventuell senere straffeforfølgelse.

Kameraovervåking og sporingsbrikke i Mandal

Våren 2006 ble Datatilsynet, gjennom henvendelser fra publikum, oppmerksom på planlagte overvåkingstiltak tenkt igangsatt av Mandal Havnevesen. Det var skissert en inngripende overvåking, der sporingsbrikker og avanserte doomkameraer skulle overvåke både båtliv, gateliv og private eiendommer i nærheten av havnene.

Havnevesenet ønsket å overvåke samtlige småbåthavner og gjestehavner, og i den forbindelse innføre obligatorisk identitetsbrikke for alle båteiere som leier kommunal båtplass. Begrunnelsen for dette var blant annet å hindre fremleie av båtplasser.

Mandal Havnevesen installerte doomkameraer i åtte småbåt- og gjestehavner. Kameratypen har meget god zoomefunksjon og kan dreies 360 grader. Havnevesenet skulle ha

kontinuerlig tilgang til bildene i sanntid, og ha mulighet til å styre kameraene når de selv ønsket det. Kameraene var plassert på kommunalt eide områder som er åpne for fri ferdsel, for eksempel i Havnepromenaden i Mandal sentrum.

Kombinasjonen kameraovervåking og ID-brikke skulle gjøre kontrollen enkel. Havnevesenet kunne på denne måten få oversendt en elektronisk liste over hvilke båter som lå i havnen. Slik kunne de kontrollere at det bare var leietakernes båter som lå der.

Overvåkingssystemet var ikke satt i drift på når Datatilsynet foretok stedlig tilsyn. Datatilsynet konkluderte at overvåkingstiltakene sannsynligvis ville stride mot personvernlovgivningen. Det er blant annet ikke adgang til å overvåke andres private grunn. Datatilsynet krevde derfor at Mandal Havnevesen måtte skjerme andres private områder. Tilsynet mente videre at havnevesenet heller ikke hadde rettslig grunnlag til å kreve at alle skulle montere ID-brikke i båtene.

Havnevesenet frafalt kravet om sporingsbrikke. Etter oversendelse av tilsynsrapporten hadde Datatilsynet også møte med leverandøren av overvåkingssystemene. Det ble gitt råd om en løsning som vil tilfredsstille personopplysningslovens krav, blant annet med maskering av privat eiendom, låsing av kameraposisjon og begrenset tilgang til overvåkingsbildene.

9.3.5 Dop- og rustester i idrett og arbeidsliv

Rusmiddeltesting av ansatte

I 2004 var Datatilsynet på tilsyn hos Securitas AS. Under tilsynet kom det frem at virksomheten innhentet samtykke fra samtlige ansatte til rusmiddelkontroll i form av stikkprøver. Datatilsynet konkluderte med at rusmiddelkontroll av samtlige ansatte var i strid med arbeidsmiljøloven og ulovfestet praksis på området. Personopplysninger innhentet gjennom kontrollen fant derfor ikke noe behandlingsgrunnlag i personopplysningsloven. Vedtaket ble påklaget til Personvernnemnda.

Ny arbeidsmiljølov som kodifiserer tidligere praksis med hensyn til rusmiddeltesting trådte i kraft 1. januar 2006. Etter lovens § 9-4 kan rusmiddeltesting finne sted når det følger av lov eller forskrift, ved stillinger som innebærer særlig risiko og når arbeidsgiver finner det nødvendig for å verne liv eller helse. I februar 2006 forelå Personvernnemnda vedtak i saken. Nemnda tok utgangspunkt i den nye loven og opprettholdt Datatilsynets vedtak, med henvisning til at rusmiddeltesting bare kan finne sted i de tilfeller som er nevnt i arbeidsmiljøloven.

Dopingtester ved treningssentre

Antidoping Norge har i samarbeid med Norsk Treningssenterforbund utarbeidet et antidopingprogram som tilbys treningssentrene. Deltakelse i programmet inkluderer blant annet kurs for de ansatte, informasjonsmateriell og et visst antall dopingprøver av treningssenterets medlemmer.

Treningssenteret innhenter samtykke til testing fra det enkelte medlem. Vanligvis skjer dette ved inngåelse av treningsavtale. Samtykke til testing er ikke noe vilkår for medlemskap. Ved positiv prøve kan treningsavtalen bli sagt opp.

Datatilsynets la til grunn at dopingtester av treningssenterets medlemmer er et for inngripende og lite egnet virkemiddel til at personvernulempene ved testene oppveies. Det ble derfor fattet vedtak om at testene måtte opphøre. Datatilsynets vedtak ble etter klage

omgjort av Personvernnemnda. Dopingtester kan nå gjennomføres under forutsetning av at treningssenteret har fått konsesjon fra Datatilsynet.

Dagens lovgivning inneholder ingen formalisert avgrensning av nedslagsfeltet for mulige dopingtester. Datatilsynet etterlyser derfor lovgivers gjennomgang og et politisk engasjement med tanke på utforming av regler som styrker muligheten for å beholde dopingfri idrett og aktivitet i Norge, samtidig som grunnleggende personvernhensyn og rettssikkerhet ivaretas.

9.4 Helse

Det er et stadig press på bruk av enkeltpersoners helseopplysninger i ulike sammenhenger. Bruken er først og fremst drevet av gode intensjoner - som forskning for bedre behandlingsmetoder og å finne årsakene til sykdommer og dårlig helse.

Men også andre aktører er på banen. Forsikringsselskapene er interessert i innsyn i den enkeltes pasientjournal i forbindelse med tegning av forsikring og utbetaling av forsikringspenger etter skade.

I helseforetakene har Datatilsynet erfart at tilgangen til pasientopplysninger er så vid at enkelte leger velger å utelate informasjon fra pasientjournalen når de behandler annet helsepersonell.

Helseopplysningene våre blir mer tilgjengelige. Til tross for at utgangspunktet for bruk skal være den enkeltes samtykke, er det mer og mer av bruken som skjer med hjemmel i et annet grunnlag enn samtykke, og uten den enkeltes kjennskap. Slik bruk av helseopplysninger kan i seg selv oppleves som et inngrep i den enkeltes integritet. I 2006 ble det avdekket at en forsker fra Rikshospitalet-Radiumhospitalet HF bygget på fingerte data i noen av sine forskningsarbeider. I debatten etterpå ble det diskutert hvordan dette hadde kunnet pågå i så stort omfang.

Det ble satt fokus på behovet for internkontroll og ledelsesforankrede beslutninger og oppfølging også når det gjelder forskning. Nylennautvalget foreslo i sitt forslag til ny helseforskningslov at forskningsinstitusjonene måtte utarbeide et internkontrollsystem.

Allerede våren 2004 påpekte Datatilsynet at svært mange helseforskningsinstitusjoner manglet det internkontrollsystemet de er pålagt å ha etter personvernlovgivningen. Institusjoner som har utarbeidet et godt internkontrollsystem har ikke hatt de samme problemene med å følge lovverket som de som har vært uten et slikt system.

Internkontrollsystemet fungerer som en viktig rettesnor for forskere når det gjelder fremgangsmåte og krav til gjennomføring av forskningsprosjekter. Datatilsynet bygger denne oppfatningen på erfaringer fra et anselig antall tilsyn innen helsesektoren.

9.4.1 Opprettelse av pseudonyme helseregistre

Helseregisterloven stiller ulike krav til opprettelse av sentrale helseregistre avhengig av hvilken registerform som velges. Det stilles mindre strenge vilkår til opprettelse av registre i pseudonym form, fordi denne registerformen innebærer et mindre inngrep i den enkeltes personvern. Per i dag har vi kun to sentrale pseudonyme helseregistre i Norge, Reseptregisteret og det pseudonyme register for individbasert pleie- og omsorgsstatistikk (IPLOS). Begge registrene er nye, og muligheter og begrensninger i ordningen kan derfor ikke sies å være spesielt godt utprøvd enda.

Helse- og omsorgsdepartementet foreslår i Ot.prp. nr. 49 (2005-2006) at Norsk pasientregister (NPR) gjøres personidentifiserbart. Formålene skal utvides slik at registeret kan benyttes til medisinsk og helsefaglig forskning, og som datagrunnlag for sykdoms- og kvalitetsregistre. Stortinget forventes å behandle forslaget primo 2007.

Helse og personvern er to forhold som i de fleste sammenhenger ikke lar seg måle i penger. Opprettelsen av et nytt NPR innebærer at det må tas et verdivalg for den videre utviklingen av helsevesenet i Norge.

Datatilsynet mener at et så omfattende register som det legges opp til, representerer en fare for personvernet. I den grad et slikt register likevel skal opprettes bør man anvende et såkalt pseudonym for den registrerte, med koplingsnøkkelen lagret hos en uavhengig instans. Med en slik løsning vil den registrertes personvern være langt bedre ivaretatt, samtidig som man kan oppfylle intensjonene med registeret. Datatilsynet kan ikke se at en slik løsning forhindrer noe av den tiltenkte bruken av registeret.

NPR vil inneholde en stor samling med sensitive opplysninger og planlegges som et register som skal følge pasienten fra fødsel til død – og deretter oppbevares på permanent basis. Denne personinformasjonen vil kunne komme på avveie. Det er, etter Datatilsynets oppfatning, bare et spørsmål om tid før noe slikt vil inntreffe. Konsekvensene av feil vil kunne bli alvorlig når den valgte registerform gjør det enklere å finne tilbake til enkeltpersonen bak opplysningene. Dersom det velges en registerform hvor det er åpnet for tilgang til identifiserende opplysninger, vil det også være enklere å ta ut opplysningene til ikke-legitime formål. Misbruksfaren øker drastisk. Eksemplene på mulige feil og misbruk er mange; Uautorisert oppslag (snoking), utilsiktet utlevering grunnet menneskelig feil, svikt i rutiner og tekniske feil. Det kan også være angrep fra utsiden og uautorisert utlevering, der opplysningene kommer på avveie med noens vitende og vilje.

Samtidig med debatten om hvilken registerform det fremtidige personentydige NPR skal ha, er det blitt reist sterk kritikk mot IPLOS. Til tross for at den pseudonyme registerformen er valgt, opplever de registrerte, de pleie- og omsorgstrengende i kommunene, registreringen som et stort inngrep i deres privatliv. For best mulig å kunne nyttiggjøre seg data fra det sentrale IPLOS-registeret, har man sett seg nødt til å innføre retningslinjer og skjemaer for samordnet registrering av opplysninger i IPLOS. Dette har for eksempel ført til at personer som i utgangspunktet kun har behov for hjemmehjelp en gang i uken, er blitt stilt intime og påtrengende spørsmål om toalettvaner og intimhygiene. Dette viser at registrering i seg selv kan oppleves belastende, til tross for at formålene bak registreringen er både legitime, nødvendige og velmenende.

9.4.2 Manglende sikring av pasientjournaler

I samarbeide med Helsetilsynet ble det gjennomført tilsyn med to større helseforetak, Helse Bergen HF og Akershus universitetssykehus HF. Tilsynet fokuserte på om løsningene for elektronisk pasientjournal (EPJ) internt i helseforetaket var gode nok til at helselovgivningens krav om forsvarlighet, taushetsplikt, tilgangsstyring og informasjonssikring ble ivaretatt.

For begge de kontrollerte helseforetakene ble det avdekket at journalsystemene var innrettet slik at taushetsbelagte helseopplysninger ikke var tilstrekkelig vernet mot innsyn fra ansatte som ikke har legitimt behov for opplysningene.

At helseforetakene ikke evner å gi tilstrekkelig fortrolighet rundt opplysningene de mottar for å yte helsehjelp, er etter Datatilsynets syn svært alvorlig. Dette illustreres best ved at

den enkelte pasient må be om innsyn i loggen over oppslag i egen journal, for å kunne avdekke eventuell snoking i journalen.

Det er grunn til å anta at tilsvarende avvik også finnes ved andre helseforetak, og sektoren bør følges opp. Samarbeidet mellom tilsynsmyndighetene evalueres, og vurderes videreført.

9.4.3 Anmeldt for snoking

I 2005 anmeldte Datatilsynet Helgelandsykehuset HF på grunn av brudd på informasjonssikkerheten, etter urettmessig lesing av journalopplysninger. Politiet henla først saken, men Statsadvokaten i Nordland omgjorde henleggelsen. Sykehuset vedtok senere et forelegg på kr 50 000, for sin manglende informasjonssikkerhet.

Innsyn i taushetsbelagte opplysninger ble imidlertid ikke ansett straffbart. Påtalemyndigheten var av den oppfatning at det kun er videreformidling av taushetsbelagt materiale som rammes av helsepersonellovens hovedregel om taushetsplikt. Datatilsynet mener at aksept av en slik tolkning er ytterst problematisk, og anbefaler at forholdet klargjøres i regelverket.

9.4.4 Norsk helsearkiv

I utredningen Norsk Helsearkiv - Siste stopp for pasientjournalene ble det drøftet ulike modeller for depotordninger for pasientjournalene i spesialisthelsetjenesten. Utvalget konkluderte med at det bør etableres en egen depotordning for spesialisthelsetjenestens arkiver. Frem til i dag har arkiver fra spesialisthelsetjenesten blitt avlevert både til kommunale, fylkeskommunale og statlige arkivdepoter. Undersøkelser viser at omfanget av det avleverte materialet er lite. For offentlige institusjoner er det også per i dag en bevaringsplikt av såkalt arkivverdig materiale, men utvalget foreslår at det skal opprettes en felles arkiv- og depotordning for utvalgte pasientjournaler hentet fra hele spesialisthelsetjenesten. Begrunnelsen for dette er blant annet å legge til rette for bruk av materialet i forskning.

Datatilsynet påpekte i sin høringsuttalelse at forslaget vil kunne bryte med prinsippet om at innsamlede og registrerte personopplysninger kun skal benyttes til det formål de er samlet inn for. Registrering av opplysninger i pasientjournal er av avgjørende betydning for å gi pasienten den helsehjelp vedkommende har behov for, og krav på, etter en medisinsk vurdering. Det er videre viktig at den helsehjelp som er gitt, dokumenteres som et grunnlag for fremtidige medisinske vurderinger. Det fremstår imidlertid som langt utenfor det opprinnelige formålet at journalen som hovedregel skal bevares for ettertiden, i sin fullstendige form.

Det er et faktum at de fleste i befolkningen har en oppfatning av at pasientjournalen inneholder svært private og følsomme personopplysninger. Det er ikke ønskelig at andre enn helsepersonell som direkte har med den enkelte pasient å gjøre skal ha tilgang til opplysningene i journalen. Dette rimer dårlig med at det innføres en slik felles arkivordning, med det formål å legge til rette for forskning og andre dokumentasjonsformål.

Det foreslås i dag at et noe begrenset antall institusjoner og materiale skal omfattes av oppbevaringsplikten. Erfaring tilsier likevel at en slik ordning vil skape presedens for senere utvidelse av arkivets omfang. Det er alltid mulig å begrunne et etterfølgende formål for bruk av all type informasjon. Dessuten vil det for enkelte være en belastning i seg selv å vite at ens pasientjournal vil bli oppbevart også etter ens død.

9.4.5 Tilsyn - helseforskning og helseregistre

Tilsyn med nasjonale helseregistre

Tilsyn gjennomført mot fire nasjonale helseregistre avdekket at det gjennomgående var mindre bruk av de utvalgte registrene enn det som opprinnelig hadde vært intensjonen. Det virket som relativt komplisert å administrere innsamling av personopplysninger fra lokale aktører og samtidig oppfylle den databehandlingsansvarliges lovpålagte plikter. Særlig gjelder dette kravet om tilfredsstillende kvalitet på opplysningene.

Det var gjennomgående lite refleksjon rundt hvilke utfordringer bruk av opplysninger fra et slikt register kunne medføre. Datatilsynet konstaterte videre at det ikke var utarbeidet tilfredsstillende rutiner når det gjaldt utlevering av opplysninger fra registrene.

Registrene inneholder, i tillegg til opplysninger som er hentet fra pasientjournalen, egne medisinske opplysninger som ikke blir registret i journalen. Systemet fungerer dermed på siden av pasientjournalsystemet. Følgen av dette er at journalsystemet fragmenteres og viktige sikkerhetstiltak ikke opprettholdes.

Tilsyn med forskningsprosjekter

Datatilsynet gjennomførte høsten 2006 ti tilsyn med tilfeldig utvalgte forskningsprosjekter. Fire av prosjektene var konsesjonspliktige. Det ble her foretatt stedlige tilsyn. Seks av prosjektene var tilrådd av et personvernombud og dermed meldepliktige etter personopplysningsforskriften § 7-27. For disse ble det foretatt brevkontroll.

Det ble fra Datatilsynets side fokusert utelukkende på hvorvidt forskningsprosjektene var gjennomført i samsvar med konsesjonens forutsetninger og vilkår, eller i tråd med den prosjektbeskrivelse personvernombudet hadde gitt sin tilrådning på grunnlag av.

Kontrollene fra de stedlige tilsynene avdekket ikke avvik som ga grunnlag for vedtak.

Det ble kun behandlet avidentifisert materiale i prosjektene, ved at identifiserende elementer var erstattet med kodenøkler. Videre ble det i stor grad også benyttet koder i stedet for mer direkte parametere, for eksempel kjønn og bosted. Muligheten for indirekte identifisering er derfor liten. I daglig bruk vil opplysningene fremstå som anonyme, både for den enkelte forsker og for eventuelle uvedkommende. Det er kun dersom man har tilgang til kodenøkkel at identitet kan avsløres.

Under forutsetning av at kodenøklene sikres tilstrekkelig, også i perioden umiddelbart etter datainnsamlingen, fremstår den praktiske håndteringen av dataene som sikkerhetsmessig tilfredsstillende.

9.5 Arbeidsliv og e-post

I 2005 anmeldte Datatilsynet Redningsselskapet og AS Vinmonopolet for brudd på informasjonsplikten i personopplysningsloven. Politiet henla begge sakene under henvisning til at ”intet straffbart forhold anses bevist”. Datatilsynets mener at henleggelsene bygger på uriktig forståelse av både jus og faktum. Når det gjelder Redningsselskapet la politiet blant annet avgjørende vekt på at arbeidsgiver hadde en datainstruks som åpnet for innsyn i e-post, uten å undersøke om instruksen faktisk ble fulgt ved innsynet. Det ble også lagt til grunn at instruksen var kjent av de ansatte – også de som hadde sluttet i selskapet før instruksen ble innført. Politiets henleggelser går langt i å si at det ikke foreligger noen krav til at ansatte skal informeres ved innsyn i e-post.

Vurderingene med hensyn til hvordan informasjonsplikten skal tolkes vil kunne få betydning også på andre områder, og bryter med den tradisjonelle tolkningen av informasjonsplikten både i Norge og øvrige land omfattet av personverndirektivet.

Informasjonsplikten er en av de viktigste forutsetningene for at den enkelte selv skal kunne ivareta sitt personvern. Dersom informasjonsplikten begrenses, reduseres samtidig den registrertes mulighet til å benytte seg av de øvrige rettighetene etter loven, som for eksempel retten til innsyn i opplysningene. Derfor er begge henleggelsene påklaget. Sakene er nå til behandling hos Riksadvokaten, som har informert om at de vil bli behandlet samlet.

I kjølvannet av disse to sakene fikk Datatilsynet inn en annen sak hvor de ansattes meldte om at deres rettigheter var tilsidesatt (Bazar Forlag AS). Saken skiller seg fra de to tidligere omtalte ved at man, etter tilsynets vurdering, ikke bare hadde gjort fysisk innsyn i de ansattes e-postkasser. Arbeidsgiver hadde også satt opp systemet slik at det, for noen ansattes vedkommende, løpende gikk kopier av all innkommende e-post til forlagssjefen. De ansatte hevder at de ikke var kjent med dette. Saken er anmeldt til Oslo politidistrikt.

De tre nevnte sakene har vært omfattet av svært stor medieinteresse. Dette har ført til at Datatilsynet har mottatt en rekke henvendelser knyttet til innsyn i e-post også i 2006. På bakgrunn av oppslagene i media har det blant enkelte dannet seg en oppfatning om at Datatilsynet anmelder enhver virksomhet som gjør innsyn i e-post, uavhengig av hva som er årsaken til innsynet, og fremgangsmåten som velges. Dette er langt fra realiteten. Datatilsynet har behandlet et tyvetalls muntlige og skriftlige henvendelser om innsyn i e-post, og vært på flere kontroller hos virksomheter etter tips om påstått ulovlig innsyn. Bare i de tre nevnte tilfellene har Datatilsynetanmeldt virksomheten for brudd på personopplysningsloven. Bakgrunnen for dette er dels at reglene om innsyn i e-post har vært uklare, og at straffebestemmelsene i personopplysningsloven er lite anvendbare. Mange av virksomhetene har også gått frem på en redelig og skikkelig måte, som ikke bryter med personopplysningsloven.

En positiv konsekvens av oppslagene i media er at det er blitt kjent blant både arbeidsgivere og arbeidstakere at Datatilsynet kan besvare spørsmål om innsyn i e-post. Stadig flere virksomheter synes nå å henvende seg til Datatilsynet før man går til det skritt å gjøre innsyn i e-post. Virksomhetene få da rettledning i hvor grensen for hva som er tillatt går, og hvordan de skal gå frem for å holde seg på rett side av loven.

Det er også blitt satt fortgang i arbeidet med utformingen av et presiserende regelverk innen området. Datatilsynet har deltatt i arbeidsgruppen som har utviklet forskriftsforslaget sammen med representanter for Justisdepartementet og Fornyings- og administrasjonsdepartementet.

9.6 Finans og forsikring

Datatilsynet gjennomførte våren 2006 tilsyn hos i alt ti virksomheter innen finanssektoren. Hovedmålet var å kartlegge hvordan kundeopplysninger flyter mellom ulike selskap i samme konsern. Videre ble det foretatt en kartlegging av felles elektroniske kundesystemer, om kundens rettigheter etter personopplysningsloven blir ivaretatt, og kvaliteten på kundeopplysningene.

Bakgrunnen for tilsynsprosjektet var dels begrunnet ut i fra det store antall personopplysninger finanskonsernene sitter med. Personvernundersøkelsen fra 2005 viste at

økonomiske opplysninger er ansett som svært følsomme, nummer tre etter fødselsnummer og helseopplysninger.

Tilsynene viste at finanskonsernene i all hovedsak følger personopplysningsloven og vilkårene i bankkonsesjonen når det gjelder flyt av kundeopplysninger.

Derimot er Datatilsynet mindre fornøyd med at tilgangen til kundesystemene i bankene er svært vide. Kundebehandlere har ofte tilgang på alle opplysningene som er registrert på bankens kunder. Dette innbefatter også opplysninger som kan gi til dels følsom informasjon om den enkelte. Tilsynsprosjektet avdekket videre at de fleste bankene har for dårlige rutiner for sletting av gamle kundeopplysninger. Mange banker var ikke kjent med konsesjonens regler for sletting.

Prosjektet ble videreført også høsten 2006. Her ble det satt fokus kundebehandlernes tilgang til personopplysninger om kunder. Datatilsynet besøkte i denne omgang mindre selskap, og alle disse tilsynsobjektene hadde tilfredsstillende rutiner for tilgangskontroll i forhold til kundeopplysninger. Dette viser at det er mulig å finne gode løsninger for å oppnå en tilfredsstillende tilgangskontroll.

Tilsynene rettet mot finanskonsern viste at bankkonsesjonen kan være noe uklar og lite praktisk, særlig når det gjelder vilkårene for sletting. Det er også grunn til å se nærmere på blant annet tilgangsstyring og begrepet vesentlig mislighold. Datatilsynet vurderer å endre konsesjonen på disse punktene, og vil følge opp med møter med bransjen med tanke på utforming av en ny bankkonsesjon.

Det kan også være hensiktsmessig å drøfte mulighetene for at den registrerte, som et supplement til virksomhetens egen kontroll, kan få en bedre innsikt i hvor ofte vedkommendes personopplysninger er blitt gjort tilgjengelig for ansatte i banken, eller andre. Dette kan bidra til å disiplinere ansatte fra å foreta uautorisert innsyn i for eksempel kunders banktransaksjoner. Det kan være mest naturlig å fremme dette som et frivillig tiltak i sektorer hvor tillitsforholdet mellom den registrerte og behandlingsansvarlig er helt avgjørende, som i finanssektoren.

9.6.1 Leietakere skal ikke kredittvurderes

I en klagesak har Personvernnemnda vurdert kriteriene for å innhente kredittopplysninger ved utleie av boliger når husleien betales forskuddsvis.

Datatilsynet krevde at KLP Eiendom Trondheim sluttet å kredittvurdere potensielle leietakere. Datatilsynet tolker saklighetskravet i personopplysningsforskriftens § 4-3 slik at det må foreligge et kredittelement før innhenting av kredittopplysninger. Et slikt element av kreditt foreligger ikke når husleien betales forskuddsvis.

Personvernnemnda er enig med Datatilsynet i at det som hovedregel er i forbindelse med inngåelse av avtale hvor man har til hensikt å yte kreditt at man kan innhente kredittopplysninger. Dette er ikke et krav i følge regelverket, men en tolking av forskriftens krav om saklig behov for kunne innhente kredittopplysninger.

Slik Personvernnemnda tolker kravet om saklig behov, vil det ikke alltid være tilstrekkelig at det foreligger et kredittelement, dersom den forretningsmessige risiko er lav. Motsatt vil det ikke alltid være nødvendig med et kredittelement, dersom den forretningsmessige risiko er høy.

Kravet til saklig grunn vil være oppfylt når bestilleren skal bruke kredittopplysningene i forbindelse med sin vurdering av kredittrisiko, for eksempel ved et tilsagn om lån eller avtale om løpende ytelser som faktureres etterskuddsvis. Dette kan typisk være ved bestilling av mobiltelefonabonnement og lignende.

En husleieleiekontrakt innebærer normalt ikke at utleier yter leietakeren kreditt. Boligen stilles til leietakers disposisjon, mot at leietaker innbetaler et depositum og betaler husleien forskuddsvis hver måned.

Nemnda er ikke enstemmig i sin avgjørelse, men et flertall mener at risikoen KLP løper er normal ved forretningsdrift, og at en eventuell kredittvurdering ikke vil fjerne denne risikoen. Videre legger flertallet vekt på at utleie av boliger til privatpersoner står i en særstilling, fordi husvære er et nødvendighetsgode.

Flertallet viser også til at det finnes gode alternativer til kredittvurdering, som referanser, bankgaranti, kommunal garanti, eller depositum.

9.6.2 SWIFT – internasjonale pengeoverføringer

Norske banker har, gjennom det globale transaksjonssystemet for internasjonale pengeoverføringer, SWIFT, utlevert personopplysninger om sine kunder til amerikanske myndigheter. USA ønsker med bakgrunn i kampen mot terror, kontroll over alle banktransaksjoner. Amerikanske myndigheter har utformet en liste over potensielle finansielle bidragsytere til terrorvirksomhet (OFAC) og ønsker å kontrollere informasjon fra SWIFT-systemet opp mot denne listen.

SWIFTs hovedkontor er plassert i Belgia, men en kopi av alle opplysninger som passerer transaksjonssystemet finnes også i USA. Da USAs Department of Treasury etter den 11. september 2001 kom med et krav om å få tilgang til opplysningene, følte SWIFT seg tvunget til å gi dem det. Datatilsynet mener, i likhet med de øvrige personvernmyndighetene i Europa, at SWIFT manglet et tilfredsstillende rettslig grunnlag for utleveringen. Datatilsynet undersøker saken i forhold til norsk rett og har i den forbindelse tatt kontakt med SWIFT Norge, Norges Bank, Finansnæringens hovedorganisasjon og Sparebankforeningen.

9.7 Salg og markedsføring

Dagens markedsføringslov stiller krav til forhåndssamtykke for markedsføring ved bruk av e-post, sms, telefaks og automatiserte oppringninger. Telefonmarkedsføring er unntatt fra denne regelen, og Barne- og likestillingsdepartementet spør i et høringsnotat om unntaket bør oppheves. Departementet ber høringsinstansene kommentere alternative forslag til endringer i regelverket.

Datatilsynet støtter i sin høringsuttalelse til ny markedsføringslov forslaget om krav til forhåndssamtykke også for direkte markedsføring per telefon og post.

Tilsynet går med dette inn for at dagens reservasjonsordning avvikles og erstattes med et register over de som faktisk ønsker direkte markedsføringshenvendelser.

Tilsynet mener det er nærliggende å trekke den slutningen at markedsføring per telefon er den typen direkte markedsføring folk flest finner mest plagsom. Dette underbygges av en undersøkelse gjennomført av Norstat våren 2006, på vegne av Norsk Markedsanalyse Forening. Hele 83 prosent av de spurte oppgir at salg per telefon ikke er greit. Selv om

Datatilsynet mottar færre klager knyttet til direkte markedsføring enn tidligere, mener tilsynet likevel at henvendelsene er for mange.

Datatilsynet innser imidlertid at innføring av et samtykkeregister får negative konsekvenser for bransjen. Det er imidlertid ikke noe i veien for at markedsførere oppretter et samtykkeregister i egen virksomhet og kontakter personer i dette registeret, i tillegg til personer som står oppført i det sentrale samtykkeregisteret.

Ved å innføre forhåndssamtykke for direkte markedsføring per telefon og post, finner Datatilsynet det naturlig å samtidig diskutere en samordning av regelverket. Tilsynet mener at spørsmål knyttet til direkte markedsføring har en nær tilknytning til forbrukerfeltet, slik at hele bestemmelsen i personopplysningsloven bør overføres til markedsføringsloven. Med en slik samordning blir det enklere for markedsførere og publikum å forholde seg til regelverket.

Vedlegg 1

Nøkkeltall for 2006

Datatilsynets tilsynsvirksomhet omfatter kontrollaktiviteter mot i alt 150 virksomheter. Datatilsynet innførte i 2004 såkalt "brevlige tilsyn" som et supplement, og i noen tilfeller alternativ, til "stedlige tilsyn". Brevlige tilsyn velges i hovedsak ved systemrevisjoner og ved verifisering av konkret dokumentasjonsplikt, men omfatter ikke besøk hos virksomheten. Sistnevnte kategori innebærer som benevnelsen indikerer fysisk besøk hos virksomheter underlagt kontroll fra Datatilsynets side.

Følgende bransjer (eller temaområder) var underlagt tilsyn i 2006:

Bransje / Sektor	**Antall**
Arbeidsliv	7
Barnevern	9
Finanssektoren *	15
Fjernsynsovervåking	32
Forsikring *	6
Forskning *	11
Helseforetak	2
Internett – søkemotorer	3
Justissektoren	2
Kommune	1
Lydopptak *	30
Personprofiler *	20
Private etterforskere	3
Sletting innen rusomsorg *	12
EURODAC	1
Schengen informasjonssystem	1
Sum	**150**

Feltene merket med * ble gjennomført som brevlig kontroll, men supplert med stedlige tilsyn.