DET KONGELEGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

St.meld. nr. 5

(2008–2009)

Datatilsynets og Personvernnemndas årsmeldingar for 2007

DET KONGELEGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

St.meld. nr. 5

(2008–2009)

Datatilsynets og Personvernnemndas årsmeldingar for 2007

Innhald

1 **Fornyings- og administrasjons-departementet sin innleiing** 5

2 **Fornyings- og administrasjons-departementets merknader til Datatilsynets årsmelding for 2007** 7

3 **Fornyings- og administrasjons-departementets merknader til Personvernnemndas årsmelding for 2007** 10

4 **Administrasjon og ressursar** 10

Vedlegg

1 Datatilsynets årsmelding 2007 12

2 Personvernnemndas årsmelding 2007 50

DET KONGELEGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

St.meld. nr. 5

(2008–2009)

Datatilsynets og Personvernnemndas årsmeldingar for 2007

Tilråding frå Fornyings- og administrasjonsdepartementet av 24. oktober 2008, godkjend i statsråd same dagen.
(Regjeringa Stoltenberg II)

1 Fornyings- og administrasjonsdepartementet sin innleiing

I eit samfunn med stadig meir overvaking, kontroll og elektroniske spor, kan personvern sjå ut til å ha blitt eit knapt gode. I byar og på større tettstader er kameraovervakinga omfattande, og vi blir registrerte med tid og stad kvar gong vi bruker bankkortet som betalingsmiddel. Daglegdagse gjeremål som mobil- og PC-bruk etterlet seg òg tydelege spor i lang tid. Når vi blir tråkka for nær, reagerer dei fleste. Men til dagleg er det få av oss som ser ut til å bry seg om den massive registreringa av våre kvardagslege aktivitetar.

2007 var likevel eit år med stor merksemd om personvernspørsmål. Fleire saker om til dels vesentlege inngrep i innbyggjarane sin privatsfære vart omtalte i media. Blant sakene finn vi debatten om implementering av datalagringsdirektivet, spørsmål om «nakenscanning» på norske flyplassar, fjernsynsovervaking på buss, tog og t-bane, og spørsmål om innsyn i pasientjournalar. Vi var òg vitne til fleire saker om massiv utlevering av personopplysningar via ulike nettløysingar som følgje av dårlege tryggleiksrutinar, med påfølgjande merksemd om identitetstjuveri.

Medvit om personvern

Datatilsynet gjennomførte ei undersøking om haldningane i befolkninga til ein del aktuelle personvernspørsmål i februar 2008 (Personvernundersøkinga 2008). Særleg dreidde spørsmåla seg om haldningar til datalagringsdirektivet (EU-direktiv 2006/24/EC). Over 60 % av dei spurde svarte at dei er heilt eller delvis einige i at det ikkje er rimeleg å lagre trafikkdata om personar som ikkje er mistenkte for eller har gjort noko gale. Tilsvarande prosentdel av dei spurde svarer at dei trur at den innsamla informasjonen vil bli misbrukt. Til samanlikning er det nesten 90 % av dei spurde som er heilt eller delvis ueinige i at ein skal lagre opplysningar om kven som sender brev til kvarandre i alminneleg post.

Det er nærliggjande å tolke den negative haldninga til lagring av opplysningar om avsendar og mottakar av post, både elektronisk og papirbasert, dit at befolkninga misliker denne typen kontroll. Dei fleste opplever at kommunikasjonen deira er privat, og slik ønskjer dei framleis å ha det. Samtidig ser vi stadig oftare at folk publiserer svært personleg informasjon i ulike samanhengar på nett, eller sender konfidensiell informasjon i usikra e-post, utan at dei har eit medvite forhold til moglege konsekvensar av dette. Folk har altså reflekterte oppfatningar om personvern når dei blir spurde, men i praksis blir personvernet ofte medvite eller ikkje medvite tilsidesett, eller gløymt.

Sjølv om mange gir uttrykk for at dei er skeptiske til overvaking og kontroll, ser det likevel ut til at dei aksepterer ei rekkje inngrep i privatsfæren når dei opplever at dei personvernkrenkjande

tiltaka gir dei tryggleik mot ulike former for kriminalitet. Dei er altså villige til å ofre litt personvern for å føle seg trygge. Samtidig viser Personvernundersøkinga 2008 at det ikkje er kriminalitet og terror folk er mest redde for. Det innbyggjarane fryktar mest, er hendingar som sjeldan kan avverjast ved overvaking og registrering av personopplysningar. Dei fryktar hendingar som trafikkulykker, helseproblem eller brann. Ca ein fjerdedel av dei spurde i Datatilsynets undersøking svarer då òg at dei meiner at verkemidla i kampen mot terror har gått for langt.

Datatilsynets kontinuerlege arbeid for å skape medvit om personvernspørsmål, både blant dei registrerte og dei handsamingsansvarlege, er viktig og nødvendig. Fornyings- og administrasjonsdepartementet støttar derfor tilsynets satsing på ulike informasjonstiltak. I år er det særleg kunstkonkurransen med tema «privatlivets fred» som står i fokus. Fire kunstnarar er valde ut til å presentere kunstverk med personvern som tema i ei utstilling på Oslo S hausten 2008.

Regelverksarbeid

Då personopplysningslova vart vedteken i 2000, la Stortinget til grunn at det ville vere føremålstenleg med ein etterkontroll av lova når den har verka ei tid. Justisdepartementet er godt i gang med denne etterkontrollen, og tek sikte på å ferdigstille eit høyringsbrev om kort tid. Som ledd i etterkontrollen, vart det òg fremja ein proposisjon om nokre endringar i personopplysningslova sommaren 2008, Ot.prp. nr. 71 (2007-2008). Endringane gjeld ein ny forskriftsheimel, heimel for ilegging av gebyr ved brot på lova og endringar i heimelen for innkrevjing av tvangsmulkt.

Fornyings- og administrasjonsdepartementet har ansvaret for personopplysningsforskrifta, og Kongens forskriftskompetanse etter personopplysningslova er delegert til departementet. Sidan hausten 2006 har departementet arbeidd med nye forskriftsføresegner om innsyn i e-post. Høyring av utkast til føresegner viste at partane i arbeidslivet har svært ulike syn på kva som er formålstenleg regulering på området. Departementet har lagt mykje ressursar i å arbeide vidare med dei innkomne høyringssvara. Det vert no utforma reglar som på ein god måte balanserer trong for innsyn og informasjon med trong for personvern og ein privat sfære. Reglane er først og fremst viktige i arbeidslivet, der ein har sett ei rekkje saker der arbeidsgivar ønskjer innsyn i den tilsette sin elektroniske kommunikasjon. Men dei vil òg gjelde på andre område, som i foreiningar og organisasjonar, og innafor høgskule- og universitetssektoren.

Personvernregelverket verkar i eit miljø prega av rask teknologisk utvikling. Dette stiller krav til eit tidsmessig oppdatert regelverk. Når arbeidet med etterkontrollen av personopplysningslova er fullført, vil Fornyings- og administrasjonsdepartementet derfor òg vurdere trongen for revisjon av resten av føresegnene i personopplysningsforskrifta. Trass i at det er gjort fleire mindre endringar i forskrifta etter at den vart iverksett i 2001, trengst det ein heilskapleg gjennomgang og revisjon i lys av dei lovendringar som måtte følgje av etterkontrollen av lova.

Personvernkommisjonen

Regjeringa ønskjer gode rammevilkår for personvernet i Noreg. Dette inneber mellom anna at vi må ha oversikt over dei utfordringar personvernet står overfor i dagens samfunn, og korleis vi på best mogleg måte kan møte desse utfordringane. Personvernkommisjonen, som vart oppnemnt 25. mai 2007, er eit ledd i regjeringas satsing på personvern. Kommisjonen skal i løpet av året avleggje rapport frå sitt viktige arbeid for å gjere greie for personvernet sine kår i Noreg. Kommisjonen har som mandat å gi ei heilskapleg oversikt over dei utfordringar personvernet møter i dagens samfunn, og å komme med forslag til prinsipp og verkemiddel som kan ivareta personvernet i møte med andre samfunnsomsyn. Den skal òg bidra til debatt om personvernspørsmål, og har i samband med dette arrangert ei rekkje opne debattmøte om personvern i ulike sektorar.

Mange aktuelle personvernsaker har stadfesta trongen for kommisjonen etter at den vart oppnemnd og byrja arbeidet sitt. Teknologisk utvikling, nye moglegheiter og ønskje om effektivitet utfordrar personvernet. Samstundes som teknologisk utvikling utfordrar personvernet, kan teknologisk utvikling og bruk av personvernfremjande teknologi i somme tilfelle vere løysinga på dei same utfordringane. Regjeringa har derfor store forventningar til kommisjonen sin rapport, som skal leverast i desember 2008.

Internasjonalt samarbeid – personvernutfordringar er grenseoverskridande

Vi må erkjenne at auka bruk av elektronisk kommunikasjon og elektroniske tenester medverkar til stadig fleire personvernkrenkingar med inter-

nasjonalt tilsnitt. Situasjonen er ofte at brukaren er å finne i eitt land og tenestetilbydaren i eit anna. Det kan vere vanskeleg for brukarane å forstå kva for eit land sine lovar som gjeld, og i tillegg å forstå dei konkrete reglane.

Den norske personopplysningslova byggjer på EUs personverndirektiv (dir. 95/46/EF). Lovgivinga i dei andre landa som har implementert direktivet vil derfor bygge på dei same prinsippa som den norske reguleringa. Dette gjeld likevel ikkje for nordamerikansk personvernregulering, som på mange område avvik frå europeisk tradisjon. Dette gjeld til dømes ved registrering og handsaming av personopplysningar som ledd i tiltak mot terror, og ved innsamling og bruk av personopplysningar i marknadsføring og andre kommersielle samanhengar. I samsvar med EUs personverndirektiv art. 25 og personopplysningslova § 29 er det likevel eit krav for overføring av personopplysningar frå EØS-land til tredjeland utanfor EØS-området, at både verksemder og myndigheitene i tredjelandet sikrar ein forsvarleg handsaming av personopplysningar dei mottek frå EØS-området.

Mange nettstader legg til grunn at dei kan nytte personopplysningar som brukarane, både vitande og uvitande, legg att ved bruk av tenestene. Det er krevjande for brukarane å setje seg inn i og forstå konsekvensane av å gi frå seg personopplysningar på utanlandske nettstader. Ikkje minst gjeld dette for barn og unge, som i stadig aukande grad nyttar digital kommunikasjon og samhandling.

Internasjonalt samarbeid er derfor viktig, og det finst ei rekkje arenaer for slikt arbeid. Datatilsynet deltek aktivt i EUs personvernsamarbeid, og finn at dette er ein god arena for tilsynet sin internasjonale kontakt. På eit meir overordna nivå deltek Fornyings- og administrasjonsdepartementet i OECDs personvernarbeid, der det mellom anna er vedteke ein rekkommandasjon om internasjonalt samarbeid om handheving av personvernregelverk. Justisdepartementet deltek i Europarådets personvernarbeid. Som følgje av det internasjonale tilsnittet personvernarbeidet har, meiner Fornyings- og administrasjonsdepartementet det kan bli stadig viktigare å opprethalde eit visst internasjonalt engasjement på personvernområdet, ikkje minst med tanke på alle jurisdiksjonstvistane som kan komme.

2 Fornyings- og administrasjonsdepartementets merknader til Datatilsynets årsmelding for 2007

Informasjonsverksemd

Datatilsynet innleier temadelen i si årsmelding med eit kapittel under overskrifta «Personvern under press». Tittelen har vore ein gjengangar i meldingsåret, noko som tydeleg viser kor viktig Datatilsynet sitt arbeid er. Datatilsynet har i meldingsåret hatt særleg merksemd retta mot tema som innhausting av personopplysningar og identitetstjuveri, mot dei anonyme alternativa som forsvinn og mot snoking i personopplysningar, og har delteke aktivt i samfunnsdebatten om desse spørsmåla.

Undersøkingar viser gong på gong at kjennskap til og kunnskap om personvernregelverket dessverre ikkje er tilfredsstillande. Informasjon om personvern er derfor viktig, og departementet støttar tilsynets satsing på dette området. Særleg vil ein framheve at departementet dei siste tre åra har styrkt tilsynet sine midlar til informasjonsarbeid med kr. 2 mill. årleg. I 2007 har Datatilsynets informasjonsarbeid vore særleg synleg gjennom undervisningsopplegget Dubestemmer og ein kunstkonkurranse som skal leie fram til ei utstilling på Oslo S.

Dubestemmer – filmprosjekt

Arbeidet med Dubestemmer-prosjektet, eit undervisningsopplegg om personvern retta mot ungdom, tok til i 2006. Prosjektet som er eit samarbeid mellom Utdanningsdirektoratet, Teknologirådet og Datatilsynet, er ein stor suksess, og har vekt både nasjonal og internasjonal merksemd. Det blir stadig sendt ut klassesett av det utarbeidde undervisningsmaterialet. Som ledd i undervisningsopplegget vart vidaregåande skular med medielinje hausten 2007 inviterte til å delta i ein filmkonkurranse der tema var personvern og digitale medium. Filmmanusa som vart valde ut blant dei mange deltakarane, er blitt tankevekkjande filmsnuttar om eit viktig tema. Filmane kan ein sjå på www.dubestemmer.no.

Kunstprosjekt

Datatilsynet og KORO inviterte våren 2008 til kunstkonkurranse med personvern som tema. Fire kunstnarar er valde ut, og skal presentere sine verk i ei utstilling som opna på Oslo S 1. oktober 2008.

Val av utstillingslokale er spennande fordi det gjer det mogleg å vise tankevekkjande kunst til eit breitt publikum. I tillegg er Oslo S eit område godt dekt av fjernsynsovervaking, noko som med sine ibuande personvernutfordringar òg gir ei spennande ramme for ei utstilling om personvern.

Innhausting av personopplysningar

2007 var året då datainnhausting vart eit kjent omgrep i norske medium. Datainnhausting er den norske omsetjinga av det engelske omgrepet «data harvesting». «Data harvesting» er i utgangspunktet eit nøytralt omgrep, som blir brukt om alle former for innsamling av opplysningar, både personopplysningar og annan informasjon, både lovleg og ulovleg. Her vil vi bruke omgrepet om situasjonar der einkvan urettmessig tileignar seg personopplysningar via ulike nettløysingar.

Fleire nettstader med bestillingsløysingar for mobiltelefonitenester vart i meldingsåret utsette for «angrep» frå uvedkommande som lasta ned store mengder personopplysningar via desse nettstadene. Slik datainnhausting er mogleg dels som følgje av dårlege tryggleiksløysingar, dels som følgje av at det finst mykje personopplysningar tilgjengeleg på nett. Dei ulike åtaka viste at det ikkje berre er nettstadene sine kundar som blir utsette for datainnhausting, men òg vilkårlege tredjepersonar. Personopplysningane hamna hos nokon som «ikkje har noko med» dei registrerte å gjere. Slik urettmessig utlevering av personopplysningar krenkjer personvernet til dei registrerte.

Ein teletilbydar hadde ei nettløysing som mogleggjorde innhausting av personopplysningar, og vart i april 2008 gitt eit førelegg på kr. 150.000 for brot på personopplysningslova sine tryggleiksføresegner og manglande varsling om tryggleiksbrotet. Førelegget er vedteke. Reaksjonen frå påtalemakta er eit viktig signal til andre næringsdrivande om å ta tryggleiksutfordringane på alvor.

Den enkelte kan føle ubehag og uro over at opplysningane har hamna på avvegar. For samfunnet kan datainnhausting svekkje tilliten til all elektronisk handsaming av personopplysningar. Det er tyngande for den som vert ramma å leve med frykta for at identiteten kan bli misbrukt, at andre kan gi seg ut for å vere han eller henne (identitetstjuveri), til dømes ved å skaffe seg kreditt i namnet til vedkommande. Identitetstjuveri kan medføre store praktiske problem og mykje ubehag for dei som blir utsette for slikt.

I denne samanheng er det viktig at næringsdrivande, offentlege verksemder og andre systemeigarar har gode rutinar for sikring av personopplysningar, slik at personopplysningar ikkje vert feilaktig utlevert. Det er òg avgjerande at dei har gode rutinar for identitetskontroll av kundar og andre registrerte. Det ser framleis ut til å vere ei utbreidd misforståing at personopplysningar det ikkje er teieplikt for, som fødselsnummer, namn eller adresse er eigna til identitetskontroll. Fødselsnummer skal ikkje vere ein nøkkel for tilgang til personopplysningar det gjeld teieplikt for. Og dersom ulykka først er ute, må det vere klårt at det er systemeigaren som ber ansvaret for ev. manglar eller svikt i eigne tryggleiksrutinar. Som ledd i arbeidet med etterkontrollen av personopplysningslova vil regjeringa vurdere om det er naudsynt å endre reglane om bruk av eintydige identifikasjonsmidlar, som fødselsnummer (personopplysningslova § 12). I samband med arbeidet med ny straffelov vurderer regjeringa òg om identitetstjuveri i seg sjølv skal vere straffbart.

Regjeringa vil òg sjå nærare på moglege tiltak for å lette situasjonen for den som blir utsett for identitetstjuveri. Dette kan til dømes vere eit «single point of contact», betre rutinar hos kredittgivarar, inkassobyrå etc. for å handtere førespurnader frå offera for id-tjuvar og/eller høg prioritering av meldingar av id-tjuveri hos politiet.

Offentleg sektor forvaltar store mengder personopplysningar, og det er viktig at tryggleiken er god i offentlege it-løysingar. Regjeringa har utarbeidd eit rammeverk for autentisering og signering i elektronisk kommunikasjon internt i og mellom offentlege etatar. Dette rammeverket gir grunnlag for harmoniserte risikovurderingar i ulike offentlege verksemder, og legg til rette for gjenbruk av tryggleiksløysingar på mellomhøgt og høgt nivå.

Arbeids- og velferdsforvaltninga

Tilsynet har i årsmeldinga si vigd merksemd til handsaming av personopplysningar i arbeids- og velferdsforvaltninga. Arbeids- og velferdsforvaltninga er eit stort forvaltningsområde med mange tilsette og svært mange brukarar. Det vart gjennomført tilsyn med sektoren i meldingsåret, og Datatilsynet er uroa over dei funna dei gjorde. Mellom anna fann dei at tilgangen til personopplysningar er svært vid etter gjennomføring av NAV-reforma, og at det er manglar i informasjonstryggleiken. Fornyings- og administrasjonsdepartementet legg til grunn at personvern blir teken på alvor i arbeids- og velferdsforvaltninga, og at ein heile tida har fokus på å handsame personopplysningar på best mogleg vis.

Datatilsynet gjev uttrykk for ein kritisk haldning til forslaget til reglar om arbeids- og velferdsforvaltninga sin tilgang til fullstendige pasientjournalar som ledd i arbeidet med å hindre trygdemisbruk. I samband med høyringa av forslaget til desse reglane, kom det inn fleire gode innspel som synte at det var trong til å gjere forslaga klårare når det gjeld tilhøvet til personvernet. I proposisjonen er det difor innarbeidd reglar som gjer det klart når opplysningar kan innhentast, formkrava som gjeld for dette og kva reglar som gjeld for handsaminga av opplysningane i etaten. Slik reglane om arbeids- og velferdsforvaltninga sin tilgang til pasientjournalar for kontrollføremål no kjem fram i Ot.prp. nr. 76 (2007-2008), meiner regjeringa at dei balanserer omsynet til brukarane sitt personvern med kva forvaltninga treng av informasjon.

Samferdselssektoren

Datatilsynet peiker i årsmeldinga på den raskt aukande registreringa av personopplysningar som finn stad i samferdselssektoren, ein sektor som omfattar både elektronisk kommunikasjon og transport av gods og passasjerar. Det blir stadig færre moglegheiter for anonym ferdsel. Innanfor elektronisk kommunikasjon er det særleg datalagringsdirektivet, og konsekvensane det vil få for personvernet, som har prega debatten. Debatt oppstod òg då Avinor hausten 2007 uttrykte ønskje om å bruke såkalla nakenscanner/kroppscanner i tryggleikskontrollen på norske flyplassar.

I transportsektoren skjer det likevel omfattande registrering av personopplysningar utan at den er emne for stor debatt, mellom anna i samband med passering i automatiske bomstasjonar, ved bruk av elektronisk billettering og i ulike reisebestillingssystem. Registrering av personopplysningar i samferdselssektoren dreier seg om omfattande registrering av daglegdagse hendingar som samla gir eit detaljert bilde av rørslene våre. Sjølv ein så alminneleg ting som ein mobiltelefon i veska vil leggje att mykje informasjon om rørslene til eigaren i løpet av ein dag. Det er ei utfordring å sjå dei ulike tiltaka og registreringane i samanheng, slik at ein får det totale biletet av situasjonen. Ofte ser ein dei ulike tiltaka isolert, og kvar for seg verkar kanskje ikkje inngrepa i innbyggjarane sitt personvern så stort. Samla sett kan det likevel dreie seg om vesentlege inngrep. Ei meir heilskapleg oversikt over situasjonen og utfordringane er derfor heilt naudsynt for å kunne vurdere ulike tiltak for å sikre personvernet til dei registrerte.

Regjeringa vil gi en grundig framstilling av personvernutfordringar i samferdselssektoren i Nasjonal Transportplan 2010-2019 som skal leggjast fram for Stortinget våren 2009.

Tilsynsverksemd

Då personopplysningslova vart iverksett i 2001, vart mykje av Datatilsynet sitt fokus flytt frå konsesjonshandsaming og førehandskontroll til tilsyn og etterfølgjande kontroll med etterleving av regelverket. I samsvar med dette, har Datatilsynet i meldingsåret hatt ei omfattande tilsynsverksemd. Tilsyn blir gjennomført hos ansvarlege for handsaming av personopplysningar i både offentleg og privat sektor. Departementet finn det urovekkjande at tilsynsverksemda gjennomgåande viser at det i mange verksemder er svært vid tilgang til personopplysningar over lang tid, dårleg tilgangskontroll og dårleg tryggleik rundt kundane sin eigen tilgang til opplysningar (innloggingsløysingar).

Når stadig meir informasjon om den enkelte blir sentralisert i store, omfattande register, er tilgangskontroll viktig. Det er viktig både å avgrense tilgangen til opplysningane i forhold til det som blir vurdert som tenestleg behov, og å føre kontroll med den faktiske bruken av tildelte tilgangsrettar, til dømes gjennom logging av tilgang. I følgje Datatilsynet er kunnskapen om og etterlevinga av personopplysningsregelverkets tryggleiksføresegner ikkje så god som ønskjeleg. Datatilsynet har utarbeidd omfattande rettleiingsmateriell om informasjonstryggleik, og drive ein god del informasjonsverksemd knytt til dette. Når etterlevinga likevel ser ut til å vere mangelfull, gir dette grunn til ettertanke.

Regjeringa vil vurdere ulike måtar å forbetre kunnskapen om og etterlevinga av dei gjeldande reglane om informasjonstryggleik. Reglane er omfattande, og det kan vere ein viss fare for at særleg mindre verksemder opplever pliktene som for tyngjande. Det kan derfor vere grunn til å gjere ein særskild gjennomgang av personopplysningsforskrifta sine føresegner om informasjonstryggleik og internkontroll. Med grunnlag i ein slik gjennomgang, kan ein vurdere om reglane bør endrast, eller om det bør setjast i verk andre typar tiltak, som til dømes ein gjennomgang av eksisterande informasjonsmateriell med tanke på å gjere det betre.

3 Fornyings- og administrasjonsdepartementets merknader til Personvernnemndas årsmelding for 2007

Fleire av dei klagesakene Personvernnemnda handsama i 2007 var av prinsipiell art. Dette gjeld mellom anna saker om rekkjevidda av personopplysningslova § 7 og spørsmål om bruk av fingeravtrykk som ledd i identitetskontroll. Nemndas oppgåve er i utgangspunktet berre å ta stilling i konkrete enkeltsaker. Departementet vil likevel peike på at avgjerder i denne typen prinsipielle saker lett får verknad ut over den konkrete saka, og at det vil kunne oppstå eit rettleiingsbehov.

Personvernnemnda peiker i si årsmelding på utfordringar knytte til personopplysningslova § 7, som regulerer forholdet mellom personopplysningslova og ytringsfridom. Dette er eit vanskeleg område sett i lys av den omfattande publiseringa av skriftleg materiale som føregår på nett, noko som etter nemndas vurdering gir grunn til rettspolitisk ettertanke. Både ytringsfridomen og retten til vern om privatlivet er konvensjonsverna menneskerettar. Fornyings- og administrasjonsdepartementet viser her til at òg Personvernkommisjonen i sitt arbeid har merksemd retta mot denne typen problemstillingar. Regjeringa vil vurdere ev. tiltak på dette området i samband med den pågåande etterkontrollen av personopplysningslova og oppfølging av personvernkommisjonens rapport.

Bruk av biometriske kjenneteikn i identifikasjonssamanheng blir stadig meir populært. Talet på klagesaker (PVN-2006-08 til PVN-2006-11) om temaet stadfester dette. Nemnda har i meldingsåret gjort fleire prinsipielle vurderingar av kor nødvendig det er å bruke biometriske data for å oppnå tilfredsstillande identifikasjon i høve til føremålet med bruken. Både Datatilsynet og Personvernnemnda har lagt seg på ei streng tolking av regelverket. Nemnda stiller i ei av sine avgjerder, Tysvær kommune (2006-07, avgjord i 2006), spørsmål ved om det er rett at bruk av fødselsnummer og bruk av biometriske data skal regulerast likt, slik tilfellet er i dag når det blir vurdert slik at begge delar fell inn under personopplysningslova § 12. Nemnda støttar Datatilsynets forslag om særleg regulering av bruk av biometriske metodar, og ei prioritering av dette området i det pågåande arbeidet med etterkontroll av personopplysningslova. Regjeringa deler tilsynsmyndigheita si vurdering av situasjonen, og det er derfor sett i gang eit særskilt utgreiingsarbeid om biometri som ledd i etterkontrollen med personopplysningslova.

Ny samansetjing av personvernnemnda

Nemnda peiker i si årsmelding på at den stadig oftare møter problemstillingar av generell forvaltningsrettsleg karakter i sakshandsaminga. Kompetanse på dette området er derfor viktig for nemnda, særleg når nemnda no pga reguleringa av funksjonstida for medlemmene, står framføre fleire utskiftingar. Departementet vil ta omsyn til mellom anna dette når det skal setjast saman ny nemnd som skal verke frå 1. januar 2009. Nemnda skal elles vere samansett av både juristar og medlemmer med annan kompetanse som set den i stand til å gjere avvegingar av personvernomsyn mot andre sentrale samfunnsomsyn.

4 Administrasjon og ressursar

Datatilsynets budsjett og rammevilkår

Datatilsynet hadde i 2007 eit budsjett på drygt kr. 25 mill. Vesentlege delar av dette går til å dekkje lønnskostnader. Personvernundersøkinga som vart gjennomført i 2005 viste at det er stor trong for informasjon om personvernregelverk. Òg fokus på personvernspørsmål i media, til dømes identitetstjuveri og datalagringsdirektivet, viser at personvern er eit aktuelt område. Aktiv deltaking i den offentlege debatten for å målbere personvernomsyn, som er ei av dei viktigaste oppgåvene til Datatilsynet, krev ressursar. Departementet har derfor dei siste åra valt å tilføre Datatilsynet midlar for å setje tilsynet i stand til å styrkje sitt informasjonsarbeid om rettar og plikter etter personopplysningslova. Tilsynet vart òg i 2008 tilført ei generell styrking på 1 million. Datatilsynet har fått mykje positiv merksemd om informasjonsarbeidet sitt, særleg arbeidet retta mot barn og unge, og budsjettstyrkinga er oppretthalden òg i inneverande år.

Personvern er ikkje berre ei sak på det nasjonale planet. Særleg problemstillingar knytte til Internett, gir personvernarbeidet internasjonal dimensjon. Samarbeid med tilsynsmyndigheiter i andre land er derfor viktig. Datatilsynet deltek mellom anna i EUs Art. 29-gruppe, som er EUs rådgivande organ i personvernspørsmål. Det er oppretta fleire undergrupper under Art. 29-gruppa, og Datatilsynet er aktiv i fleire av dei. Ein del av tilsynets budsjett er derfor bunde opp i reiseutgif-

ter. Departementet deler Datatilsynets vurdering av at internasjonalt samarbeid er viktig, og støttar tilsynets prioritering i denne samanhengen.

Personvernnemndas budsjett og rammevilkår

Personvernnemndas sekretariat er ei deltidsstilling, og har kontor saman med Forbrukarrådet og Forbrukarombodet. Nemnda er nøgd med sekretariatsordninga, og departementet meiner at ordninga fungerer godt. Nemnda sitt budsjett er i inneverande år på kr. 1,6 mill.

Det er gjennomført 9 nemndmøte og 11 saker er avgjorde. Saksmengda i Personvernnemnda har vore stabil sidan 2005, men det ser ut til at sakene blir stadig meir kompliserte og prinsipielle. Sjølv om talet på saker er forholdsvis stabilt, kan arbeidsmengda derfor likevel auke. Det er viktig at Personvernnemnda har ei vernebuing for ein auke i talet på saker og/eller arbeidsmengd, slik at ein kan unngå lang sakshandsamingstid.

Ved utgangen av 2008 har leiar og nestleiar pluss to medlemmer av Personvernnemnda fungert i to periodar av fire år. Det er då ikkje høve til å gjenoppnemne desse. Det er viktig at Personvernnemnda gjennom sine arbeidsmetodar sikrar ein viss kontinuitet ved skiftet av leiing. Det kviler i denne samanheng òg eit stort ansvar på sekretariatet.

Stortinget utnemner Personvernnemndas leiar og nestleiar, som begge skal vere juristar. Fornyings- og administrasjonsdepartementet utpeikar deretter dei andre fem medlemmene i nemnda. I arbeidet med å finne nye nemndmedlemmer skal Fornyings- og administrasjonsdepartementet leggje vekt på at nemnda i arbeidet sitt skal vege personvernomsyn og andre samfunnsomsyn mot kvarandre. Nemnda må ha så vel juridisk som teknologisk kompetanse i tillegg til god kompetanse på andre viktige samfunnsområde. I tillegg til faglege kvalifikasjonar, blir det òg lagt vekt på ei viss geografisk spreiing og balanse mellom kjønna når Personvernnemnda vert sett saman. Departementet er godt i gang med det krevjande arbeidet med å finne nye medlemmer til nemnda.

Fornyings- og administrasjonsdepartementet

t i l r å r :

Tilråding frå Fornyings- og administrasjonsdepartementet av 24. oktober 2008 om Datatilsynets og Personvernnemndas årsmeldingar for 2007 vert send Stortinget.

Vedlegg 1

Datatilsynets årsmelding for 2007

Del I

1 Om Datatilsynet

Datatilsynet vart etablert 1. januar 1980 i samsvar med den dåverande personregisterlova vedteken i 1978.

Datatilsynet har til oppgåve å verne den enkelte mot at personverninteressene blir krenkte gjennom handsaming av personopplysningar. Personopplysningar skal handsamast i samsvar med grunnleggjande personvernomsyn som trongen for vern av personleg integritet og privatlivets fred. Det juridiske grunnlaget for Datatilsynets verksemd er regulert i Lov om behandling av personopplysninger av 14. april 2000 (personopplysningslova) og Lov om helseregistre og behandling av helseopplysninger (helseregisterlova) av 18. mai 2001.

Datatilsynet er eit uavhengig forvaltningsorgan, administrativt underordna Fornyings- og administrasjonsdepartementet. Sjølvstendet inneber at departementet ikkje kan gi instruks om, eller omgjere Datatilsynets utøving av myndigheit etter personopplysnings- eller helseregisterlova. Personvernnemnda er klageinstans for Datatilsynets vedtak. Nemnda leverer si eiga årsmelding.

Datatilsynets oppgåver

Som ei følgje av at personopplysningslova den 1. januar 2001 kom i staden for den tidlegare personregisterlova, vart hovudtyngda av Datatilsynets arbeid flytta frå førehandskontroll til kontroll i etterhand. Dette i form av tilsynsarbeid, informasjon og oppfølging av brot på regelverket.

Datatilsynet skal halde seg orientert og informere om den nasjonale og internasjonale utviklinga i handsaminga av personopplysningar, og om dei problema som knyter seg til slik handsaming. Datatilsynet skal identifisere farar for personvernet og gi råd om korleis dei kan unngåast eller avgrensast. Deltaking i råd og utval er derfor ein viktig del av Datatilsynets arbeid. Òg som høyringsinstans i saker som kan ha ein konsekvens for personvernet har Datatilsynet innverknad på samfunnsutviklinga.

Datatilsynet fører ei offentleg liste over alle handsamingar av personopplysningar som er melde inn. Vidare handsamar Datatilsynet søknader om konsesjon, der lova krev dette.

Gjennom aktivt tilsyn og sakshandsaming kontrollerer Datatilsynet at lovar og forskrifter for handsaming av personopplysningar blir følgde, og at feil og manglar blir retta. Datatilsynet assisterer bransjeorganisasjonar med å utarbeide bransjevise åtferdsnormer, og gir bransjar og enkeltverksemder råd om sikring av personopplysningar. Datatilsynet motiverer òg til, og støttar verksemder som på frivillig basis har oppnemnt eit eige personvernombod.

Sist, men ikkje minst, har Datatilsynet òg ei viktig ombodsrolle. I samband med dette driv ein rådgiving og informasjon overfor enkeltpersonar som tek kontakt med tilsynet. Publikum generelt når ein i første rekkje gjennom aktiv mediekontakt og publisering på eigen nettstad. For å skape merksemd og interesse kring personvernspørsmål deltek Datatilsynet aktivt i den offentlege debatten og legg stor vekt på å praktisere meiroffentlegheit.

2 Organisasjon og administrasjon

Datatilsynets budsjett og rammevilkår

Budsjettet for Datatilsynet var i overkant av 25 millionar kroner, av desse var to millionar øyremerkte til kommunikasjonsprosjekt. Ca 65 % av det samla budsjettet går til lønnskostnader, fordelt på 33 medarbeidarar. Datatilsynet har peikt på at det er lite rom for å setje i gang tiltak som ikkje direkte knyter seg til juridisk sakshandsaming eller tilsynsverksemd. Overføringa for kommunikasjonsprosjekt er derfor vidareført i 2007.

Som tilsynsorgan skal Datatilsynet dekkje heile landet, inklusive Svalbard, og gjennomføring av tilsyn medfører ein del reiseverksemd.

Organisasjon

Datatilsynet var i 2007 bemanna med 33 årsverk, som fordeler seg slik:

- Direktøren
- Juridisk avdeling 12 medarbeidarar
- Tilsyns- og tryggleiksavdelinga 5 medarbeidarar
- Administrasjonsavdelinga 7 medarbeidarar
- Informasjonsavdelinga 8 medarbeidarar. 4 av desse er juristar knytte til Datatilsynets juridiske svarteneste, Frontservice. Frontservice svarer på førespurnader per telefon og e-post ved sida av ordinær sakshandsaming.

Datatilsynet vurderer kjønnssamansetninga jamleg og søkjer å ta omsyn til å rekruttere i høve til denne om kvalifikasjonane elles er like. Fire kvinner har i heile eller delar av verksemdsåret hatt svangerskapspermisjon.

Datatilsynet har som mål å arbeide aktivt for at etaten til kvar tid gir kvinner og menn like arbeidsforhold og like sjansar til karriereutvikling og fagleg utvikling. Gjennomsnittsalderen i Datatilsynet er for tida 40,9 år for menn og 38,7 år for kvinner.

Tre medarbeidarar slutta i verksemdsåret.

Datatilsynet ønskjer å stimulere til eit kulturelt og kompetansemessig mangfald i staben. Vidare legg ein til rette for ein personalpolitikk som skal verke motiverande, og hindre utstøyting av personar med nedsett funksjonsevne. Datatilsynet er knytt til avtalen om inkluderande arbeidsliv. Fokus har òg i 2007 vore på tiltak som førebyggjer belastningslidingar. Dette har vore tiltak knytte til trening, ergonomisk rettleiing og instruksjon om tenleg arbeidsteknikk.

3 Sakshandsaming

Det vart journalført 6520 dokument i meldingsåret. Av desse var 2952 innkomne og 3404 utgåande brev frå Datatilsynet. Resten var journalførte interne notat. Dette er omtrent på same nivå som for 2006.

Nye saker (som ikkje har starta i eit tidlegare meldingsår) utgjorde 1928, av desse vart 1428 fordelte til juridisk avdeling, mens 215 og 231 saker vart fordelte høvesvis til Datatilsynets juridiske svarteneste og tilsyns- og tryggleiksavdelinga. Resten av sakene vart fordelte til administrasjonen, informasjonsavdelinga og direktøren.

Av dei nye sakene utgjorde 1/3 klager frå publikum. Flest klager kom inn på områda kredittopplysning, direkte reklame, tele/Internett, arbeidsliv og helse. I meldingsåret mottok tilsynet 506 søknader om konsesjonar. Av desse utgjorde forsking over halvparten av søknadene. Av andre som er verd å nemne er søknader om konsesjon innan forsikring, bank og barnevern. Med unntak av forskinga er dette konsesjonar som i stor grad er standardiserte.

I årsmeldinga for 2006 vart det gjort greie for konsekvensane av tilknyting til ny forskingslov. No vart ikkje ny forskingslov vedteken i 2007, og vil tidlegast bli det i 2008, men synspunkta vil ha same relevans.

Ei sak som i stor grad prega sakshandsaminga i Datatilsynet var dei mange klagene frå publikum i samband med «innhaustinga» av personopplysningar i tilknyting til Tele2-saka. Dette var klager som vart formidla til oss både brevleg, via e-post og telefon. Datatilsynet melde eitt teleselskap til politiet i saka.

Konsesjonsplikta

Plikta til å søkje konsesjon gjeld i all hovudsak for handsaming av sensitive personopplysningar, mellom anna opplysningar om helse, rase, religiøs oppfatning, politisk tilknyting, fagforeiningsmedlemskap, straffbare handlingar og seksuell åtferd.

Datatilsynet kan òg avgjere at andre handsamingar av personopplysningar skal vere konsesjonspliktige, så framt handsaminga openbert vil krenkje tungtvegande personverninteresser.

I 2007 vart det gitt 237 konsesjonar.

Meldeplikta

Meldeplikta inneber at den som ønskjer å setje i gang ei handsaming av personopplysningar skal orientere Datatilsynet seinast 30 dagar før handsaminga startar. Det er likevel ein del unntak frå meldeplikta.

I 2007 kom det inn 2952 meldingar om handsaming av personopplysningar mot 3019 i 2006. Totalt er det no 8946 meldingar i meldingsdatabasen, mot 8954 året før. 2989 meldingar vart sletta frå databasen i 2007 mot 5518 året før.

Klagesaker til Personvernnemnda

I meldingsåret oversende Datatilsynet 7 saker til Personvernnemnda for vidare klagehandsaming: Dette gjaldt:

- Klage på Datatilsynets avgjerd om tilgang til Det norske tvillingpanelet og om bruk av sank-

sjonar mot Universitetet i Oslo for ulovleg bruk av personregister
- Klage på vedtak om krav om samtykke for registrering i historisk database – Bibliotek-systemer
- Klage på vedtak om at utlegging av eigedoms-informasjon i Asker og Bærums Budstikke er å rekne som journalistisk verksemd.
- Elektronisk billettering i Rogaland
- Publisering om personopplysningar om foster-foreldre på internettsida www.likestilling.no
- Klage på avvisningsvedtak – innsyn i person-opplysningar hos OBOS
- Klage på vedtak om bruk av fødselsnummer på www.ung1881.no

Personvernombod

Datatilsynet har òg i 2007 hatt fokus på person-vernombodsordninga. Talet på nye ombod auka like mykje som året før, og tilsynet er stolt over å kunne telje 100 personvernombod.

Den raske veksten stiller òg store krav. Tilsy-net må sørgje for at omboda blir tekne vare på, og at kvaliteten på ordninga er god. For å hjelpe omboda med fagleg påfyll og inspirasjon, har tilsy-net starta ei ordning med å sende ut månadlege nyheitsbrev til omboda på e-post. Her kan det til dømes informerast om vedtak frå Personvern-nemnda, arbeid frå artikkel 29-gruppa og interes-sante artiklar kan leggjast ved.

Utsendinga av nyheitsbreva viser seg òg å vere eit effektivt verkemiddel for tilsynet for å fange opp ombod som ikkje lenger er operative. Det er dessverre slik at mange verksemder gløy-mer å gi melding til tilsynet ved bytte av ombod, til dømes i samband med at eit internt ombod sluttar i verksemda. Datatilsynet har utarbeidd ei liste over verksemder som har personvernombod, som er tilgjengeleg på tilsynets heimeside. Denne skal til kvar tid vere oppdatert.

Datatilsynet har gjennomført fire kurs for eksisterande personvernombod i 2007. To av kursa knytte seg til opplæring av nye ombod. Til-synet synest det er viktig at nye ombod relativt raskt får eit tilbod om grunnleggjande person-vernrett. Tilbakemeldingane frå omboda er gode.

29. og 30. mai 2007 vart det arrangert seminar for alle ombod. For første gong vart omboda delte inn i bransjar i delar av sesjonen, mellom anna bank, inkasso, kommunar, privat verksemd og hel-sesektoren. Ei slik inndeling kravde stor ressurs-bruk av dei tilsette i tilsynet. Omboda var svært nøgde med denne måten å arrangere seminar på.

To av tilsynets medarbeidarar som jobbar med personvernombodsordninga var på studietur til Paris. Der deltok dei på eit seminar som det fran-ske datatilsynet, CNIL, arrangerte, og utveksla erfaringar med franskmennene.

4 Deltaking i offentlege råd og utval

Datatilsynet skal medvirke til å fremje respekten for privatlivet til kvart enkelt samfunnsmedlem, særleg når det gjeld bruk av personopplysningar. Tilsynet arbeider mellom anna for å påverke at nasjonal og internasjonal lovgiving tek omsyn til respekten for at privatsfæren er viktig for å ta vare på menneskerettar, demokratiet og rettsstatens institusjonar.

I meldingsåret har Datatilsynet vore med i føl-gjande råd, utval eller samarbeidsfora:

Arbeidsgruppe for revisjon av person-opplysningslov og personopplysningsforskrift

Personopplysningslova skal etterkontrollerast. I samband med dette er det sett ned ei arbeids-gruppe som arbeider med problemstillingar knytte til lovrevisjonen. Gruppa har medlemmar frå Justis- og politidepartementet, Fornyings- og administrasjonsdepartementet og Datatilsynet. Gruppa hadde ei rekkje møte våren 2007 der Datatilsynet på førespurnad frå Justis- og politide-partementet gjorde greie for trong for endringar. Hausten 2007 vart det ikkje gjennomført nye møte.

Arbeidsgruppe for oppretting av Offentleg elektronisk postjournal (OEP)

Gruppa blir leidd av Fornyings- og administra-sjonsdepartementet. Mandatet er mellom anna å kartleggje trongen for utfyllande felles reglar for journalføring og kvalitetssikring av offentleg jour-nal, med føremål å hindre utilsikta konsekvensar av at journalen blir allment tilgjengeleg over Inter-nett. Arbeidet er ikkje avslutta.

Samarbeidsråd for helsesektoren

Rådet er oppretta av Sosial- og helsedirektoratet med sikte på å koordinere arbeid med informa-sjonsteknologi i helsesektoren. Arbeidet i gruppa tek utgangspunkt i direktoratets strategiplan «E-2007» som omhandlar strategi og planar for å fremje bruk av informasjonsteknologi. Føremålet

med rådet er å styrkje samarbeidet aktørane i mellom og med dei sentrale myndigheitene. Datatilsynet deltek som observatør og oppfattar deltaking i rådet som eit viktig ledd i å kommunisere tilsynet sine standpunkt.

Bransjenorm for helsesektoren

Sosial- og helsedirektoratet har vore initiativtakar til eit større prosjekt der føremålet har vore å utvikle ei bransjenorm for helsesektoren. Norma skal medverke til å harmonisere nivået i helsesektoren når det gjeld informasjonstryggleik. Gjennomførte tilsyn har avdekt stor trong for eit felles løft. Datatilsynet har assistert med råd og rettleiing ved utforming av norma. Arbeidet vart avslutta september 2006. Ei styringsgruppe har teke over ansvaret for forvaltning av norma. Arbeidet no er å få ei tenleg spreiing og implementering av norma i sektoren. Dette skaper store utfordringar ut frå samansetjinga av små, mellomstore og store aktørar. Datatilsynet deltek som observatør i styringsgruppa.

KIS – Koordineringsutvalet for informasjonstryggleik

Utvalet har medlemer frå sju departement, Statsministerens kontor og ni direktorat. Opprettinga av koordineringsutvalet er eit ledd i gjennomføringa av Nasjonal strategi for informasjonstryggleik. Arbeidet omfattar alminneleg IT-tryggleik og spørsmål knytte til rikets tryggleik, vitale nasjonale tryggleiksinteresser og kritiske samfunnsfunksjonar. Utvalet skal samordne vidareutviklinga av IT-tryggleiksregelverket, få fram felles standardar, normer, metodar og verktøy for IT-tryggleik og sørgje for samordning av tilsynspraksis. Utvalet skal òg drøfte aktuelle risiko- og sårbarheitsspørsmål og medverke til koordinering av informasjonstiltak og beredskapsplanlegging Mykje av arbeidet i KIS blir delegert til arbeidsgrupper. Datatilsynet har prioritert å vere aktiv i desse arbeidsgruppene.

SARI – Samordning av regelverk innan informasjonstryggleik

Gruppa er oppretta av koordineringsutvalet. Alle myndigheiter som regulerer informasjonstryggleik sit i denne gruppa. Siktemål er regelverksforenkling innan regulering av informasjonstryggleik.

KOBI – omgrepsapparat innan regulering av informasjonstryggleik

Koordineringsutvalet oppretta KOBI som ei ny gruppe i 2006. Alle myndigheiter som regulerer informasjonstryggleik sit i denne gruppa. Siktemålet er å lage ein metode for klassifisering av informasjon, ut frå trong for vern.

Koordineringsutvalet for E-forvaltning

Utvalet skal arbeide med samordning mellom dei forskjellige offentlege organ for å realisere planen E-2009. Møta blir leidde av Fornyings- og administrasjonsministeren. Arbeidet fokuserer på måla i E-2009, og korleis dei enkelte aktørane kan medverke til å realisere desse.

Arbeidsgruppe for implementering av datalagringsdirektivet

Dette er ei interdepartemental gruppe for implementering av datalagringsdirektivet.

Mandatet til utvalet er å tilpasse ei eventuell innføring av datalagringsdirektivet til norsk lov. Datatilsynet er representert med ein observatør i gruppa. I dette arbeidet har Datatilsynet spesielt lagt vekt på avklaring rundt ei eventuell lagringstid, kvar informasjon skal lagrast, kven som skal ha tilgang og terskel for bruk av data.

Ny folkeregisterlov

Folkeregisteret inneheld nøkkelopplysningar om alle innbyggjarane i landet. Ei rekkje aktørar har teke til orde for å utvide omfanget av opplysningar som blir registerte, og å gi lettare tilgang til opplysningane for aktørar i privat og offentleg verksemd. Datatilsynet deltek med ein observatør i arbeidet.

Nasjonalt identitetskort, elektronisk signatur og elektronisk identitet

Justisdepartementet har teke initiativ til å utgreie trong for nasjonale identitetskort. Datatilsynet deltek med observatørstatus i ei arbeidsgruppe som greier ut dette. Datatilsynet har vore oppteke av mange aspekt ved nasjonalt identitetskort. Mellom desse er kva som skal inngå av opplysningar i kortet, bruk av RFID-teknologi, om det skal etablerast eit sentralt register, og kven som i så fall skal få tilgang til dette. Arbeidet som observatør i denne gruppa har kravd monaleg meir ressursar

enn det Datatilsynet hadde føresett. Dette skuldast i hovudsak at tilsynet har hatt vesentlege merknader til gruppa sine konklusjonar.

NAFAL

NAFAL er eit såkalla «tilpassingsråd for sivil luftfart». Hovudtema er implementering av tryggleiksløysingar på flyplassar. Innan denne tematikken blir det reist ei rekkje spørsmål i forhold til personvern.

5 Internasjonalt samarbeid

Som med deltaking i norske offentlege råd og utval, er òg deltaking på internasjonale møte og arbeidsgrupper ein viktig arena for å påverke lovgivinga på området. EU er den viktigaste premissleverandøren for framtidige personvernrettslege normer og reglar. Datatilsynet har derfor valt å vere deltakar i utvalde arbeidsgrupper under artikkel 29-gruppa. Dei internasjonale møta er òg ein arena for utveksling av synspunkt. Nedanfor er ei oversikt over dei internasjonale arbeidsgrupper og råd som Datatilsynet er representert i.

Artikkel 29-gruppa

Den norske personopplysningslova reflekterer personvernprinsippa som er nedfelte i EU-direktivet om personvern. Saman med kollegaer frå dei ti søkjarlanda til EU-medlemskap, har Datatilsynet delteke som observatør i arbeidsgruppa oppretta etter direktivet artikkel 29. Gruppa har som oppgåve å drive fram koordinering og synkronisering av EU/EØS-landas nasjonale personvernarbeid, med utgangspunkt i personverndirektiv 46/95. Gruppa har ein rådgivande funksjon overfor Kommisjonen og står fritt til å tolke og konkretisere innhaldet i direktivet. I løpet av meldingsåret heldt gruppa fire to-dagars møte i Brussel, i tillegg til det større «vårmøtet», som denne gongen vart arrangert på Kypros.

Gruppa arbeider ofte med utgangspunkt i dokument frå uformelle arbeidsgrupper, der alle medlemslanda kan vere med. Utan at det ligg føre noko formelt vedtak, er det i praksis akseptert at òg observatørland kan tiltre desse gruppene. Datatilsynet har i meldingsåret vore representert i tre slike arbeidsgrupper.

– *Medical Data.* Arbeidsgruppa har hovudfokus på helsejournalar.
– *Identity management.* Arbeidsgruppa tek for seg autentisering og identifisering i den elektroniske verda. Gruppa har ikkje hatt møte i meldingsåret.
– *Internet task force.* Arbeidsgruppa arbeider med internettrelaterte spørsmål, med vekt på det tekniske. I meldingsåret har gruppa mellom anna jobba med definisjonen av omgrepet «personopplysning» og bruk av søkjemotorar på Internett.

Det internasjonale datatilsynsmøtet

Kvart år blir det halde ein internasjonal konferanse for datatilsynssjefar med deltakarar frå heile verda. Konferansen inneheld ein open del som òg andre enn datatilsynssjefane kan delta på. I 2007 vart konferansen halden i Montreal. Datatilsynet deltok med to representantar.

Berlin-gruppa

Den internasjonale arbeidsgruppa for personvern innan telekommunikasjon, Berlin-gruppa, er primært nedsett for å arbeide med tekniske problemstillingar knytte til telekommunikasjon, men handsamar òg andre tekniske problemstillingar. Mellom dei mest sentrale sakene i meldingsåret var:

– Søkjemotorane sin praksis med omsyn til lagring av søk
– Planlagd bruk av det europeiske satellittsystemet Galileo innan samferdselssektoren
– Bruk av RFID i legitimasjonsdokument og betalingskort
– Digitalisert overvaking: Internett og kameraovervaking

Ei rekkje andre tekniske problemstillingar var gjenstand for drøftingar i gruppa. Arbeidet i gruppa gir Datatilsynet viktige bidrag i arbeidet med tekniske problemstillingar.

Police Working Party

Gruppa arbeider med spørsmål vedrørande politisamarbeid som fell inn under tredje søyle, det vil seie utanfor den indre marknaden. Datatilsynet er representert med ein sakshandsamar.

Joint Supervisory Authority

JSA er det felles tilsynsorganet for Schengen Informasjonssystem (SIS). Informasjonssystemet

inneheld opplysningar om personar som er ettersøkte, sakna, nekta innreise til Schengenområdet, eller er straffedømde i eit av medlemslanda. Normalt blir det halde fem møte årleg i Brussel, og Datatilsynet er representert med eitt medlem i gruppa. I tillegg har ein informasjonsmedarbeidar hjelpt til i arbeidet med å utvikle informasjonsmateriell knytt til innføringa av SIS II.

Internasjonalt sakshandsamarmøte

Dette er eit internasjonalt samarbeidsforum for sakshandsamarar. Det vart halde to møte, eitt i Helsinki og eitt i Lisboa. Diskusjonane handla mellom anna om handsaming av personopplysningar på Internett og bruk av biometri. Begge desse temaa vart vurderte som såpass viktige at dei òg blir vidareførte til møta i 2008. I tillegg vart det diskutert bruk av kredittopplysningar i forskjellige samanhengar, overvaking i arbeidslivet og i samferdselssektoren. Datatilsynet var representert med to sakshandsamarar på desse møta.

Nordisk datatilsynsjefmøte

Dette er eit møte for direktørane i dei nordiske datatilsyna, og blir arrangert anna kvart år. I år vart møtet halde på Island.

Nordisk sakshandsamarmøte

Dette er eit årleg nordisk forum for sakshandsamarar. Arrangementet går på rundgang mellom deltakarlanda og i 2007 var turen kommen til Noreg. Møtet vart halde i Bergen og Datatilsynet var representert med tre sakshandsamarar. Møtet hadde særleg fokus på kontroll i arbeidslivet og på samferdselssektoren. I tillegg vart handsaming av personopplysningar på Internett diskutert. Nytt av året var at tilsynsmyndigheitene på Færøyane deltok med to representantar.

Nordisk teknologimøte

Det vart ikkje halde møte i meldingsåret.

6 Informasjonsverksemda

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

Dette er likevel tradisjonelle verkemiddel med sine klare avgrensingar. Datatilsynet fekk derfor i 2006 løyvd to millionar kroner til å utvikle ei ekstra satsing på kommunikasjonstiltak som kan gi både innbyggjarane som rettshavarar og verksemder som plikthavarar auka merksemd, refleksjon og kunnskap om viktige personvernspørsmål. Dei øyremerkte ekstramidlane for kommunikasjonstiltak vart vidareførte og ytterlegare styrkte i 2007, noko som har gitt synlege og dokumentert gode resultat.

Undervisningsopplegget «Dubestemmer»:

«Dubestemmer» er utvikla av Teknologirådet, Utdanningsdirektoratet og Datatilsynet i eit nært og godt samarbeid. Alle desse tre aktørane har medverka med ressursar til å realisere ein utradisjonell og verknadsfull kampanje overfor ungdom som målgruppe. Opplegget er knytt opp til dei nye læreplanane i skoleverket, som inneheld kompetansekrav når det gjeld IKT og personvern.

Undervisningsopplegget vart lansert måndag 29. januar 2007 på eit pressearrangement der fornyings- og administrasjonsminister Heidi Grande Røys deltok. Lanseringa fekk omfattande og positiv medieomtale i landsdekkjande og lokale medium, i tillegg til fagpressa.

Undervisningsopplegget inneheld eit hefte med faktaopplysningar, historiar frå det verkelege livet og diskusjonsoppgåver. Det er òg laga veggplakatar til klasserommet, ein multimediepresentasjon med tre humoristiske, men tankevekkjande filmsnuttar, og ei lærarrettleiing. Alt dette materiellet, og utfyllande informasjon, kan lastast ned frå nettstaden www.dubestemmer.no.

Det vart ved lanseringa sendt ut prøvepakkar på undervisningsopplegget til alle ungdoms- og vidaregåande skular i landet. I samband med nytt skoleår hausten 2007 vart det sendt ut ei ny påminning om undervisningsopplegget, saman med to nye filmar. Dette resulterte i ei fornya interesse og ein ny straum av tingingar. Det er derfor prenta eit nytt, tredje opplag av brosjyren og materiellet som høyrer med.

Per 31.12.2007 har det komme inn meir enn 1 300 tingingar på samla over fem tusen klassesett. Dette inneber om lag 160 000 utsende brosjyrar.

Etter oppdrag frå Datatilsynet har TNS Gallup evaluert undervisningsopplegget mellom dei lærarane som har tinga materiellet. Resultata frå evalueringa er svært oppløftande. To av tre lærarar vurderer elevane si samla interesse for tematikken som stor eller svært stor. Like mange seier at materiellet i stor eller svært stor grad førte til diskusjon og refleksjon i klassen. Nesten alle lærarane opplevde at opplegget auka kunnskapen og medvitet om personvernspørsmål mellom elevane. 78 prosent av lærarane gir opplegget ei bra eller svært bra vurdering som pedagogisk støtteverktøy. Ingen gir undervisningsopplegget ei negativ vurdering, og heile 96 prosent av lærarane ønskjer å nytte opplegget igjen ved eit seinare høve.

Hausten 2007 vart kampanjen presentert for dei andre datatilsynsmyndigheitene i Europa på eit møte i Berlin. Dette har resultert i fleire førespurnader frå land som ønskjer å nytte heile eller delar av opplegget. Brosjyren vart som følgje av den store interessa òg prenta i ein engelskspråkleg versjon, og dei tre filmane fekk engelsk teksting.

I desember mottok Dubestemmer-prosjektet heider og ære i Madrid. Under *European Seminar on Best Practices in Data Protection and Award Giving Ceremony* vart prosjektet tildelt ein *First Special Mention*, det vil si at det fekk heiderleg omtale.

Prosjektets fase to – ungdom som filmskaparar

I løpet av våren 2007 vart elever på Lillehammer vidaregåande skule utfordra til å lage to filmar med personvern og digital mobbing som tema. Elevane skreiv manus nært knytte til situasjonar henta frå deira eigen kvardag. Kortfilmane vart deretter produserte i samarbeid med studentar ved Høgskolen i Lillehammer, og blir per i dag sende ut saman med det andre materiellet i klassesetta.

Tilbakemeldingane i evalueringa som vart gjennomført mellom lærarane viste at kortfilmane i undervisningsopplegget slo godt an. Lærarane ønskte fleire filmar som utgangspunkt for diskusjonar i klassen.

I oktober vart det derfor sendt ut ein invitasjon til alle vidaregåande skular med medielinje om å delta i ein manuskonkurranse med personvern og digitale medium som tema. Ungdom kjenner sjølv best sin eigen røyndom. Film er dessutan ei formidlingsform som når fram til denne gruppa. Håpet er at tematikken ein kjem inn på i dei nye filmane ytterlegare vil medverke til å auke ungdoms medvit og kunnskap om eige og andre sitt personvern.

Mellom alle manus som kom inn, valde ein jury ut vinnarmanusa. I desember vart dei seks vinnargruppene samla i Oslo for ein workshop der dei vidareutvikla manusa etter råd frå filmfaglege mentorar. Filmane gjekk deretter til produksjon på skulane, og heile tida har elevane tilgang til filmfagleg hjelp. Dei seks nye filmane har premiere mars 2008 og vil deretter bli sende ut til alle skulane i landet, i tillegg til å bli lagde ut på Internett.

Datatilsynet har òg gått inn som hovudsponsor for Amandusfestivalen 2008, ein filmfestival for unge filmskaparar under 20 år. Arrangørane inviterte derfor til manuskonkurranse med personvern og digitale medium som tema. Vinnarmanuset vil bli filmatisert av studentar på Den Norske Filmskolen og får premiere på Amandusfestivalen i mars 2008. Dei seks filmane som blir produserte i regi av Dubestemmer-prosjektet vil òg bli viste på festivalen.

Med dette håper Datatilsynet å møte ungdommen der dei er, på deira arenaer, og kunne skape ei auka interesse for og eit medvit rundt temaet personvern.

Opplæring og rettleiing overfor verksemdene

Det er gjennom fleire års tilsynsverksemd blitt dokumentert trong for å motivere og leggje til rette for auka etterleving av personvernlovgivinga i verksemder som handsamar personopplysningar. Dette gjeld offentlege så vel som private.

Takk vere dei ekstra ressursane til betalt kommunikasjon, vart Datatilsynet sett i stand til å gjennomføre informasjonstiltak òg overfor norske verksemder. Målet har vore å auke verksemdene sitt kjennskap til regelverket og pliktene om internkontroll og informasjonstryggleik.

Det er blitt utarbeidd eit nytt og omfattande rettleiingsmateriell, mellom anna:

- Motivasjonsheftet *Pokerfjes*
- Ein fullstendig rettleiar for internkontroll
- Ulike malar for dokument til bruk i internkontrollen
- Tilpassa materiale for verksemder som berre har personopplysningar om eigne tilsette og kundar
- Eit støtteverktøy som hjelper verksemda med å kontrollere si eiga etterleving av dei lovpålagde pliktene

I tillegg vart det kjøyrd ein kampanje overfor utvalde bransjar. Ansvarspersonar i konkrete verk-

semder vart kontakta med tilbod om oppfølging og rettleiing, mellom anna gjennom seminar i Trondheim, Bergen og Oslo. Seminara vart fullteikna.

Jamvel om det er blitt utarbeidd eit fagleg godt og gjennomarbeidd rettleiingsmateriale, har Datatilsynet inntrykk av at materialet i alt for liten grad er blitt teke i bruk av norske verksemder. Dette kjem truleg av at leiinga i verksemdene ikkje har tilstrekkeleg forståing for kvifor dette er viktig. Både offentlege og private verksemder vegrar seg mot å prioritere ressursar til arbeidet. Det blir derfor i praksis nedprioritert inntil det kjem tilsynsbesøk frå Datatilsynet, eller det skjer ei hending som blir oppfatta som kritisk frå verksemdleiinga si side. Masseinnhaustinga av fødselsnummer og andre personopplysningar frå ulike teleoperatørar sommaren 2007 er eit døme på dette. Like eins kommunars ukritiske publisering av personopplysningar på Internett.

Ved bruk av kommunikasjon og dialog er det mogleg å skape monaleg resultat, slik kampanjen overfor ungdom har vist. Datatilsynet meiner derfor at det bør setjast av ressursar til å utvikle presentasjonsmateriell som på ein overtydande måte motiverer til å setje i gang arbeidet med internkontroll og informasjonstryggleik. Det bør òg satsast ytterlegare på ordninga med personvernombod.

Personvern uttrykt gjennom kunst

Fornyings- og administrasjonsdepartementet løyvde sommaren 2007 ekstra midlar til eit prosjekt der personvern skal uttrykkjast gjennom kunst. Tanken er at ein ved å involvere kunstnariske uttrykk utvidar debatten om personvern, privatliv, integritet og overvakingssamfunnet. Tradisjonelt har kunstnarar hatt ei viktig rolle i samfunnsdebatten. Kunstprosjektet kan derfor løfte problemstillingane og tilføre noko nytt, tankevekkjande og viktig. For å ivareta den kunstfaglege kompetansen er det i inngått eit samarbeid med KORO, Kunst i offentlege rom. Det blir arrangert ein open idékonkurranse med arbeidstittelen «Respekten for privatlivets fred» som vil vere open for forskjellige uttrykk innan visuell kunst.

Konkurranseutlysinga vil skje i februar 2008. Utstillinga av dei ferdige verka vil finne stad hausten 2008 på Oslo sentralstasjon.

Personvernrapporten fekk stor merksemd

For fjerde gong vart det laga ein publikasjon som populariserer noko av innhaldet frå årsmeldinga for året før, men som òg skodar framover. *Personvernrapporten 2007* vart prenta i ni tusen eksemplar og distribuert til ca 5 700 mottakarar. Datatilsynet lanserte Personvernrapporten ved å arrangere ein pressefrukost i april. Det møtte opp femten journalistar frå ei rekkje medium, både aviser, tv og radio. Det vart på pressefrukosten gitt heile 21 ulike intervju, som alle resulterte i nyheitsoppslag. Personvernrapporten har utelukkande fått positiv omtale.

På grunn av langt fleire etterbestillingar enn tidlegare år vart det i august trykt opp eit ekstra opplag på 2 000 eksemplar. Per 31.12.2007 var det komme inn 626 etterbestillingar av til saman 2 165 eksemplar.

Datatilsynets heimeside

Heimesida www.datatilsynet.no er på mange måtar sjølve navet i Datatilsynets informasjonsverksemd. Det blir derfor lagt stor vekt på å bruke nettsida aktivt.

Det vart produsert 85 eigenproduserte nyheitssaker i 2007. I tillegg har Datatilsynet halde fram med den planmessige oppbygginga og gjennomgangen av informasjonen om sektorar og spesifikke teknologiar.

Datatilsynet sender e-postvarsel når framsida blir oppdatert til 3 053 abonnentar som sjølve har meldt seg på varslingslista.

Personvernrapporten 2007 vart i meldingsåret lasta ned meir enn 10 500 gonger. Telefonsal og reklame er det undertemaet som blir lese mest på nettsida.

Datatilsynets heimeside vart i 2007 vurdert til ein lågare poengsum enn tidlegare (frå fem til tre stjerner) i Noreg.no si kåring av offentlege nettstader. Delvis skuldast dette strengare krav til kor tilgjengeleg nettsida og stoffet der skal vere. Datatilsynet ser det som eit essensielt mål at nettstaden skal vere best mogleg tilgjengeleg, og har allereie bestilt utbetringar av løysinga.

Datatilsynet vart òg trekt for at ikkje fulltekstdokument/postliste ligg tilgjengeleg på nett, at tilsynet ikkje har delar av sine sakshandsamingssystem tilgjengelege frå Internett, eller har avanserte tovegsløysingar mot innbyggjaren. Men slike løysingar utgjer ein vesentleg risiko når det gjeld tryggleik. Som tilsynsmyndigheit på dette området må Datatilsynet vise spesiell varsemd. I tilsynspraksisen erfarer Datatilsynet at fleire av dei løysingar som blir nytta i dag ikkje tilbyr god nok tryggleik for at det berre er rette vedkommande som får tilgang til opplysningane. I tillegg har mange aktørar problem med å kvalitetssikre utlegginga av dokument. Det medfører at opplys-

ningar som ikkje skulle vore publiserte, likevel hamnar på Internett. Dette kan medføre store konsekvensar for dei som blir utsette for dette.

Tilsynet har spelt inn ein del konkrete råd til departementet når det gjeld e-forvaltning. I tillegg har tilsynet søkt om midlar til eit prosjekt som kan munne ut i ein beste-praksismetode for korleis omsynet til personvern og ønsket om effektivitet og aktiv publisering av saksdokument kan sameinast.

Mediekontakt

Ved sida av heimesida er ein aktiv mediekontakt eit svært prioritert verkemiddel for å skape merksemd og debatt kring trongen for å respektere òg personvernomsyn når nye teknologiar og velmeinte tiltak skal setjast i verk. Som ledd i dette har Datatilsynet sett det som viktig å utvikle ein organisasjon og kultur som gjer at mange medarbeidarar kjenner seg rusta til å uttale seg til media innan eigne saksområde, og delta i debattar på radio og tv. På denne måten har Datatilsynet, sett i forhold til kor stor organisasjonen er, stor kapasitet til å kunne tale personvernets sak når høvet byr seg.

I løpet av meldingsåret har Datatilsynet svart på over 1 350 førespurnader frå media, i form av å gi intervju, eller delta i debattar. Dette har resultert i over fem tusen registrerte medieoppslag der Datatilsynet er omtalt.

Av saker som har fått særleg medieomtale kan nemnast:

- Den sosiale nettverkstaden Facebook
- Fødselsnummer, irekna masseutlevering av personopplysningar
- ID-tjuveri
- Personvernrapporten
- Tilgangar til helseopplysningar, brot på teieplikt
- Bruk av fingeravtrykk og annan biometri
- Lansering av undervisningsopplegget «DuBestemmer»
- Nakenskannar på flyplassar
- NAV – og tilgang til journalar

Datatilsynet har i 2007 òg hatt inne fleire eigenproduserte kronikkar og debattinnlegg.

Foredragsverksemd

Datatilsynet tilbyr ikkje eigne seminar eller kurs ut over det som blir arrangert i samband med personvernombodsordninga. Unntak frå dette var kursa som vart kjørte våren 2007 i samband med den ekstra kommunikasjonssatsinga overfor verksemder om etablering av system for internkontroll. Datatilsynet stiller likevel så langt som mogleg opp med foredragshaldarar når det kjem førespurnader om dette til seminar i regi av andre. Datatilsynet har som følgje av dette vore representert med foredragshaldarar på 140 ulike seminar og konferansar. Nedgangen i forhold til året før er ein konsekvens av ei medviten og strengt naudsynt prioritering.

Tabell 1.1

	2005	2006	2007
Tal foredrag	92	157	140

Publikumsrettleiing

Datatilsynet legg stor vekt på å vere til stades og yte god assistanse overfor dei enkeltpersonar og representantar for verksemder som på eige initiativ tek kontakt for å søkje råd og rettleiing. Dei aller fleste direkte publikumsførespurnader får derfor svar av ei juridisk svarteneste med fire juristar. Desse trekkjer på teknologisk kompetanse når dei har trong for det. I tillegg medverkar dei òg med vanleg juridisk sakshandsaming, i den grad dette ikkje går ut over tilgjengelegheit og service i rettleiingsarbeidet.

Den juridiske svartenesta har i 2007 registrert 7 300 telefonførespurnader med svar, mot tilsvarande 8 125 året før. Nedgangen skuldast hovudsakeleg færre førespurnader om innsyn i e-post og direkte marknadsføring. I tillegg kjem nedgangen truleg òg av at publikum i stadig større grad blir fortrulege med å nytte Internett for å innhente kunnskap og rettleiing, framfor å ty til telefonen.

Tilgjengelegheit/svartid på telefonservicen blir gjennomgåande vurdert å vere svært god. Tilsvarande òg kvaliteten i den rettleiinga som blir gitt.

Kva handlar førespurnadene om?

Tabellen nedanfor viser telefonførespurnadene som den juridiske svartenesta har svart på. Førespurnadene er fordelte på tema, og om innringaren opptrer som (eller på vegner av) plikt- eller rettshavarar.

Den prosentvise fordelinga kan ikkje direkte samanliknast med tidlegare år. Dette skuldast mellom anna at det er gjort enkelte endringar i temakategoriane. Ein må òg vere merksam på at Tilsyns- og tryggleiksavdelinga svarer på ein del

Tabell 1.2

	Plikt	Rett	Total	Prosent
Arbeidsliv	598	557	1155	16 %
Barn/Ungdom	130	78	208	3 %
Biometri	13	22	35	0 %
Fødselsnummer	89	533	622	9 %
Helse/forsking	296	96	392	5 %
Informasjonstryggleik med svar FS	186	202	388	5 %
Internasjonalt (overføring utland)	120	12	132	2 %
Internett (over 18 år)	208	235	443	6 %
Kameraovervaking	361	247	608	8 %
Kunderegister/medlemsregister	229	116	345	5 %
Melding/konsesjon	645	33	678	9 %
Reservasjon – DM	56	505	561	8 %
Velferd	82	76	158	2 %
Økonomi	170	530	700	10 %
Anna	308	567	875	12 %
Sum	3491	3809	7300	100 %

førespurnader om informasjonstryggleik, til saman 1070 førespurnader i meldingsåret. Desse er ikkje med i den omtalte oversikta.

Arbeidsliv er framleis det temaet det kjem flest førespurnader om, sjølv om det har vore ein nedgang frå året før. I tillegg til spørsmål om rutinar for arbeidsgivars innsyn i e-post, logging av datamaskinbruk mv, inngår førespurnader om kameraovervaking og andre systematiske kontrolltiltak frå arbeidsgivars side.

Det er òg verdt å merke seg ein vedvarande og markert nedgang i talet på førespurnader om direkte marknadsføring, særleg knytt til reservasjonsregisteret. Datatilsynet mottok 505 telefonførespurnader frå rettshavarar i 2007. Dette utgjer ein tredel av talet på førespurnader tre år tidlegare. Som tidlegare nemnt var likevel telefonsal og reklame det temaet som var mest lese på Datatilsynets heimeside i 2007. Ei forklaring på nedgangen i talet på førespurnader om direkte marknadsføring kan dermed dels vere at publikum finn svar på spørsmåla sine på nettet, framfor å ringje eller skrive e-post til Datatilsynet.

Tabell 1.3

År	2004	2005	2006	2007
Tal telefonførespurnader om DM	1 496	838	617	505

Talet på førespurnader vedrørande informasjonstryggleik og fødselsnummer har framleis auka. Dette kjem av eit auka fokus i media på saker om manglande informasjonstryggleik, masseinnhausting av fødselsnummer frå teleselskap mv.

Førespurnader per e-post

Det har komme inn 2 673 førespurnader per e-post til den juridiske svartenesta, mot 3 058 året før.

Den juridiske svartenesta har som mål at gjennomsnittleg svartid på e-post ikkje skal overstige to verkedagar etter at førespurnaden kom inn til avdelinga. Ingen e-post skal liggje utan svar lenger enn fem verkedagar. I ein periode var svartidene lengre enn dette, men dette vart i løpet av hausten brakt under kontroll. Ved årsskiftet var det ingen usvarte e-postførespurnader.

Førespurnadene fordeler seg tematisk omtrent som ved telefonførespurnader, likevel slik at spørsmål vedrørande Internett og fødselsnummer utgjer ein noko større prosentdel av e-postførespurnadene enn pr. telefon.

Tilsyns- og tryggleiksavdelinga svarte på 429 e-postførespurnader i 2007.

7 Tilsyns- og tryggleiksarbeid

Dei fleste verksemder innan offentleg og privat sektor kan underleggjast tilsyn etter personopplysningslova. Datatilsynet gjennomfører, i likskap med dei fleste tilsynsorgan, risikobasert tilsynsverksemd. Dette inneber at innsatsen blir retta inn mot område der regelbrot er mest sannsynleg og konsekvensane størst.

Grunnlaget for tilsynsarbeidet ligg i dokumentet «Strategi og metodikk for operativt tilsyn med personopplysningslova». Denne strategiplanen omtaler Datatilsynets forvaltningsområde som heilskap, og legg føringar i forhold til operativt tilsyn. Verksemdsplanen legg føringar for val av sektorar, bransje og/eller tema. I tillegg er oppfølging av tips og klager frå publikum viktig.

Etter at avvika er lukka hos den enkelte verksemda vil Datatilsynet gjerne medverke til at liknande verksemder unngår å gjere dei same feila. Metodane som blir nytta er mellom anna:

- Kontakt med aktuell bransjeforeining eller andre bransjeorgan for å drøfte lovforståing og tolking, initiere bransjenorm eller publisere fagartiklar i medlemsblad.
- Kontakt med eigarinteressene.
- Beskrive problem i media, lage rettleiingar som blir lagde ut på tilsynets heimeside, eller medverke med foredragsverksemd.
- Starte prosjekt der dei nye problemstillingane kan gjennomgåast.

7.1 Funn i fleire sektorar

Informasjonsteknologien er framleis i ein tidleg fase når det gjeld spørsmålet om intern tryggleik og samhandling. Verksemdene føler ein trong for å bruke sine IT-system til å skape betre informasjonsflyt – òg når det gjeld personopplysningar. Problemet er at naudsynte mekanismar for intern tryggleik og trygg samhandling ikkje har vore på plass.

Problemstillinga har i hovudsak fem dimensjonar:

- Kor mange medarbeidarar som har tilgang til personopplysningar
- Tidsrommet desse har tilgang
- Mengda informasjon kvar enkelt har tilgang til
- Kontrollmekanismane kring tilsettes bruk av personopplysningar
- Tryggleik knytt til kundane sin tilgang til eigne opplysningar

Kontrollverksemda til Datatilsynet indikerer at mange verksemder kjem dårleg ut i forhold til fleire av desse dimensjonane. Dette representerer ein markant trussel mot personvernet til den enkelte. Det at verksemdene er for lite restriktive med kven av dei tilsette som får tilgang, kombinert med manglande kontrollmekanismar med kven som gjer oppslag, utgjer truleg den største enkeltrisikoen.

Den manglande tryggleiken rundt kundane sin tilgang til eigne opplysningar følgjer som ein god nummer to. I dei fleste tilfella er det berre krav om ei svak autentisering av kunden før det blir gitt tilgang til personopplysningane.

Brot på føresegnene om informasjonstryggleik og internkontroll er like framtredande som tidlegare år. Gjennomgåande slit verksemder med å dokumentere tryggleiken slik regelverket føreskriv.

Truleg skjer det kvar dag at nokon får krenkt personvernet sitt, utan at det blir kjent for den det gjeld. Det kan vere uautorisert innsyn i ulike typar sensitive personopplysningar, eller gjenbruk av personopplysningar utan at det ligg føre noko nytt handsamingsgrunnlag. Det er ofte svært vanskeleg å avdekkje slike krenkingar, delvis fordi dette skjer i lukka miljø, og delvis fordi systema ikkje er eigna til ein effektiv kontroll av misbruk.

Datatilsynet merker seg at respekten for føresegnene om sletting gjennomgåande er låg. Dette gir grunnlag for bekymring, spesielt når terskelen for å registrere opplysningar òg er låg. Få verksemdsleiarar ser ut til å ha vurdert trongen for å slette personopplysningar. Mange hevdar at langvarig oppbevaring kan vere nyttig for verksemda. Dermed er vi i ein situasjon der fleire og fleire verksemder lagrar fleire opplysningar om individet – over stadig lengre tid.

I tillegg skuldast lagringa eit langt på veg uavklåra forhold til rekneskapslovgivinga som pålegg lagring av visse typar opplysningar i ein gitt periode.

Det blir generert monalege mengder overskotsinformasjon. Regelverket føreset at informasjonen som blir lagra samsvarer med føremålet og skal vere sakleg. Informasjonssystem som blir utvikla blir i mange tilfelle ikkje bygde etter dette prinsippet. Tvert imot blir alle dei opplysningar systemet gir rom for lagra, utan at dei ansvarlege i det heile ser ut til å reflektere over det.

Nærmare omtale av tilsyna er teke inn i fagdelen, del II.

7.2 Nøkkeltal frå kontrollverksemda

Datatilsynets kontrollverksemd omfattar kontrollaktivitetar mot i alt 134 verksemder.

Tabell 1.4

Bransje/Sektor	Tal
Arbeidsliv	1
Biometri	1
Eigedomsmeklarar	6
E-signatur	2
Finanssektoren	1
Forsking	7
Fjernsynsovervaking	25
Fødselsnummer	15
Helse	7
Internett	14
Justissektoren	1
Kommune	6
NAV	4
Nettkafé	2
Offentlege nettstader	5
Rekruttering	3
Rusomsorg	10
Samferdsel	2
Sletting	16
Statleg innkrevjing	3
Telekommunikasjon	2
Trussamfunn	1
Sum	134

Bransjane (eller temaområda) i tabell 1.4 var underlagde tilsyn i 2007.

Del II

8 Tema og tendensar i 2007

Ein viktig del av Datatilsynets mandat er å identifisere farar for personvernet, og gi råd om korleis ein kan unngå eller avgrense dei. Datatilsynet vil trekkje fram sju tendensar som har vore særleg framtredande i meldingsåret.

Tendensane er henta frå erfaringar frå tilsyn og sakshandsaming, frå høyringsarbeidet, deltaking i forskjellige arbeids- og styringsgrupper nasjonalt og internasjonalt, og gjennom saker som Datatilsynet er blitt merksam på gjennom medieomtale. Skildringa av tendensane byggjer på ein grundigare omtale andre stader i årsmeldinga.

8.1 Personvernet er under press

Personvernet er under press på nær sagt alle område der det er gjennomført tilsyn i inneverande år. Når ein ønskjer å innføre eit nytt tiltak, og personvernet blir oppfatta som ei hindring, ser det ut til at mange gløymer at personvernet samtidig må sjåast på som ein viktig garanti for ei skikkeleg handsaming av personopplysningar. I praksis ser Datatilsynet at personvernet ofte må vike, utan at ein vurderer konsekvensane av at denne garantien blir svekt eller fjerna.

Presset kjem frå fleire retningar. Den eine er ei «klassisk Orwellsk» overvaking, der ein Storebror, eller kanskje «småbrør», overvaker andre systematisk som eit ledd i sin kontroll og maktutøving. Datalagringsdirektivet kan stå som eit døme på eit slikt tiltak.

Den andre pressfaktoren kjem frå omsorgsovervakinga. I omsorgsovervakinga blir Storebror erstatta av ei «Store Mor». Mange gode hjelparar vil verne vår helse, økonomi, utdanningsnivå og velferd. Føresetnaden for hjelp er at hjelparane får tilgang til til dømes helseopplysningar, opplysningar om psykososial velferd, mappa frå barnehage og skolegang, spelevanar og medisinbruk. Dersom trongen til dei vaksne ikkje kan grunngi eit tiltak, kan kanskje vernet av det forsvarslause barnet vere grunn god nok?

Effektivisering er ei tredje kjelde til vesentleg press mot personvernet. Det verkar som det å vise omsyn til den menneskelege faktoren i seg sjølv blir oppfatta som ei hindring for effektive løysingar. Ein ønskjer i stor grad å forsyne seg med dei opplysningane ein meiner ein treng. Ein vil ikkje ta seg bryet med å informere eller spørje den opplysningane gjeld, eller den opplysningane stammar frå. Ein vil ha personopplysningane enkelt tilgjengelege for alle i sitt datasystem, og ikkje ta omsyn til at menneske er grunnleggjande nysgjerrige. Ein vil ikkje ta seg bryet med å etablere tilgangskontroll og eit forsvarleg tryggleiksnivå. Resultatet er at innbyggjaren mistar kontrollen med kven som har tilgang til informasjonen om han.

Datatilsynet er sterkare uroa for utviklinga ved utgangen av meldingsåret enn tidlegare år. Ansvarskjensla har vist seg å vere lita hos mange aktørar. I tilsynsrapport etter tilsynsrapport blir det peikt på manglande oversikt over og kontroll med personopplysningar. Problemstillinga blir ytterlegare aktualisert ved utsetjing av driftsoppgåver og IT-system til eksterne leverandørar. Datatilsynet har gong på gong sett at handsaminga av personopplysningar er sett bort til data-

handsamarar utan tilfredstillande avtale, og utan at ein har forvissa seg om at opplysningane er forsvarleg sikra.

Offentlege og private verksemder kan i stor grad skyve konsekvensane ved å tilby dei registrerte eit dårleg personvern over på kunden, pasienten eller brukaren. Når eit menneske har blitt utsett for krenkingar ber han sjølv tapet – i tid, pengar og psykiske påkjenningar. Desse tapa blir ikkje reflekterte i rekneskapane til verksemdene. Nedprioritering av personvern kan dermed vere eit etisk tvilsamt val som likevel blir forsvart ut frå rein bedriftsøkonomisk veging av kostnader og inntekter. Det har vore få saker der den fornærma har reist erstatningssøksmål mot den ansvarlege for handsaminga av personopplysningane.

Kontrollane til Datatilsynet er ikkje nok til å få verksemdene til å etterleve regelverket. Det krevst forståing av trongen for eit godt personvern hos verksemdene sjølve, og eit vakent publikum som reagerer på overtramp. Tal frå personvernundersøkinga frå 2005 tyder på at folk flest har tillit til verksemdene. Dersom ein skal leggje Datatilsynet sine funn til grunn, er mange verksemder, både offentlege og private, ikkje denne tilliten verdig.

8.2 Anonyme alternativ forsvinn

Datatilsynet har gjennom fleire årsmeldingar peikt på tendensen til at dei anonyme alternativa er under spesielt press. I meldingsåret vart det bestemt at det ikkje lenger skal vere mogleg å passere bomringen i Oslo anonymt. Det reelt anonyme alternativet, myntbetalinga, blir teke bort, og bommen blir heilautomatisk.

I fleire fylke ser ein ei oppbygging av sporbar elektronisk billettering i kollektivtransporten.

Løysingar der personlege, elektroniske brikker erstattar ihendehavarbevis som klippekort, dagsbillettar eller kontantar, medfører ein vesentleg fare for personvernet. Datatilsynet meiner det bør vere mogleg å lage dei elektroniske løysingane på ein slik måte at ein ikkje knyter elektronisk billett eller brikke til éin bestemt person. I praksis ser tilsynet likevel at viljen til å lage slike løysingar er bortimot fråverande. Offentlege og private verksemder ønskjer i stor grad å kunne følgje den enkelte personen i sine system.

I meldingsåret kom det òg fram eit forslag om pliktig registrering av sjølve brukaren av telefonen, ikkje berre abonnenten. Her vart omsorga for mobilbrukarar under 18 år oppført som årsak til å gjennomføre ei endring som vedgår alle. Datatilsynet uttalte seg tvilande til at ei pliktig registrering av barn vil føre til færre uønskte førespurnader retta mot dei. Tvert imot meiner tilsynet at fleire foreldre ønskjer at mobilabonnementet skal stå på dei, nettopp for å verne barna. Registreringa av brukaren har då òg i fleire tilfelle ført til at barn, utan at dei føresette har visst om det, er blitt oppførte med fullt namn og mobilnummer på nummeropplysningstenester. Tryggleiken for barnet har dermed ikkje blitt betra.

8.3 Personopplysningar blir ikkje sletta

Lagring av elektroniske data er blitt billegare enn å ha rutinar for sletting. Datatilsynet såg spesielt på sletting i meldingsåret, og avdekte manglande respekt for sletteføresegnene på nær sagt alle område. Så å seie alle tilsyn førte til merknader. Verksemdene vel ofte minste motstands veg, vidare lagring og større harddiskar.

Overgangen frå kontant betaling til elektroniske betalingsmetodar ser ein innanfor dei aller fleste samfunnssektorar. Stadig oftare tek ein vare på all informasjonen ein har, i staden for å lagre berre det som er naudsynt etter rekneskapslovgivinga. Som heimelsgrunnlag viser ein til rekneskapslovgivinga. Det vil seie at detaljopplysningar som før ikkje ville blitt lagra, eller som ville blitt lagra i kort tid, no i staden blir lagra i minst ti år. Dette såg Datatilsynet ved tilsyn mellom anna hos nettbutikkar og hos hotell. I meldingsåret kom det òg fram at fleire fylkesskattekontor bad om innsyn i gamle passeringsopplysningar hos bompengeselskapa. Ein kan lese meir om desse sakene i fagdelen, kapittel ni.

I tillegg ser Datatilsynet ein manglande vilje til å utbetre feil som finst i eksisterande system. Politiet har ikkje sletta eller sanert opplysningar om pågripingar og reaksjonar i Det sentrale straffe- og politiopplysningsregisteret (SSP) etter 2001. Årsaka er ein teknisk feil, og evna til å utbetre registeret ser ut til å mangle. Dette fører til at rettane til dei registrerte blir neglisjerte.

8.4 Snoking blir ikkje avdekt

Datatilsynet har i meldingsåret fått inn fleire førespurnader frå enkeltmenneske som meiner at banktilsette, fengselstilsette, helsepersonell og politi går inn i databasar og les opplysningar om dei, utan å ha tenestleg trong. Datatilsynet har kunna undersøkje ein del av påstandane, og funne at dei stemmer.

Mørketala på området er truleg store. Svært mange verksemder har mangelfull kontroll med kven som slepp til i databasane, og altfor få kontrollerer loggane i etterkant. Derfor vil snokinga i mange tilfelle vere vanskeleg å avdekkje.

Svært mange verksemder opnar for vidare tilgang til databasane enn det som var mogleg tidlegare. Meir enn 13 000 personar har tilgang til politiets sentrale straffe- og politiopplysningsregister (SSP). Talet på NAV-tilsette som kan gå inn i fagsystema til tidlegare Trygdeetaten, sosialtenesta og Aetat er truleg dobla etter samanslåinga. For bankane har vi ikkje gode tal, men òg her har svært mange tilgang til opplysningane om alle kundane.

I praksis har Datatilsynet sett at sjukehus og bankvesen tilbyr betre vern til kjendisar. Datatilsynet går likevel ut frå at ein god del av dei urettmessige oppslaga gjeld snokaren sin eigen omgangskrins, ikkje kjendisar. Same type vern bør ein derfor kunne tilby alle som ønskjer det.

I meldingsåret sende Helse- og omsorgsdepartementet ut eit lovforslag som gjer det tydeleg at helsepersonell ikkje kan lese andres helseopplysningar utan tenestleg trong for det. Datatilsynet er nøgd med forslaget, men føreslår at ein vurderer å ta inn eit supplement, at alle pasientar får ein rett til kostnadsfritt å sjå kven som har slått opp i deira journalopplysningar.

Når verksemdene sjølve kontrollerer loggane, kan ein del oppslag vere vanskelege å identifisere som snoking. Personen det gjeld vil ha betre føresetnader. Tilsynet meiner at ein slik rett til å få vite kven som har hatt tilgang til opplysningane i databasane, òg bør gjelde overfor fleire aktørar.

8.5 Datainnhausting er blitt enklare – store lekkasjar i meldingsåret

8.5.1 Datainnhausting

Datainnhausting er innsamling av store mengder personopplysningar, anten for eigen bruk, eller for vidaresal. Fleire faktorar ligg til rette for at innhausting av informasjon om deg og meg er enklare enn det bør vere i Noreg. Éin ting er å hauste inn informasjon den enkelte har publisert om seg sjølv, frivillig, og med opne augo for at slik nedlasting vil skje. Noko heilt anna er innhausting av informasjon den enkelte ikkje eingong visste var tilgjengeleg for alle, eller informasjon ein pliktar å gi frå seg til heilt andre føremål.

Kombinasjonen av for dårleg tryggleik og liberal praksis med publisering av personrelatert informasjon dannar eit trusselbilete som gir grunnlag for uro. Datatilsynet opplever at aktørane ofte rører seg i gråsona for kva som kan vere forsvarleg. Omsynet til brukarvennlege løysingar, kostnader og dynamikk gjer at ein vel eit for lågt tryggleiksnivå, og dermed skaper unødverdige personverntruslar.

I 2007 vart det vist i praksis at slik innhausting kan gjennomførast i Noreg, at nokon er villig til å gjere det, og at det kan få store konsekvensar. Omlag 180 000 nordmenn vart ramma av denne datainnhaustinga.

Innhaustinga av personopplysningar skjedde ved at einkvan kjørte eit dataprogram mot utvalde nettsider. Ved hjelp av eit anna dataprogram hadde dei generert fødselsnummer som kunne vere i bruk i Noreg. Desse vart seinare sjekka mot ei offentleg nettside for å luke ut nummer som ikkje er tildelt ein person. Fødselsnumra vart brukte til å søkje fram namn og adresse til innehavaren via nettsidene til fleire teleselskap.

Dei fleste det gjaldt hadde aldri hatt noko med dei aktuelle teleselskapa å gjere. Datatilsynet opplevde mange telefonar frå sinte nordmenn som ikkje kunne forstå at dette var mogleg. Saka skapte debatt i media, i styreromma og hos tilsynsmyndigheitene.

Dei som gjennomførte dette, sat tilbake med ein grunndatabase som truleg vil ha ein varig verdi. Ein base som inneheld fødselsnummer, med andre ord ein offisiell, varig og eintydig identifikator, namn og andre kontaktopplysningar til kredittverdige nordmenn. Med ein database av såpass høg kvalitet, kan ein med relativt høg tilslagsgrad føye til annan informasjon. Til dømes frå norske skattelister, som ein finn ordna til for enkel nedlasting på Internett, eller frå andre aktørar som tilbyr dårleg vern av personopplysningar.

8.5.2 Offentleglova

Den nye offentleglova legg opp til at det offentlege i større grad enn før skal kunne gjere sine dokument tilgjengelege på Internett. Gjennom publisering av postlister og dokument på nettet, har mange aktørar i offentleg sektor gjort spørsmålet om offentlegheit til ei global sak. Det norske domenet .no er tilgjengeleg for kven som skulle ønskje det, i Kirkenes, Lindesnes eller New Dehli. Lesaren treng heller ikkje vere eit menneske. Det kan vere maskinar, robotar, som skannar gjennom sidene, indekserer innhaldet og tek vare på det for framtida. Det er mogleg å hauste inn og systematisere informasjon om nordmenn frå kvar som helst i verda.

Søkjemotorane er for lengst identifiserte som moglege truslar mot personvernet. Søkjemotorane har blitt svært kraftige, og gjer personopplysningar tilgjengelege i samla form, trass i at dei i utgangspunktet er publiserte hos ulike aktørar. All samhandling med offentleg sektor som innbyggjaren har, og som ikkje er unnateke offentlegheit, vil vere tilgjengeleg ved søk på namn – med mindre det er sett i verk vern mot dette.

I tillegg til det materialet som blir lagt ut med rette, er det ein del som blir lagt ut ved ein feil, manglande opplæring eller regelrett slurv. Dei som samlar inn informasjon ser sjølvsagt ikkje forskjell på tilsikta og ikkje-tilsikta publisering. Dei treng ikkje eingong å forstå norsk.

Det eksisterer allereie i dag kommersielle verksemder som gjennomsøkjer nasjonale domene etter personopplysningar, samlar desse inn og systematiserer informasjonen. Føremålet er å samle tilstrekkeleg informasjon til at dei kan avgjere at det finst ein betalingsvilje. Verksemda kan dermed selje informasjon om individet som er samla inn over tid frå til dømes offentlege postlister og dokument. Dersom desse verksemdene er lokaliserte utanfor EØS-området, vil det vere svært vanskeleg å handheve rettar nordmenn har fått i personopplysningslova.

8.6 Auka fare for identitetstjuveri i Noreg

Når det blir lagt til rette for enkel datainnhausting, blir innbyggjarane sårbar for identitetstjuveri. Etter gjennomgangen i punkta over, spør Datatilsynet om ein ikkje i realiteten er i ferd med å setje saman ein ståande buffé for identitetstjuvar.

Personopplysningar har fått omsetningsverdi i kriminelle miljø. Dess større mengder informasjon ein ID-tjuv klarer å skaffe til vegar, dess større sjanse har han til å lukkast med å opptre som ein annan person. Å ha eit legitimasjonsdokument vil i dei fleste tilfelle verke overtydande. Dersom identitetstjuven i tillegg kan supplere med detaljert informasjon om offeret, er vegen kort til «gyldig identifisering».

Ein metode som er velkjend for å skaffe tilgang til personlege dokument har vore å omadressere post. Inntil ganske nyleg hadde Posten Noreg AS eit lågterskeltilbod for å endre postadresse. Berre tilgang til fødselsnummer og eksisterande postnummeradresse var naudsynt for ei slik omadressering. Etter påtrykk frå mellom anna Datatilsynet er dette no endra. Det er likevel framleis enkelt å endre adresse. Det held å ta ein telefon til Posten.

For at ein skal vere mindre sårbar for datainnhausting og ID-tjuveri må ein verne personopplysningar betre, òg dei som ikkje er kategoriserte som sensitive.

I meldingsåret fikk vi ein debatt om testing av tryggleik på nettsider. Ei forskargruppe ved Universitetet i Bergens testa tryggleiken i bankane sin elektroniske ID-løysing, BankID. Forskarane publiserte sine funn, og vart møtte med massiv kritikk frå mellom anna bankane og Post- og teletilsynet. Datatilsynet meiner det er viktig med aktive forskingsmiljø som saman med tilsynsmyndigheitene identifiserer veikskapar i slik sentral infrastruktur. Datatilsynet opplever for sin eigen del at mange verksemder ikkje rettar seg etter åtvaringar dei får og at det først er etter omtale i media at det kjem til handling. Tilsynet har derfor forståing for at forskarar finner det naturleg å gå offentleg ut med åtvaringar som ikkje er tekne på alvor hos aktørane. Forskarane har ei svært viktig rolle i forhold til å bidra til å utvikle infrastrukturen i ei positiv retning.

Datatilsynet har merka seg at lovforslaget som følgjer datakrimutvalets delrapport II kan utløyse vanskelege problemstillingar rundt forskarane si rolle i framtida. Kva som blir sett på som kriminell åtferd blir definert så uklårt at samfunnskritisk forsking innan teknisk infrastruktur kan bli skadelidande. Les meir om dette i avsnittet om justissektoren.

8.7 Blir vi tryggare av inngripande tiltak?

Perioden etter tusenårsskiftet har vore prega av hendingane 11. september 2001. Medieoppslag om terror, truslar og vald evnar å setje til side jamvel dei mest overtydande forskingsresultat og statistikkar.

I iveren etter å gi innbyggjarane kjensle av tryggleik, har styresmaktene i fleire vestlege land gått svært langt. Mange er villige til å gå på akkord med grunnleggjande prinsipp, sjølv om dei berre oppnår marginal reduksjon i risiko.

For sterk kontroll med innbyggjarane er ein trussel mot rettstryggleik, fridom og demokrati. Det sentrale i eit demokrati er ikkje at staten skal overvake innbyggjaren, men tvert imot at innbyggjaren skal kontrollere staten. Det er berre på denne måten vi kan forvisse oss om at statsmakta held seg innanfor akseptable rammer.

Vi har vore vane med at ordensmakta set i verk tiltak for å etterforske, tiltale og dømme kriminelle. Ved introduksjonen av datalagringsdirektivet er denne førestillinga snudd 180 grader

rundt. Direktivet føreset at informasjon om bruk av elektroniske kommunikasjonskanalar for alle landets innbyggjarar, ikkje berre for dei som er mistenkte for noko, omhyggeleg skal loggførast. Dette skal gjerast i tilfelle det skulle bli naudsynt å etterforske nokon av oss i etterkant. Direktivet krev ei lagringstid på minst eit halvt år, oppetter avgrensa til to år.

I desse gigantiske databasane vil det gå fram kven du har ringt til, kvar du har ringt frå, når du har ringt og kor lenge, både via fasttelefon og mobiltelefon. Tilsvarande òg kven som har kontakta deg. Direktivet krev lagring av informasjon om når du nytta Internett og med kva adresse. Vidare skal det loggførast kven du har sendt e-post til og motteke e-post frå.

I meldingsåret kom òg Avinors planar om å prøve ut kroppskanning på norske flyplassar. Forslaget føydde seg etter Datatilsynets meining inn i rekkja av stadig meir integritetskrenkjande tiltak. Etter massive protestar bestemte Avinor seg for å leggje prosjektet på is.

I nokre tilfelle tilbyr produsentar av ny teknologi sterkt reduserte prisar for å få sin teknologi inn i prestisjeprosjekt. Med dette oppnår dei å få eit utstillingsvindauge for sitt konsept, og samtidig skape legitimitet for sine løysingar.

Innføringa av mange integritetskrenkjande tiltak er ikkje tufta på tilstrekkelege avvegingar. Fleire ser meir ut som resultatet av ei sterk lyst til å vere innovativ, kopla med ein iver etter å vise handlekraft.

Datatilsynet etterlyser ein tilsvarande iver og handlekraft når det gjeld å evaluere dei integritetskrenkjande tiltaka som allereie er innførte.

9 Nærmare om utvalde saksfelt

9.1 Justissektoren

9.1.1 Tiltak mot kvitvasking og terrorfinansiering

Finansdepartementet sende i meldingsåret eit forslag til revisjon av kvitvaskingslova til høyring (NOU 2007:10). Forslaget skal implementere det tredje kvitvaskingsdirektivet, og er utarbeidd av eit utval som hadde som mandat mellom anna å vurdere korleis «…hensynet til personvern kan ivaretas på en hensiktsmessig måte.» Etter Datatilsynets meining har ikkje utvalet gjennomført dette.

Fem fundamentale spørsmål er etter tilsynets meining usvarte i lovendringsforslaget:

1) Nytteverdien av den eksisterande rapporteringsplikta er ikkje dokumentert

Økokrim har dei siste fem åra motteke heile 22 767 rapportar om mistenkjelege transaksjonar. Talet ser ikkje ut til å minske. Berre eit fåtal av dei innmelde transaksjonane endar med domfelling, men bruken av meldingane ser ut til å vere nyttig for andre aktørar, og for andre føremål. Datatilsynet sin uro er primært retta mot alle dei uskuldige som openbert er innmelde til Økokrim. Utviklinga i forhold til meldeplikta for finansinstitusjonar går i retning av at ein heller rapporterer éin for mykje enn éin for lite, då brot på meldeplikta er straffesanksjonert.

2) Manglande trongsanalyse – treng ein dei foreslåtte endringane?

Utvalet har ikkje dokumentert kva slags kriminalitetstypar som ikkje blir oppklarte ved dei eksisterande reglane. Eitt av forslaga går likevel ut på å gjere terskelen lågare for overtreding av reglane om lovpålagd rapportering til òg å omfatte grov aktløyse. Ei skildring av trusselbiletet og den reelle trongen er heilt naudsynt for at høyringsinstansar og lovgivar skal kunne ta stilling til om tiltaka er naudsynte og forholdsmessige.

3) Kor langt skal samfunnet tillate privat etterforsking?

Heilt nytt i lovforslaget er at rapporteringspliktige skal underleggjast ei plikt til å utføre omfattande kundekontroll. I tillegg er det stilt krav om forsterka kontrolltiltak overfor politisk eksponerte personar og deira krins. Datatilsynet er kritisk til at sivile samfunnsinstitusjonar skal påleggjast ei plikt til å kartleggje sensitive forhold rundt kunden. Forslaget inneber eit endå tettare institusjonalisert samarbeid mellom sivile samfunnsinstitusjonar og politiet. Spørsmålet om kor lange politiets forlengjande armar skal vere fortener ein prinsipiell politisk debatt.

4) Kva konsekvensar har det at viktige rettstryggleiksgarantiar blir oppheva?

Datatilsynet konstaterer at det nye lov- og forskriftsforslaget vil føre til større grad av hemmeleghald overfor den innrapporterte enn tidlegare. I kombinasjon med ei utvida undersøkingsplikt for den rapporteringspliktige, medverkar dette til at det blir vesentleg vanskelegare for kvar enkelt å få vite kva andre veit om han eller henne. Hem-

meleghald er med på å svekkje den grunnleggjande tilliten mellom individ og styresmakter, som igjen er ein grunnleggjande føresetnad for eit velfungerande og vitalt demokrati.

I saker som vedgår kommunikasjonskontroll, har den kontrollerte i ettertid høve til å gjere seg kjent med omfanget av kontrollen. Ein tilsvarande rett bør innrømmast personar som blir innrapporterte ut frå til kvitvaskingslova.

Datatilsynet vil heller ikkje utelukke at ein større grad av openheit når det gjeld innhenting, utlevering, bruk og vidareformidling av opplysningar òg vil kunne ha ein preventiv effekt. Vissa om at nokon «ser ein i korta» kan kanskje verke med til at ein avstår frå vidare kriminell verksemd.

5) Kva rolle skal Kontrollutvalet ha?

Det samla lov- og forskriftsforslaget representerer såpass store innhogg i personvernet at rolla til Kontrollutvalet burde vore drøfta i utgreiinga. Når innsynsmoglegheitene manglar, bør kanskje Kontrollutvalets rapportar, funn og møtereferat, dersom slike eksisterer, vere offentleg tilgjengelege i ei eller anna form.

9.1.2 Datakrim

Datakrimutvalets delrapport II vart send på høyring i meldingsåret. Datatilsynet erkjenner at nye former for kriminalitet krev nye straffeføresegner og nye måtar å etterforske lovbrot på. Tilsynet hadde i si høyringsfråsegn likevel innvendingar, mellom anna at forslaget er språkleg vanskeleg tilgjengeleg.

Beskrivingane av dei straffbare handlingane er svært runde og vide, men blir følgde av omfattande skjønnsmessige avgrensingar. Desse viser gjerne til noko «utanfor seg sjølv», til dømes normer, etikk, retningslinjer osv. Omgrepet «uberettiget» er brukt i nesten alle føresegnene i lovforslaget, og gjer dei vanskelege å tolke. Til dømes: «For uberettiget bruk straffes den som uberettiget nytter andres datasystem eller elektroniske kommunikasjonsnett».

Datatilsynet meiner at skjønnsmessige omgrep må definerast nærare slik at både innbyggjarar og rettsapparat kan ha klare idear om kva ein skal te seg i forhold til. Det kan bli vanskeleg å vite når ein er på rett og gal side av lova. Dei følgjande føresegnene viser til «uberettiget befatning med» diverse verktøy og kodar. Kven klarer, på fornuftig vis, enkelt å forklare kva slag handling som kan utløyse straffeansvar etter føresegnene under?

§ 10 Ulovlig befatning med tilgangsdata

For ulovlig befatning med tilgangsdata straffes den som uberettiget anskaffer, innfører, fremstiller, besitter, markedsfører eller tilgjengeliggjør for andre passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem.

Straffen er bøter eller fengsel i 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

§ 11 Skadelig dataprogram og utstyr

For ulovlig befatning med skadelig dataprogram straffes den som uberettiget anskaffer, fremstiller, modifiserer, besitter, markedsfører eller tilgjengeliggjør dataprogram som er særlig egnet til å begå handlinger som er straffbare etter §§ 4-8, 10 eller 13-14 i dette kapitlet. Lignende befatning med utstyr som er særlig egnet til tilsvarende føremål straffes på samme måte.

Straffen er bøter eller fengsel inntil 1 år. For grov overtredelse er straffen bøter eller fengsel inntil 3 år.

Datatilsynet er uroa for at føresegnene, slik dei er formulerte, kan få eit for vidt nedslagsfelt. Som mindretalet i utvalet peikte på, er det normalt ikkje straffbart å eige eller ha gjenstandar som kan nyttast til kriminelle føremål, til dømes ei øskje fyrstikker eller eit brekkjern. Mindretalets merknad om at dataprogram som har eit skadepotensial og blir brukte til straffbare forhold òg kan nyttast til lovlege og nyttige føremål bør det leggjast vesentleg vekt på.

Datatilsynet er generelt kritisk til å kriminalisere handlingar som ikkje i seg sjølve krenkjer noka verneverdig interesse. Føresegnene inneber ei uheldig dreiing mot auka subjektivisering av strafferetten, noko som igjen kan leie til eit auka kontrollnivå i samfunnet.

Bruk av fiktiv identitet

Bruk av fiktiv identitet er noko barn og unge blir oppfordra til av fleire samfunnsinstitusjonar, òg av Datatilsynet. Sjå til dømes nettstaden www.dubestemmer.no. Tanken bak denne oppfordringa er at barn og unge betre skal kunne verne seg mot uønskte og straffbare handlingar. Lovforslaget vil kunne verke med til vesentleg utryggleik knytt til bruk av pseudonym eller kallenamn.

Datatilsynet er klar over at det kan førekomme krenkjande handlingar ved bruk av uriktig identitet. Likevel er bruken av uriktig identitet utbreidd, og

bør i mange samanhengar reknast som legitim. Å gi opp uriktig identitet kan eventuelt vurderast som straffeskjerpande i kombinasjon med anna kriminell handling, men bør ikkje vere ei ulovleg og straffbar handling i seg sjølv.

Filtrering

Eit mindretal foreslo at tenesteytarar skal kunne påleggjast å blokkere tilgangen til særskilde stader på Internett for sine brukarar dersom innhaldet vil kunne medføre straffeansvar i Noreg. Datatilsynet støttar ikkje forslaget. Spørsmål om filtrering er eit svært ømtolig tema som eventuelt først må bli gjenstand for ein brei konsekvensanalyse. – Kven skal avgjere kva som skal blokkerast? spurde Datatilsynet i høyringsfråsegna, og peikte på at det vil vere høgst ulike meiningar om slike spørsmål i eit demokrati.

9.1.3 Skal pressa og forskarar kunne følgje politiet under arbeid?

Justisdepartementet sende ut eit forslag om at andre enn dei som gjer teneste eller arbeid for politiet skal kunne få løyve til å følgje og observere politiets tenesteutøving på privat og offentleg stad. To samfunnsaktørar vart vurderte spesielt, nemleg forskarar og pressemedarbeidarar.

Desse to samfunnsaktørane er vidt forskjellige både med omsyn til kva interesser dei representerer og kva rettsleg regulering dei er underlagde. Datatilsynet støttar ikkje forslaget om å tillate pressemedarbeidarar å følgje og observere politiets tenesteutøving på privat stad.

Pressa er ikkje underlagd alle dei avgrensingar i forhold til teieplikt og andre føresegner som skal ivareta personvernet for kvar enkelt. Heller ikkje personopplysningslova vil komme til bruk dersom pressa handsamar opplysningane i strid med føremålet, då lova, i det vesentlegaste, ikkje gjeld handsaming av personopplysningar for journalistiske føremål.

Stor og uoppretteleg skade vil kunne skje dersom pressa publiserer personopplysningar som resultat av observasjon av politiets tenesteutøving. Ein «smekk på fingrane» frå PFU i ettertid vil ikkje kunne reparere ein slik skade, da skaden skjer i og med publiseringa.

Verken journalist eller pressemedarbeidar er ein verna tittel. Dette vil i praksis kunne skape problem med å avgrense kva for aktørar som skal kunne få løyve.

Eit løyve til at forskarar skal kunne følgje og observere politiets tenesteutøving er mindre problematisk.

9.1.4 Tilsyn i fengselsvesenet – Ila fengsel

Datatilsynet retta skarp kritikk mot Justis- og politidepartementet, etter å ha gjennomført ein kontroll med den handsaming av sensitive personopplysningar som skjer i fengselsvesenet. Dei alvorlege lovbrota som er avdekte viser at personvernet til meir enn 30 000 tidlegare innsette og deira pårørande ikkje er ivareteke.

Datatilsynet har over fleire år motteke klager frå innsette ved fengsla her i landet, knytte til handsaming av personopplysningar i fengsla. Særleg har det vore klaga på at opplysningane om fangane og deira pårørande ikkje er tilstrekkeleg verna. Datatilsynet sende spørsmål om handteringa av opplysningane til Justis- og politidepartementets kriminalomsorgsavdeling. Under korrespondansen kom det fram opplysningar som etter tilsynets vurdering gav grunnlag for å foreta ein nærmare kontroll. Datatilsynet drog på tilsyn til Ila fengsel hausten 2007.

Datatilsynet konkluderte med at det finst eit uoffisielt og ukontrollert personregister ved Ila («innsatt per nummer»). Registeret inneheld svært sensitive personopplysningar. I tillegg manglar bruken av personopplysningar i fagsystemet Kompis eit rettsleg grunnlag.

Dei registrerte sine grunnleggjande rettar etter personopplysningslova, med omsyn til innsyn, retting og sletting, blir ikkje ivaretekne.

I tillegg påpeikte Datatilsynet at Kriminalomsorgsavdelinga ikkje har etablert eit internkontrollsystem for å sikre at handsaminga av personopplysningar skjer i samsvar med lovgivinga, ikkje har gjort relevante risikovurderingar av handsaminga, eller sytt for tilfredsstillande informasjonstryggleik, særleg med tanke på konfidensialitet.

Datatilsynet meiner òg at Justisdepartementets kriminalomsorgsavdeling har gitt tilsynet mangelfull og feilaktig informasjon på vesentlege punkt.

Har ein innsett rett til eit personvern?

Ved første augekast er det ikkje innlysande at ein som sit i fengsel har rett til eit personvern. Heile føremålet med fengselsopphaldet er jo nettopp fridomsrøving, gjennom ein kontinuerleg personkontroll. Den som sit fengsla har då heller ikkje eit tra-

disjonelt privatliv. Avhengig av dei konkrete soningsvilkåra vil privatlivet vere kraftig avgrensa, med mellom anna ransaking av celle og kontroll av postsendingar.

Personvern er ein menneskerett. Den er nedfelt i den europeiske menneskerettskonvensjon (EMK) artikkel 8, som Noreg har forplikta seg til å etterleve. Òg Grunnlova har føresegner som inneber at innbyggjarane har ein grunnleggjande rett til personvern. EMK gir staten på visse vilkår høve til å straffe enkeltmenneske, gjennom å ta frå dei individuelle fridomar. Desse kan likevel ikkje setjast til side i større grad enn naudsynt for å gjennomføre soninga. Fangar har altså rett til personvern, irekna respekt for den eventuelle rest som er att av eit privatliv i fengslet.

Særleg viktig er det at opplysningar om at ein person sit eller har sete i fengsel, og dei nærmare omstenda rundt dette, blir handsama konfidensielt. Det er heilt naudsynt for mellom anna å sikre at den innsette har reelle sjansar til å bli ført tilbake til samfunnet. Og nettopp det å gjere den innsette i stand til å føre eit fullverdig liv utanfor murane er jo eitt av hovudføremåla med straffa.

Vidare er det viktig at dei personane som opplysningane gjeld (medrekna pårørande), får tilstrekkeleg informasjon til å kunne ivareta dei andre rettane sine, mellom anna rett til innsyn i opplysningane.

9.1.5 Overføring av passasjeropplysningar til USA

Etter terrorangrepa i 2001 har styresmaktene i USA kravd ei rekkje opplysningar om flypassasjerar som kjem inn i amerikansk luftrom. I meldingsåret vart ein ny avtale om overføring av passasjerdata underteikna av EU og USA. Kravet om personopplysningar omfattar passasjeranes namn, kontaktopplysningar, reiserute, reiseføLgje og eventuell diett, og ei rad andre opplysningar.

Den nye avtalen mellom USA og EU om overføring av flypassasjerdata gir vesentleg svekt personvern, uttalte Artikkel 29-gruppa, eit offisielt rådgivande personvernorgan i EU, då dei behandla avtalen.

Avtala legg opp til at ei enno større mengd opplysningar skal kunne overførast. Føremål, sikring og personverngarantiar i avtalen er ikkje presist formulert, og opnar for mange unntak. Lagringstida er auka til minst 15 år. Det er mellom anna ikkje lenger noko krav til tryggleiksnivået ved vidare overføring frå Department of Home Security (DHS) til andre kontor innan USA eller i utlandet.

Overgangen frå ein tilstand der USA forsyner seg sjølv i reiseselskapa sine register, til ein tilstand der reiseselskapa sender opplysningane på førespurnad, er uavklart på fleire punkt, påpeikte Artikkel 29-gruppa vidare. Mellom anna er det ikkje openbert korleis DHS, som i unntakstilfelle skal få høve til å hente ut andre opplysningar av registeret enn dei som er ramsa opp i avtalen, skal kunne få tak i desse opplysningane når dei ikkje lenger får forsyne seg sjølve hos reiseselskapa.

Artikkel 29-gruppa reagerte òg på at ingen uavhengige tilsynsmyndigheiter er tiltenkt rolla som kontrollør.

Artikkel 29-gruppa bad Kommisjonen klargjere fleire punkt, mellom anna:

- Kva flyselskap er omfatta av avtalen?
- Når kan dataa bli brukte til andre føremål enn hovudreglane i avtalen tilseier?
- Korleis skal opplysningane kunne hentast ut etter unntaksregelen, utan å gjeninnføre prinsippet om at amerikanske styresmakter forsyner seg sjølve i flyselskapa sine databasar?
- Kva for 13 flyselskap overfører data i dag, og kva krav må dei oppfylle?
- Når vil tilsyn finne stad?

I tillegg ønskte gruppa forsikringar om at tidsfristen for opphøyr av «sjølvforsyning», 1. januar 2008, ikkje blir skove på fleire gonger.

Noreg er ikkje omfatta

Noreg er ikkje omfatta av den nye avtalen når denne årsmeldinga blir levert til Fornyings- og administrasjonsdepartementet. For at eit flyselskap lovleg skal kunne utlevere passasjerinformasjonen frå Noreg, må det innhente samtykke frå passasjeren, eller søkje Datatilsynet om dispensasjon frå forbodet mot å utlevere personopplysningar til statar som ikkje sikrar eit tilstrekkeleg sikringsnivå. Justisdepartementet og Utanriksdepartementet arbeider med å få til ein avtale mellom USA og Noreg.

Datatilsynet legg stor vekt på at passasjerane får informasjon før billettkjøpet, slik at han eller ho veit kva føresetnader som ligg til grunn for reisa.

9.2 Datalagringsdirektivet

I 2007 har Samferdselsdepartementet førebudd høyringa for implementeringa av datalagringsdi-

rektivet i Noreg. Direktivet vart vedteke i EU i 2006, og skal implementerast i EU-landa seinast innan starten av 2009. Noreg har ikkje hatt moglegheit til å påverke innhaldet.

Datatilsynet har vore oppteke av å få fram at direktivet er eit heilt nytt verktøy for styresmaktene si overvaking av innbyggjaranes elektroniske kommunikasjon. I årsmeldinga for i fjor påpeikte Datatilsynet at innføringa av datalagringsdirektivet er eit paradigmeskifte i det norske rettssystemet. Med dette direktivet innfører ein eit etterforskingsmiddel som omfattar heile innbyggjarane. Det er eit breiddtiltak, ikkje målretta mot enkeltpersonar eller grupper av personar det heftar ein mistanke ved.

Hittil har det vore naudsynt å ha eit klårt grunnlag for å lagre trafikkdata om innbyggjarane sin kommunikasjon. Teleoperatørane har lagra trafikkdata for å kunne fakturere kundar i ettertid. Dei kommunikasjonsmetodane som ikkje er baserte på fakturering av forbruk, har det ikkje blitt lagra trafikkdata for. Direktivet krev at trafikkdata for fasttelefon, mobiltelefon, breibandstelefoni, e-post og internettilgang, skal lagrast. For enkelte tenester innan telefoni har det i Noreg vore lagra trafikkdata i tre til fem månader. For e-post og internettilgang har det ikkje vore vanleg å lagre trafikkdata.

Direktivet krev lagring i frå seks månader til to år. Mange europeiske land legg seg på eitt års lagring. Det er ymta om at Tyskland vil velje kortast mogleg lagring, seks månader.

Lagringa er detaljert. Når det til dømes gjeld e-post, der det ikkje er blitt gjort trafikkdatalagring tidlegare, skal det no lagrast kven du sender e-post til og kven du mottek e-post frå. Vidare skal det lagrast tidspunkt for e-postforsendinga og kva IP-adresse du nyttar. Når det gjeld mobiltelefon, vil lokaliseringsopplysningar bli lagra, i motsetning til før.

Direktivet krev ikkje lagring av innhaldet i meldingane. Datatilsynet spør likevel om ein, når ein legg opp til ei så radikal omlegging av tidlegare prinsipp, vil stoppe med dette.

Ei rekkje fagfolk har påpeikt at det er uklårt korleis ein skal forstå direktivet. Er det berre politiet som skal få tilgang, eller skal andre, som tollvesenet, skattevesenet eller liknande etatar òg få tilgang? Direktivet legg opp til at kvart enkelt land sjølv må avklare ei rekkje parameter. Det har vore mykje diskusjon rundt kva som skjer dersom nokre land vel seks månaders lagringstid, mens andre vel to år.

Datatilsynet er uroa for at alt det som er uklårt rundt direktivet vil føre til ei ukontrollert overvaking av den einskilde.

9.3 Telefoni

9.3.1 Omfattande lekkasjar frå teleselskapa – politimelding

Nettstadene til fleire teleselskap vart nytta til innhausting av personopplysningar i perioden 28. juli til ca. 7. august 2007. Datatilsynet hadde i lang tid frykta slike hendingar på grunn av måten fleire kundesider var konstruerte på. Tilsynet var òg kritisk til at fleire aktørar berre kravde å få oppgitt fødselsnummer når dei skulle identifisere personar ved etablering av eit nytt kundeforhold. Datatilsynet tok opp spørsmålet med fleire av aktørane første gong hausten 2006, utan å møte stor forståing for tematikken.

Datatilsynet kontrollerte ei rekkje verksemder, mens andre mottok brev frå tilsynet med oppfordring om å sørgje for at deira system ikkje hadde denne veikskapen.

Innhaustinga av personopplysningar starta med ei liste fødselsnummer laga av eit dataprogram. Desse vart seinare sjekka mot ei offentleg nettside for å luke ut nummer som ikkje er i bruk. Fødselsnumra vart vidare nytta til å søkje fram namn og adresse på enkeltpersonar via teleoperatøranes nettsider. Få av personane som vart ramma hadde noko med verksemdene å gjere, og svært mange vart opprørde og overraska over at dette ramma nettopp dei.

Datatilsynet var kritisk til følgjande punkt:

1. Teleselskapa sine nettstader tillet kven som helst å tinge abonnement berre ved å gi opp fødselsnummeret til eit individ. Verksemda sikra ikkje at kommunikasjon skjedde med rette vedkommande.
2. Nettsida føydde til namn, adresse og om innehavaren av fødselsnummer var kredittverdig eller ikkje. Dermed gav selskapa innsyn i personopplysningar utan at dei på rimeleg vis hadde forvissa seg om at dette skjedde til rette vedkommande. I realiteten brukte dei fødselsnummeret som eit slags «legitimasjonsbevis».
3. At verksemdene ikkje på sjølvstendig initiativ sikra informasjon forsvarleg.
4. Fleire av verksemdene oppfylte ikkje meldeplikta til tilsynet etter personopplysningsforskrifta § 2-6, men først gav underretning etter krav frå tilsynsmyndigheita.
5. Fleire av verksemdene tok seg ikkje bryet med å varsle dei som vart offer for dette.

Datatilsynet meiner at dei klårt alvorlegaste krenkingane ligg i mangelfull sikring av informasjon, respons med tilleggsinformasjon og at fleire verksemder ikkje tok seg bryet med å varsle offera for hendinga. Manglande varsling av dei det gjaldt vitnar om ein manglande respekt for personvernet til den enkelte.

Ikkje alle dei ovannemnde regelverksbrota er straffesanksjonerte. Datatilsynet valde å politimelde brot på personopplysningslova § 13 om informasjonstryggleik, og personopplysningsforskrifta § 2-6 om varslingsplikt overfor tilsynet. Det var berre verksemda Talkmore AS som oppfylte begge kriteria, og som dermed vart meld til politiet.

I vurderingane som vart gjorde, avdekte Datatilsynet veikskapar i regelverket. Terskelen for straffereaksjonar i høve til denne typen saker er høg. Bruk av overtredingsgebyr hadde truleg vore langt meir eigna enn melding til politiet. Men etter gjeldande lovverk har ikkje Datatilsynet slike verkemiddel.

9.3.2 Tilsyn hos to teleoperatørar

Datatilsynet vitja to teleoperatørar hausten 2007. Begge dei kontrollerte verksemdene hadde ei utilfredstillande sikring av trafikkdata for kundane. For mange tilsette hadde tilgang til denne type data, og kontrollmekanismar, som til dømes bruk av loggar, var fråverande. Eit anna fellestrekk var brot på sletteplikta etter personopplysningslova § 28.

Handsaminga av personopplysningar i telebransjen er konsesjonspliktig. Ei av verksemdene hadde ikkje konsesjon frå tilsynet. Den andre verksemda hadde konsesjon, men braut konsesjonsvilkåra på det aktuelle tidspunktet, ved at lagringstida overskreid den maksimale lagringstida med god margin. Begge braut informasjonsplikta, og fekk merknader for ein ikkje tilfredsstillande internkontroll.

Det gjennomførte tilsynet styrkte Datatilsynet si uro i forhold til ei eventuell innføring av datalagringsdirektivet. Teleoperatørane ser ikkje ut til å ha utvikla ei forståing av at trafikkdataa dei handterer er særleg sikringsverdige. Dette meiner tilsynet å kunne slå fast basert på synspunkta verksemdene gav under kontrollen, funna som vart gjorde og tidsrommet brota openbert har gått føre seg i.

9.3.3 Pliktig registrering av telefonbrukarar, ikkje berre av abonnentane

Samferdselsdepartementet har i løpet av året 2007 lagt fram eit forskriftsforslag om at ikkje berre mobilabonnentane skal registrerast, men òg den som faktisk bruker mobilen. Abonnent og brukar er ikkje naudsyntvis same person. Noreg har allereie gått vesentleg lenger enn andre europeiske land. Anonyme abonnement på mobiltelefonar kan ikkje lenger opprettast i Noreg. I Sverige kan ein framleis vere anonym.

Det verkar som at hovudargumentet for å innføre registreringa av identitet er å fange opp brukarar under 18 år. Dei mindreårige skal dermed kunne vernast frå å få reklame, eller andre førespurnader som ikkje eigner seg for dei.

Datatilsynet meiner det ikkje er naudsynt å gjere ei full registrering av brukarane av mobilar for å forhindre dette. Det er i tillegg openbert at òg mange personar *over* 18 år helst vil sleppe denne typen førespurnader.

Datatilsynet er spesielt uroa over pliktig registrering av brukarar under 18 år. Mange foreldre vel å la mobiltelefonane stå i eige namn, nettopp for å verne barna. Det som er tenkt å verne barna mot uønskt reklame kan gjere dei sårbare for førespurnader frå personar som ikkje vil dei vel. Registreringa av brukaren har i fleire tilfeller ført til at barn, utan at dei føresette veit om det, er blitt oppførte med fullt namn og mobilnummer på nummeropplysningstenester. Tryggleiken for barnet har dermed ikkje blitt betra.

9.4 Internett

9.4.1 Tilsyn: Det offentlege sine nettstader

Datatilsynet førte tilsyn med eit avgrensa tal nettstader innan offentleg sektor. Sektoren ønskjer å leggje til rette for at nettstadene blir meir tilgjengelege og får auka interaksjon med publikum. Dermed har det mellom anna blitt lagt opp til innsending av elektroniske skjema.

Slik bruk av Internett krev god tryggleikskultur og ryddig handtering av brukaranes rettar til m.a. føremålsmessig lagring, sletting, informasjon og innsyn. Datatilsynet vurderte heimesidene til verksemdene, og avdekte fleire, omfattande og systematiske manglar når det gjaldt informasjon til den enkelte, tryggleik og forsvarlege rutinar.

Det kom i løpet av tilsyna fram at svært mange kommunar nyttar ein ekstern leverandør til å ta i mot søknader. Det var ikkje laga tilfredsstillande avtalar for dette. Den eksterne leverandøren lagra kopier av alt som vart innsendt via tenesta. Tilsette hos den eksterne leverandøren hadde full tilgang til å lese søknader som var sende til rundt 160 norske kommunar over ein periode på meir enn eitt år.

Datatilsynet er uroa for at svært mange offentlege aktørar har lågt medvit rundt personvernspørsmål og dårleg informasjonstryggleik i tilknyting til nettstadene sine.

9.4.2 Ny offentleglov

Forslaget til forskrift til den nye offentleglova pålegg ei rekkje organ og etatar å gjere den elektroniske postjournalen tilgjengeleg på Internett.

Dette medfører trong for klåre reglar om kva som kan publiserast og kontrollrutinar for å forhindre menneskelege feil og systemsvikt.

Datatilsynet peiker spesielt på fire behov:

1. Skjerming av fleire opplysningstypar, som trivielle personopplysningar, fødselsnummer og elevlister.
2. Avgrensingar med omsyn til kva søk ein kan gjere.
3. Avgrensingar i høvet til å hauste journalar og dokumenter i store mengder.
4. Sanksjonsmoglegheiter.

Om det offentlege publiserer store mengder trivielle opplysningar om den enkelte, vil det føre med seg ein fare for misbruk. Masseinnhausting av personopplysningar kan gi omfattande profilar av kvar enkelt. Desse kan mellom anna bli tekne i bruk til marknadsføring, men òg vere nyttige for ID-tjuveri. Den som ønskjer å stele ein identitet kan skaffe seg ei tilnærma fullstendig oversikt over eit enkelt individ sine handlingar og preferansar. Dermed kan det òg bli vanskelegare å avsløre ein person som står fram med falsk identitet. Svara på spørsmål som tidlegare var eigna til å skilje rett person frå falsk, vil kunne liggje tilgjengeleg på Internett.

Datatilsynet har sett ei rekkje døme på at kommunar har publisert personopplysningar som ikkje skulle ha vore tilgjengelege på Internett. Nokre av dokumenta har innehalde opplysningar om fødselsnummer, andre er frå enkeltmenneske i krise som har søkt hjelp frå kommunen, andre har vore fullstendige jobbsøknader med skanna attestar og vitnemål. Når gleppen er eit faktum, kan konsekvensane vere store for den det gjeld.

Etatar og kommunar som opplever at personopplysningar som det er teieplikt om blir publiserte, grunngir gjerne hendinga med at det har skjedd ein menneskeleg feil. Datatilsynet meiner for sin del at gjentekne «gleppar» tyder på systemsvikt hos verksemda. Det kan vere at det finst for dårlege rutinar for gjennomgang av dokument før publisering, eventuelt i kombinasjon med at rutinane ikkje blir følgde. Rutinar og praksis er eit leiaransvar, og det er for enkelt når offentlege organ støtt og stadig skyv sine tilsette framfor seg og viser til deira menneskelege feil. Datatilsynet ber derfor i høyringsfråsegna om at ein gjer det mogleg å sanksjonere brot på føresegnene.

Vern mot eksponering via søkjemotorar

Ikkje alle offentlege instansar vernar personopplysningane i internett-publiserte dokument mot direktesøk gjennom søkjemotorar. Eit vern inneber at ein først må klikke seg fram til det aktuelle forvaltningsområdet, og så søkje derfrå. Mange av sakene som blir behandla i offentleg sektor gjeld enkeltpersonar. Saksinformasjon som gjeld ein privatperson kan dermed lett komme til å dukke opp når ein søkjer på Internett, kanskje med heilt andre søkekriterium, og heilt andre mål for søkinga. Det er ikkje målet med offentleglova at personopplysningar skal pådyttast den som ikkje ønskjer informasjonen.

9.4.3 Tilsyn: Postlister på nettet

I mai 2007 vart det gjennomført ein kontroll hos Ålesund kommune. Bakgrunnen var at Datatilsynet gjennom media vart gjort kjent med eit tryggleiksbrot. Via søk i søkjemotoren Google på Internett var det mogleg å finne fram til personar som hadde klaga til Klagenemnda for sosialsaker i 2005.

Kommunens utlegging av sensitive personopplysningar skuldast fleire uheldige omstende. Ei avgrensa mengd opplysningar om klagesaker vart ført på eit lågare tryggleiksnivå enn desse normalt blir handsama på i kommunen. Denne praksisen vart etter hendinga avslutta.

Informasjonen var ikkje tilgjengeleg direkte frå kommunen sine heimesider. Filene vart likevel fanga opp av søkjemotorar, og dei som søkte på namn eller andre tilgjengelege ord i dei store søkjemotorane, fekk dermed tilgang.

Datatilsynet påla kommunen å etablere eit hinder slik at ikkje postjournalar og dokument systematisk kan søkjast fram utanfrå, via eksterne søkjemotorar.

9.4.4 Datatilsynets råd til regjeringa om e-forvaltning

Frå byrjinga av 90-talet tok det offentlege for alvor til å bli interessert i elektronisk samhandling. Ein så ei moglegheit for å utvikle nye, demokratiske kanalar og skape betre føresetnader for teneste-

yting frå offentleg sektor. Visjonane var at innbyggjaren i stor grad kunne sitje i si eiga stove, der han enkelt kunne sende inn informasjon og ta imot relevante tenester frå det offentlege ved hjelp av nokre tastetrykk. Dei siste åra har løysingane for samhandling byrja å komme.

I eit brev til Fornyings- og administrasjonsdepartementet trekkjer Datatilsynet fram fleire punkt tilsynet meiner forvaltninga må vere spesielt merksam på ved vidare utbygging av slike tenester:

Datatilsynet sine råd kan oppsummerast slik:

– Ikkje bruk fødselsnummer på offentlege portalar,
– vis varsemd med å knyte sak og person saman ved publisering av saksdokument på Internett, og
– stimuler til auka bruk av e-ID og e-signatur.

Fødselsnummeret er ein eintydig identifikator, kvar person får eitt, og same nummer blir ikkje delt ut til fleire enn denne eine. Styrken i nummeret ligger i at det kan brukast til å skilje personar frå kvarandre, til dømes i ein database, slik at nye opplysningar kan registrerast i tilknyting til rett person. Men ein utstrekt bruk av fødselsnummer på Internett vil kunne utgjere ein fare for at personopplysningar kjem på avvegar. Ein slik lekkasje fann stad i meldingsåret, dette kan ein lese meir om i avsnittet *Datainnhausting er blitt enklare*.

Mengda personopplysningar som blir publiserte i portalar og på offentlege nettstader kan over tid bli så omfattande og lett tilgjengeleg at profilar på enkeltindivid kan få kommersiell verdi. Det er viktig å peike på at òg verksemder utanfor EØS-området kan hauste store mengder personinformasjon mot viljen til den enkelte. Då er det ikkje mogleg verken for Datatilsynet eller andre europeiske myndigheiter å handheve rettane i personopplysningslova eller EU-direktivet.

Datatilsynet tek vidare til orde for at regjeringa aktivt skal fremje sikker og trygg samhandling på nettet ved å stimulere til auka bruk av e-ID og e-signatur. Mangelen på slike instrument inneber at det er vanskeleg å vite kven ein samhandlar med på nettet. Datatilsynet har teke dette spørsmålet opp med skiftande regjeringar. Saka ser likevel ikkje ut til å vere mindre aktuell idet vi går inn i 2008.

9.4.5 Skattelister på Internett

Som følgje av lovendringa Stortinget vedtok våren 2007, kan pressa tinge skattelistene for 2006 elektronisk. Tenesta er open for aviser, magasin og vekepresse i alle medium. Listene inneheld følgjande opplysningar om skattebetalarane; namn, fødselsår, poststad og postnummer, skattekommune, nettoinntekt, nettoformue og utlikna skatt.

Skattedirektoratet understrekar at dei som mottek listene er ansvarlege for at handsaminga av desse skjer i samsvar med krava i personopplysningslova. Datatilsynet vil i den samanheng poengtere at journalistisk verksemd i hovudsak er unnateke frå føresegnene i personopplysningslova. Det er opp til kvar enkelt redaktør å definere om eigen bruk av opplysningane frå skattelistene fell inn under kategorien journalistisk verksemd. Datatilsynet har ingen intensjon om å avgjere kva slags bruk av skattelistene som kan seiast å ha ein journalistisk verdi. Det ville i så fall vere ei rolle tilsynet meiner er svært problematisk i forhold til viktige grunnprinsipp om ei fri, norsk presse.

Då lovendringa vart handsama, gav Datatilsynet uttrykk for at endringa er uheldig for personvernet. Tilsynet meiner det strir mot sentrale personvernprinsipp at opplysningar kvar enkelt norsk borgar er pliktig til å levere inn, skal kunne brukast til underhaldning, gjerast søkbar eller tilbydast for sal i form av SMS-tenester eller liknande. Det er òg urovekkjande at offentleggjeringa av skattelistene skjer før fristen for å klage på likninga har gått ut.

Regjeringas grunngiving for å gjeninnføre pressas innsyn i skattelistene var mellom anna eit ønskje om å styrkje den kritiske debatten rundt skattesystemet. Datatilsynet spør om ein, ved langtidspublisering av skattelisteopplysningar, ikkje i staden oppnår ei stigmatisering av låglønnsgrupper og deira familiar. I tillegg ser Datatilsynet at faren for ID-tjuveri aukar for norske skatteytarar når informasjon om dei finansielle forholda til kvar enkelt ligg så lett tilgjengeleg på Internett.

9.4.6 Fosterforeldre på Internett

Belastande opplysningar om fosterforeldre vart publiserte på ei særskilt internettside. Nettsida inneheldt mellom anna kommentarar og slengmerknader om namngitte fosterforeldre sin oppførsel, framferd og utsjånad. Tilsynet forstod fortvilinga til fosterforeldra, men vurderte det slik at opplysningane måtte sjåast på som opinionsdannande, og dermed verna av ytringsfridomen. Datatilsynet streka under at det er ein forskjell mellom profesjonelle aktørar, som må forventast å tole meir omtale, og privatpersonar som har opna sin private heim for å ta imot barnevernsbarn.

Tidlegare har Personvernnemnda handsama spørsmål om det er lovleg å publisere opplysningar om profesjonelle aktørar i barnevernssaker på dei same sidene. Dette gjeld mellom anna psykologar, barnevernstilsette, politikarar, advokatar og journalistar. Den gongen fall nemnda ned på at bruken av opplysningane var eit ledd i opinionsdannande verksemd. Når bruken av personopplysningane har eit utelukkande journalistisk eller opinionsdannande føremål, gjeld personopplysningslova berre i avgrensa grad. Det betyr mellom anna at ein ikkje treng samtykke for å publisere opplysningar om enkeltpersonar.

Norsk Fosterhjemsforening klaga på Datatilsynets avgjerd, og peikte mellom anna på at opplysningane er svært sensitive, ofte feilaktige, og at publiseringa er ei stor belastning for fosterforeldra.

Personvernnemnda tok stilling til Internettsida slik den var på klagetidspunktet. Nemnda er einig med Datatilsynet i at føremålet med bruken av opplysningar om fosterforeldra må sjåast på som opinionsdannande. Forskjellen mellom dei profesjonelle gruppene og fosterforeldra er etter nemnda si meining ikkje så stor at vurderinga bør bli ei anna. Nemnda opprettheldt Datatilsynet sitt vedtak.

9.4.7 Tilsyn: Nettenester retta mot barn og unge

Datatilsynet var på tilsyn hos totalt fem nettenester med barn og unge som målgruppe. Føremåla til nettsidene femner vidt, frå reine hjelpetiltak til å tilby kommersielle tenester. Nettenestene rettar seg mot fleire grupper, frå små barn til ungdom og vaksne personar.

Nettenestene hadde til dels store manglar når det gjaldt internkontroll. I to nettsamfunn var kommunikasjonsinnhaldet tilgjengeleg for den ansvarlege verksemda. Dette ser Datatilsynet som klårt integritetskrenkjande. Medlemmen vil oppfatte det slik at det han skriv og seier ikkje er tilgjengeleg for andre enn samtaleparten. I den «analoge» verda er andres tilgang til kommunikasjonsinnhald mellom to samtalepartar strengt regulert. Den same konfidensialiteten må gjelde når ein kommuniserer i ei virtuell verd. Det let til at nokre nettenester oppfattar det som legitimt å lagre kommunikasjonsinnhald for eventuell framtidig bruk av myndigheitene. Dette er i så fall ei svært urovekkjande utvikling.

For tenestene med ideelt føremål, hjelp til unge, avdekte kontrollen mangelfull tryggleik i kommunikasjonen. Dette er alvorleg, fordi tenesta legg opp til at det blir kommunisert sensitive og til dels svært personlege opplysningar.

Manglande overhalding av meldeplikt og informasjonsplikt var òg eit tema i fleire rapportar. Når nettenestene til dels informerer dårleg, har mangelfull tryggleik og dårleg passordvern, ligg det til rette for at opplysningar om barn og unge kjem på avvegar, eller lettare kan misbrukast.

9.4.8 Når Internett blir ei felle for barn

Faremo-rapporten, «Forebygging av internettrelaterte overgrep mot barn», vart lagt fram for Justisdepartementet i januar i meldingsåret. Datatilsynet foreslår i si høyringsfråsegn at Kripos bør få eit ansvar for å hjelpe barn og unge med å fjerne bilete og filmar av seg sjølve frå Internett.

Dagens barn og ungdommar har flytta mykje av kommunikasjonen og uttestingsarenaene over til Internett. Dei bruker webkamera i samtalar dei oppfattar som private. Dei utvekslar film-snuttar og bilete med mobiltelefonane. Dei chattar og lagar heimesider. Barn kan, under si naturlege uttesting, stå i fare for å produsere noko som samfunnet etterpå vil sjå på som barneporno.

Når det gjeld bilete som kan karakteriserast som barnepornografi, risikerer ungdommen, eller hjelparane deira, straffeforfølging dersom dei prøver å søkje fram bileta for å få dei fjerna. Politiet er den einaste instansen som har lov til å søkje.

Det viktigaste for offera vil ofte vere å avgrense spreiinga av materialet. Dei utsette barna treng at nokon får eit definert ansvar for å få filmane og bileta fjerna, så fort som mogleg. Det er ein av måtane ein kan avgrense skaden på.

I meldingsåret vart Datatilsynet kontakta i samband med ei konkret sak der ei mindreårig jente vart teken bilete av, og bileta seinare vart publiserte på nett. Bileta ville kunne bli tolka som barneporno. Dette sette jenta i ein umogleg situasjon. Ho kunne ikkje søkje fram bileta for å få kravd dei sletta, fordi det er straffbart å søkje etter barneporno. Ho måtte derimot leve med kunnskapen om at bileta var der, og at dei igjen kunne gjere det vanskeleg for henne, utan at ho kunne gjere noko med saka. Saka fekk store konsekvensar. Jenta måtte byte namn, familien flytta, og ho byrja på ny skole.

9.4.9 Tilsyn: Nettsamfunn for vaksne

Datatilsynet vitja to nettsamfunn for vaksne hausten 2007. I tillegg vart det gjennomført brevlege/nettbaserte kontrollar mot ytterlegare seks nettsamfunn. Tidlegare tilsyn har avdekt uklåre forhold når det gjeld korleis tilgang til system og

applikasjonar skal fastsetjast. Vidare er det i ei rekkje tilsyn påpeikt at ansvarleg for handsaminga av personopplysningar i liten grad sjekkar relevante loggar. Dette skaper ein situasjon der ansvarleg for handsaminga av personopplysningar i avgrensa grad har kontroll med kven som skaffar seg tilgang til personopplysningar.

Nettsamfunn er «eit rom for å kommunisere». Føremålet med tenesta er å leggje til rette for at brukarane etter eige ønske kan samhandle om det dei sjølve er opptekne av. Verksemda tilbyr i utgangspunktet ei kommunikasjonsplattform og legg avgrensa føring på korleis denne skal brukast. Utover det er det medlemen sjølv som avgjer innhaldet i kommunikasjonen.

Nettsamfunna har såkalla moderatorar som har ei slags myndigheit i nettsamfunnet. Hos eit av nettsamfunna var moderatorane tilsette i verksemda som dreiv nettsamfunnet, mens hos den andre var det frivillige medlemer av nettsamfunnet. Det var rundt 20 moderatorar hos begge nettsamfunn. Medlemstalet var høvesvis rundt 250 000 og 550 000.

Datatilsynet meinte at verksemdene ikkje gav tilstrekkeleg informasjon til medlemene. Mellom anna mangla utfyllande informasjon om føremålet med handsamingane, opplysningar om i kva situasjon utlevering kan bli aktuelt, verksemdas praksis med omsyn til sletting, prosedyre ved endring av vilkår som rører ved personvernet mv.

Begge nettsamfunn hadde mangelfull sletting av personopplysningar. Tilsynet påpeikte spesielt manglande sletting av klagar på andre medlemmer. I desse klagane kunne det komme fram relativt støytande skuldingar. Tilsynet påpeikte at når desse sakene vart sjekka ut, måtte informasjonen anonymiserast eller slettast.

Begge nettsamfunna fekk påtale for mangelfull sikring av personopplysningane. Påtalane gjaldt utilfredstillande vern av administrasjonstilgangar, uklåre ansvarsforhold, mangelfull datahandsamaravtale, manglande tilgangskontroll og mangelfull logging.

9.5 Identifikasjon og legitimasjon

9.5.1 Ikkje mindre kontroll med folkeregisteret

Skattedirektoratet sende i meldingsåret ut eit forslag til ny folkeregisterforskrift på høyring. Forslaget inneber svekt kontroll og oppfølging av tilgangen til personopplysningane i folkeregisteret. Folkeregisteret skulle etter forslaget ikkje lenger ha ei lovmessig plikt til å halde oversikt over kven som har tilgang til kva opplysningar, vilkåra for tilgangen, eller kontroll med at desse vilkåra blir overhaldne.

Tal frå Skattedirektoratets eigne heimesider viser at i alt 1500 verksemder hadde tilgang til databasen i folkeregisteret i 2005. Kvart år blir det gjort omtrent 30 millionar oppslag i denne databasen. Datatilsynet påpeikte trongen for ei innskjerping snarare enn ei lemping av kontrollen med tilgangen til dette registeret.

Datatilsynet gjennomførte i meldingsåret tilsyn hos fleire teleoperatørar. Det vart avdekt ei rekkje omstende som viser trong for tettare kontroll og oppfølging av vilkår og tilgang til denne typen opplysningar. Dette meiner Datatilsynet i første rekkje bør vere folkeregisterets eige ansvar.

Datatilsynet påpeikte at det er viktig at vilkåra for tilgang til og kontroll av personopplysningar blir oppretthaldne. Personopplysningar som til dømes fødselsnummer har vore ei viktig råvare for identitetstjuveri. Dersom folkeregisterets lovmessige plikt til å halde oversikt over tilgangen til, vilkåra for og kontrollen med opplysningane i databasen fell bort, aukar òg risikoen for at misbruk ikkje blir fanga opp eller kan ettersporast. I og med at det her handlar om det sentrale personregisteret i Noreg er Datatilsynet oppteke av å jobbe for å halde ein balanse mellom tilgang til og kontrollen av registeret.

Datatilsynet var tilfreds med at tilsynets merknader i høyringsrunden vart ivaretekne. I den nye folkeregisterforskrifta § 9-2 framgår det no at registermyndigheita skal sikre dokumentasjon om kven som har fått folkeregisteropplysningane, kva typar av opplysningar som er utleverte og dei vilkår som er knytte til vedtaket. I tillegg skal registermyndigheita følgje opp om vilkåra blir overhaldne.

9.5.2 Utstrekt bruk av fødselsnummer aukar risikoen for ID-tjuveri

Alle unike identifikatorar vil ha ein eigenverdi fordi dei eintydig identifiserer eit individ. Unike identifikatorar gjer det mogleg å samle informasjon som gjeld ein gitt person, slik at ein får eit meir fullstendig bilete av personen.

Eit fødselsnummer blir utstedt til norske innbyggjarar. Eit tilsvarande nummer (D-nummer) blir utstedt til utlendingar som har bu- og arbeidsløyve. Til fødselsnummeret er det knytt namn, bustad, alder, det ein har av eigedom, økonomiske aktiva, sosiale rettar mv. Dei offentlege aktørane nyttar først og fremst nummeret til å halde orden på sitt

omfattande registerregime. Dersom ein ser offentleg sektor under eitt, har ein ei gigantisk samling av opplysningar om kvart enkelt individ. Registreringane skjer kontinuerleg frå fødsel til død.

Ein meir utbreidd bruk av fødselsnummer vil føre til at stadig fleire aktørar får tilgang til ein unik nøkkel. Om kopling mellom individ og fødselsnummeret er kjend, vil det i første omgang innebere at nokon har tilgang til ein unik nøkkel som kan, men ikkje nødvendigvis vil, bli brukt. Auka bruk av eintydige og varige identifikatorar inneber ein auka risiko for identitetstjuveri. Dette heng saman med at denne felles identifikatoren forenklar tilførsel av nye opplysningar dersom det skulle dukke opp fleire kjelder.

Tenestespekteret som blir tilbode frå offentleg og privat sektor inneber trong for ein kontroll av identitet. Dessverre har ikkje arbeidet med e-ID halde tritt med utviklinga av tenestespekteret. Det har oppstått eit vakuum som blir fylt med mindre gode løysingar. Fleire bruker brukarnamn, passord og i nokre tilfelle eingongskodar eller passordgeneratorar. Slike løysingar kan vere tilstrekkelege i høve til somme føremål, men er slett ikkje eigna i eit lengre perspektiv. For det første er det eit stort problem at passord blir brukte om att, for det andre at dei sjeldan blir bytte ut og for det tredje at dei ikkje allment kan trekkjast tilbake, då det ikkje er føresett tredjepartsverifikasjon.

Dersom nokon skulle få tilgang til ein dårleg sikra base over passord er det dermed stor sjanse for at informasjonen kan misbrukast overfor andre verksemder.

9.5.3 Tilsyn: E-signaturar

Datatilsynet har i løpet av meldingsåret vore på tilsyn hos fleire e-ID leverandørar. Tilsyna har etterlate eit inntrykk av at feltet enno er i startfasen, med ein monaleg auke i utstedde e-ID'ar mot slutten av 2007. Store private aktørar som Buypass og Bank-ID har allereie distribuert eit stort tal e-ID'ar til innbyggjarane. Vidare står òg det offentlege på trappene med sine e-ID-løysingar.

Datatilsynet meiner at innbyggjaranes gryande tilgang til e-ID'ar vil kunne dekkje ein trong for å kunne identifisere seg i den elektroniske verda. Det er avgjerande viktig for Datatilsynet at dei nye e-ID-løysingane blir av tilstrekkeleg kvalitet òg når det gjeld informasjonstryggleik. Datatilsynet samarbeider med Post- og teletilsynet på dette feltet, i samband med handteringa av e-signaturlova.

Det er viktig at brukarane forstår kor kraftig ein e-ID med kvalifisert signatur er. Passord (PIN-kodar) og eventuelle kort og andre tryggleiksmekanismar må handterast på ein måte som gjer at dei ikkje kan misbrukast av uvedkommande. Det er viktig at e-ID leverandørane gir krystallklar informasjon til brukarane om dette.

Det er likevel òg viktig at moglegheita til å kunne identifisere personar over Internett ikkje fører til eit krav om at ein skal identifisere seg i alle samanhenger. Datatilsynet kan allereie no sjå faren for at aktørar framover vil nytte identifiseringsløysingar utan at det strengt teke er naudsynt. Datatilsynet vil følgje nøye med, no som folket i større grad får tilgang til elektroniske identitetar, og passe på at unødvendig bruk av e-ID ikkje skjer.

9.5.4 Norsk Tipping

Norsk Tipping har utfordra personvernet på ei rekkje frontar i meldingsåret. Spelarkortet som spelarane får tilbod om har ein brei funksjonalitet utover det som er naudsynt for å kunne spele Norsk Tipping-spel. Overvaking av spelaktiviteten er òg aukande.

Spelarkortet kan nyttast for nokre av spela og må nyttast i andre spel, til dømes for spela Joker og Extra. Det er framleis mogleg å spele uregistrert via kommisjonær. Spelarkortet kan, etter ein tilleggsprosedyre, brukast til e-signatur. Datatilsynet er oppteke av at kundane til Norsk Tipping blir tilstrekkeleg informerte om kva tippekortet kan brukast til og at dette er eit kort som brukarane må passe på, på lik linje med til dømes eit bankkort. Datatilsynet har derfor bedt Norsk Tipping om å betre informasjonen til brukarane.

Datatilsynet har teke opp tryggleiken ved utsteding av spelarkortet med Norsk Tipping, Buypass og Post- og teletilsynet. Det ligg føre konkrete døme på at ID-kontrollen ikkje er tilstrekkeleg for å forhindre ID-tjuveri og misbruk, i tillegg til at kunnskapen spelarane sit inne med er låg.

Datatilsynet har registrert at Norsk Tipping legg opp til full overvaking av spelåtferd. Verksemda vil overvake kor mykje, kor fort, og kor lenge det blir spelt. Norsk Tipping vil regulere kva som skal kunne takast ut og spelast for i løpet av ein time.

Norsk Tipping vil i stor grad vil kunne identifisere enkeltspelarane. Datatilsynet er uroa for moglegheitene for profilbygging. Datatilsynet er òg uroa for at det skjer ei utgliding med tanke på kven som har tilgang til det kraftige overvakingsverktøyet.

9.5.5 Fingeravtrykk i pass

Datatilsynet hadde innvendingar mot tryggleiken då dei nye passa kom for nokre år tilbake. Passa inneheld biometriske data lagra i ei brikke som kan avlesast på avstand. I utgangspunktet vart eit ansiktsbilete valt som biometrisk opplysningstype. Men planen er å ta i bruk fingeravtrykk i tillegg. Datatilsynet meiner passa ikkje har tilstrekkeleg tryggleiksnivå for den nye, tiltenkte bruken.

Politiet har i slutten av 2007 testa sine nye biometristasjonar der mellom anna fingeravtrykk blir henta inn for innplassering i framtidige pass. Føremålet med testane er å sjekke om mellom anna kommunikasjonen frå biometristasjonane og til produsent av pass vil fungere tilfredsstillande.

Justisdepartementet har enno ikkje orientert nærare om korleis ei eventuell seinare innplassering av fingeravtrykk i passa skal handterast. Datatilsynet er uroa for informasjonstryggleiken, både i samband med passhandteringa sentralt og korleis brukarane skal forholde seg til denne typen pass. Eit bilete av eit fingeravtrykk i eit pass vil kunne misbrukast. Det er viktig at tilstrekkelege tryggleiksmekanismar blir etablerte.

Det er framleis uklårt kva føremålet med fingeravtrykka er, og dermed kven som skal ha tilgang til denne informasjonen. At denne integritetssensitive informasjonen ligg på ei brikke som kan avlesast på avstand, gir ekstra grunn til bekymring.

9.5.6 Biometri – bruk av fingeravtrykk

Biometriske kjenneteikn kan seiast å vere kjenneteikn som kjem frå kroppen, som er unike for den registrerte og samtidig permanente eller stabile over tid. Ved å måle desse kjenneteikna kan dei nyttast til å gjenkjenne ein person, eller den påståtte identiteten til ein person.

Biometri blir ofte skildra som «noko vi er» når det blir samanlikna med dei tradisjonelle metodane for å gjenkjenne eller stadfeste ein persons identitet. Dei tradisjonelle metodane omfattar «noko du veit», til dømes eit passord, og «noko du har», til dømes ei kodebrikke. Biometri har sin eigenart, det er uløyseleg knytt til kroppen vår, på godt og vondt.

Dei mest kjende formene for biometriske kjenneteikn er fingeravtrykk, handavtrykk og ansiktsform, pluss dei to augeteknologiane netthinne- og irisavlesing.

Biometrisk informasjon blir normalt lagra i form av ein såkalla «template». Dette er ein kodebasert representasjon av materialet, i staden for å lagre ei hel måling, til dømes eit fullt bilete av eit fingeravtrykk, med alle sine detaljar. Slike templates blir mellom anna brukte fordi det gjer det lettare å samanlikne eit avgitt fingeravtrykk opp mot tidlegare registrert fingeravtrykk.

Datatilsynet har ikkje noko prinsipielt imot bruk av fingeravtrykk eller andre biometriske kjenneteikn, men tolkar formuleringane i personopplysningslova § 12 slik at høvet til bruk er snevert. Brukt rett kan biometri vere eit godt og effektivt verktøy for tryggleik. Løysingar som baserer seg på biometri nyter generelt høg tillit blant innbyggjarane, med omsyn til presisjon og tryggleik. Det er derfor viktig å forhindre uriktig bruk av slike verktøy.

I 2007 mottok Datatilsynet fire vedtak frå Personvernnemnda knytte til bruk av fingeravtrykk. Sakene gjeld bruk av fingeravtrykk i kombinasjon med ID-kort i inngangskontrollen til Essos tankanlegg, fingeravtrykk som erstatning for medlemskort ved to forskjellige treningssenter, og bruk av fingeravtrykk i tilknyting til timeregistrering for tilsette i REMA1000. Esso fikk medhald i ønskjet om å bruke fingeravtrykk under føresetnad av samtykke frå den registrerte. I dei andre sakene opprettheldt nemnda Datatilsynets avslag. Frå 2006 ligg det i tillegg føre eit vedtak frå Personvernnemnda om at fingeravtrykk kan brukast for pålogging for kommunetilsette til datamaskinar med sensitive personopplysningar, dersom den tilsette samtykkjer.

Personvernnemnda har uttalt at dei fem vedtaka om biometri er konkrete, og skaper presedens berre i avgrensa grad. Datatilsynet finn likevel at nemnda gjennom vedtaka har sagt ein god del om korleis personopplysningslova § 12 skal forståast òg i andre samanhengar, og kvar nedre grense for bruk av fingeravtrykk ligg. I begge sakene der bruk av fingeravtrykk vart akseptert har nemnda vist til trongen for tryggleik. Og i begge sakene er bruken basert på samtykke frå den registrerte.

På denne bakgrunnen har Datatilsynet i meldingsåret omgjort eit vedtak som forbaud Stortinget å bruke fingeravtrykk i pålogging til datamaskinar, slik at dette no er tillate. Stortinget nytta nøyaktig same påloggingsløysing som den nemnda vurderte i saka frå 2006.

Datatilsynet har vidare bestemt at SAS kan nytte fingeravtrykk i samband med innsjekking av bagasje i sjølvbeteningsskrankar for å oppnå betre tryggleik. Det er ein føresetnad for avgjerda at det framleis er mogleg å sjekke inn bagasje i betent

luke utan å gi frå seg fingeravtrykk, og at den reisande får tilstrekkeleg informasjon om løysinga og alternativa.

I meldingsåret gav Datatilsynet rettleiing om regelverket til fleire produsentar og distributørar av fingeravtrykksløysingar. Ingen ting tyder på at sakstilfanget på dette området vil bli mindre i nærast framtid. I tillegg til å handtere nye saker på feltet, vil Datatilsynet halde eit vakent auge med dei aktørar som lovleg kan nytte fingeravtrykk for å sikre at føresetnadene ikkje blir sette til side.

9.6 Arbeidsliv

9.6.1 Innsyn i tilsette sin e-post

I 2007 såg Datatilsynet ei viss endring i forhold til førespurnader om innsyn i e-post. Det kan synast å ha skjedd ei vriding frå konkrete klager frå tilsette som har opplevd innsyn i sin e-postkasse, til at førespurnadene i større grad kjem i forkant av at innsyn blir gjennomført, gjennom at verksemda sjølv gir Datatilsynet informasjon om sine planar. Datatilsynet ser dette som ei stadfesting av at fleire verksemder no er kjende med at det finst grenser for når innsyn i e-post kan gjennomførast, og at det er ein del reglar og retningslinjer for den faktiske gjennomføringa. Førespurnadene Datatilsynet har motteke ber òg preg av at verksemdene ønskjer å opptre korrekt og i tråd med dei reglar som gjeld på området. Når tilsette vender seg til Datatilsynet, er det i aukande grad fordi dei faktisk har motteke informasjon om at det er planlagt å gjennomføre innsyn, og at dei ønskjer å få stadfesta at framgangsmåten er i tråd med lovar og reglar.

Førespurnadene tyder òg på at fleire verksemder lagar interne reglar og instruksar om innsyn i e-post. Samtidig er det ikkje til å legge skjul på at innsyn i e-post synest å ha blitt ein «vanleg» prosedyre i ein del saker, til dømes i tiknyting til interne granskingar av forskjellige slag. Datatilsynet har ikkje grunnlag for å seie at det skjer meir innsyn i e-post no enn før, men det kan synast som om vi står overfor ein aukande tendens, utan at dette nødvendigvis har samanheng med at trongen for innsyn har auka tilsvarande.

Vinmonopolet og Redningsselskapet

Datatilsynet melde i 2005 Vinmonopolet og Redningsselskapet til politiet for brot på føresegnene i personopplysningslova om informasjonsplikt i samband med innsyn i tilsettes e-post. I 2006 vart begge sakene lagde til side av påtalemakta. Datatilsynet klaga på desse avgjerdene, men dei vart oppretthaldne av Riksadvokaten. Riksadvokaten bad likevel om at Statsadvokaten måtte ta stilling til om det skulle gjerast vidare etterforsking for å avdekkje om tilsette i Redningsselskapet hadde halde tiltake opplysningar for Datatilsynet. Òg denne saka vart lagd vekk i oktober 2007.

Bazarsaka

Datatilsynet melde i 2006 Bazar Forlag AS til politiet for brot på personopplysningslova. Meldinga skjedde på bakgrunn av eit gjennomført tilsyn med forlaget hausten 2005.

Bakgrunnen for saka var at forlagssjefen i Bazar Forlag AS oppretta ein «overvakingskonto» med namnet backup@bazarforlag.com. Via «overvakingskontoen» skjedde det ei automatisk blindkopiering av inngåande e-postkorrespondanse til leiaren for forlaget sitt kontor i Sverige. Den tilsette sin personlege e-postkonto var verna med brukarnamn og personleg passord.

Forlagssjefen gjorde innsyn i den tilsettes inngåande e-post gjennom «overvakingskontoen». Den tilsette som fekk lasta ned og opna sin inngåande e-post, fekk ingen informasjon om nedlastinga av e-postane, innsynet i desse, føremålet med handsaminga eller eventuell utlevering av informasjonen.

Etter Datatilsynets vurdering braut Bazar Forlag AS føresegnene i personopplysningslova på fleire punkt, og etter tilsynet si vurdering var lovbrota av alvorleg karakter. Spesielt alvorleg var brota på informasjonsplikta etter personopplysningslova § 19 og § 20.

Politimeisteren i Oslo sikta Bazar Forlag AS og forlagssjefen for brot på informasjonsplikta og gav førelegg til begge. Både forlaget og forlagssjefen vedtok førelegget.

9.7 Kameraovervaking

9.7.1 Kamera i «offentlege pauserom»

Hovudtema for kontrollarbeidet innan kameraovervaking var tilsyn med såkalla «offentlege pauserom», nemleg kafear, restaurantar, barar og utestader. Desse utgjorde til saman 11 av dei i alt 25 kontrollane.

Barar og utestader, kafear og restaurantar har mange likskapstrekk med den funksjonen «pauserommet» har, òg sjølv om det ikkje er på arbeidsplassen, og heller ikkje direkte innanfor ein privat sfære. Folk går til desse stadene for å treffe andre, for å hyggje seg, kople av og drive ei form for rekreasjon, ete, drikke, feste og danse. Datatilsy-

net meiner ein ikkje kan vurdere desse stadene på same måte som ein vurderer kameraovervaking av butikkar. Verken stadene eller funksjonen deira er lik butikkane, og gjestene si personverninteresse vil heller ikkje vere tilsvarande i dei to forskjellige settingane. Mykje av den samhandlinga som skjer på barar, restaurantar og utestader har ein privat karakter – midt i det som òg er eit offentleg rom. Datatilsynet meiner at diskresjonsomsyn i ein viss grad må gjelde. Samtidig må ein ta omsyn til krava som følgjer av det faktum at barar, utestader, kafear og restaurantar òg er nokon sin arbeidsplass.

Sjølv om tryggleik i ein viss grad blir skyvd føre som eit generelt, diffust argument, er dei konkrete grunngivingane i stor grad knytte til vern av materielle verdiar, kanskje særleg svinn av varer og pengar. For dei stader der tryggleiksproblematikk gjer seg reelt gjeldande, er truleg dørvakter og interne rutinar det avgjerande for tryggleiken til gjestene og dei tilsette.

Alle kontrollane førte til varsel om pålegg. Dette dreier seg om ei rekkje forhold, som mangelfull varsling og manglande melding. Alle stadene vart varsla om anten opphøyr av overvakinga eller innskrenkingar i den eksisterande overvakinga.

Dei konkrete vurderingane i samband med kontrollane viser at det er vanskeleg å få til ei lovleg overvaking av denne typen stader:

1. Det vil normalt ikkje liggje føre noko gyldig grunnlag for overvaking av publikumsområda i lokalet.
2. Overvaking av området rundt bardiskane er vanskeleg å få til då det finst eit todelt personvernomsyn, nemleg både gjestene og dei tilsette. Konkret har tilsynet vurdert at overvakinga ikkje er tillaten om den medfører at tilsette blir tilnærma totalovervaka i sin primære arbeidsstasjon, som bak bardisken. Om slik overvaking skal kunne tillatast, må det liggje føre meir tungtvegande omsyn enn svinnproblematikk. Tilsynet har likevel falle ned på at gjestene lovleg kan filmast i det dei går inn eller ut av lokalet, der det har vore ein trong for dette.

9.7.2 Tilsyn: Private kan ikkje overvake det offentlege rom

Datatilsynet såg i meldingsåret på kameraovervaking i tilknyting til eit fotballstadion og overvaking av eit større område brukt til næringsverksemd. Desse to har eitt felles tema, kameraovervaking av område som blir brukte av allmenta. Konklusjonen i desse to tilsyna viser at private aktørar ikkje på generell basis kan overvake det offentlege rom, til dømes ein turveg, sjølv om vegen går over privat grunn.

9.8 Samferdsel – Personvern ved reiser frå A til B

Datatilsynet observerte i 2006 at det vart bygd opp ein omfattande infrastruktur for overvaking av reisande, både bilistar og innan kollektivtrafikken. Dette dreier seg om alt frå overgripande overvaking med satellittar, overvaking ved hjelp av kamera og radiofrekvensbrikker (som AutoPASS), til såkalla «svarte boksar» som sit i den enkelte bilen og registrerer kjøringa. I meldingsåret har denne utviklinga halde fram. Mellom anna er det bestemt at bomringen i Oslo skal bli heilautomatisk, det vil seie at det ikkje lenger skal vere mogleg å passere bompengeanlegget utan å leggje att spor.

9.8.1 Bombrikker – AutoPASS

Datatilsynet mottok våren 2007 opplysningar om at alle passeringar i bomstasjonane rutinemessig vart fotograferte. Denne informasjonen samsvarte ikkje med den offisielle kravspesifikasjonen for AutoPASS, eller dei opplysningane tilsynet tidlegare hadde motteke om temaet frå Vegdirektoratet. Det var nemleg berre ugyldige passeringar som skulle fotograferast.

Vegdirektoratet vart bede om å stadfeste/avkrefte om alle passeringar ved bomstasjonane i Noreg blir fotograferte. På bakgrunn av svarbrevet frå Vegdirektoratet, måtte Datatilsynet konstatere at det blir teke bilete av alle passeringar, ved alle bomstasjonar. Bileta blir likevel berre sende vidare i systemet dersom passeringa er ugyldig, eller ved stikkprøvekontrollar. Ei anna avgrensing skal visstnok liggje i at internminnet i kameraet er av avgrensa storleik, og at bileta som ikkje blir vidaresende derfor blir overskrivne relativt raskt.

Datatilsynet finn det beklageleg at systemet ikkje samsvarer med kravspesifikasjonen, og at verken publikum eller tilsynet har blitt informert om forholdet på eit tidlegare stadium.

Tilsynet føreset at systemet blir utbetra innan rimeleg tid.

Dei 100 seinaste passeringane blir lagra i AutoPASS-brikka

I byrjinga av meldingsåret avdekte Datatilsynet det faktum at dei seinaste 100 passeringane i bomstasjonar ein AutoPASS-brukar hadde passert, vart registrerte i AutoPASS-brikka. I tillegg vart fleire andre passeringspunkt registrerte. Verken Statens vegvesen, som systemeigar, eller bompengeselskapa hadde informert brukarane om forholdet. Datatilsynet reagerte òg på at desse personopplysningane vart lagra på brikker som kan avlesast på avstand, totalt utan konfidensialitetsvern.

Datatilsynet meiner at Statens Vegvesen har late vere å gi utførleg og naudsynt informasjon om lagringa av passeringsopplysningar i AutoPASS-systemet.

Både i Datatilsynet, Personvernnemnda og Samferdselsdepartementet har det vore lagt til grunn at passeringsopplysningane blir sletta så raskt som mogleg etter at faktura er betalt. Det er òg lagt til grunn at dei som ønskjer det, kan inngå ein avtale om at opplysningane blir sletta seinast etter 72 timar. Det mest alvorlege er likevel at dei ca. ein million brukarane av AutoPASS ikkje er blitt aktivt informerte om at passeringsbrikka på frontruta òg er ei lagringseining som lagrar opplysningar om tid og stad for dei 100 seinaste passeringane.

Dårleg tryggleik

I tillegg til lagringa av personopplysningar i AutoPASS-brikka, blir passeringsopplysningar lagra sentralt. Desse opplysningane er òg tilgjengelege for brukarane via diverse påloggingsløysingar. Desse løysingane ser òg ut til å ha for dårleg informasjonstryggleik, med omsyn til konfidensialitet og passordvern. Statens vegvesen har i løpet av året 2007 gitt informasjon om at desse systema skal betrast. Datatilsynet er ikkje fornøgd med at dette arbeidet tek lang tid.

I løpet av året 2007 er det ei rekkje andre verksemder som ønskjer å nytte AutoPASS-systemet, til dømes til tilgangskontroll. I Stavanger ønskjer ein å nytte AutoPASS-brikka for å gi utvalde kjøretøy tilgang til avgrensa områder i byen. Andre private verksemder har òg gitt uttrykk for same ønskje. Auka bruk av AutoPASS-systemet til andre føremål enn det opphavlege, å krevje inn bompengar, gir etter Datatilsynets meining eit mindre godt personvern.

9.8.2 Bompasseringar til likningskontoret

I januar tok Datatilsynet kontakt med Skattedirektoratet om utlevering av bompasseringsopplysningar til kontroll av likninga. Bakgrunnen for førespurnaden var at ei rekkje bompengeselskap hadde fått førespurnader om innsyn frå fylkesskattekontora.

Datatilsynet ønskte i første omgang ei tilbakemelding på kva heimelgrunnlag Skattedirektoratet legg til grunn for å krevje utlevering av passeringsopplysningar. I tillegg ønskte Datatilsynet ei avklaring av kva passeringsopplysningar som skal registrerast, og kor lenge dei skal lagrast av rekneskapsomsyn.

Per i dag registrerer bompengeselskapa passeringsopplysningar etter retningslinjer som Vegdirektoratet har gitt. Skattedirektoratet kan etter likningslova krevje innsyn i opplysningar knytte til konkrete kjøretøy nytta i næringsverksemd. Skattedirektoratet grunngir trongen for innhenting av opplysningane med at desse vil kunne kaste lys over påstandar i likninga. Det blir likevel gjort klårt at skattemyndigheitene ikkje vil krevje innsyn i opplysningar som skulle ha vore sletta.

I praksis blir det i bompengeselskapa ikkje gjort nokon skilnad mellom lagring av passeringsopplysningar for kjøretøy brukte i næringsverksemd eller privat bruk. Datatilsynet åtvarar mot ein situasjon der passeringsopplysningar for private kjøretøy blir oppbevarte unødig.

Det er i hovudsak tre ulike betalingsformer som er tilgjengelege; periodeavtalar, forskotsbetalte avtalar og etterskotsbetaling av enkeltpasseringar. Innanfor kvar av desse betalingsalternativa blir det praktisert ulike retningslinjer for sletting av passeringsopplysningar.

Datatilsynet vil ikkje nekte bompengeselskapa å oppbevare passeringsopplysningar for kundar som eksplisitt ønskjer dette. Men det er viktig at denne oppbevaringa blir avtalt særskilt med kundane, og at dei samtykkjer aktivt. Kundane må òg vere innforståtte med at skattemyndigheitene, og eventuelt andre kontrollmyndigheiter, då vil kunne krevje tilgang til dei lagra opplysningane.

Tilsynet er innforstått med at bokføringsreglane er relevante på dei fleste område, og at det kan tenkjast at registrerte opplysningar blir nytta til å kaste lys over påstandar i likninga. For tilsynet er det likevel viktig å understreke at ein overgang frå kontantbetaling til elektroniske betalingsmåtar ikkje automatisk skaper ein trong for langtidsoppbevaring av all detaljinformasjon. For

å oppfylle kravet etter bokføringsregelverket skal ein berre lagre dei detaljane om kjøpet som er naudsynte for å ivareta krava i dette regelverket.

9.8.3 Tilsyn – Tromskortet, elektronisk billettering

Ordningar med elektronisk billettering er under rask framvekst i samferdselssektoren. Samferdsel er i stor grad eit fylkeskommunalt ansvar, og utviklinga skjer derfor hovudsakleg regionalt. Dette medfører at det veks fram fleire ulike løysingar. Sakene som ligg føre viser tydeleg mangel på etterleving av personopplysningslova i sektoren. Særleg alvorleg er det at identifiserbare reiseopplysningar blir registrerte og oppbevarte på ubestemt tid.

Elektronisk billettering inneber ein trussel for den grunnleggjande retten kvar enkelt har til sporfri ferdsel i samfunnet. Datatilsynet meiner derfor at det er viktig at dei ulike systema oppfyller krava i personopplysningslova. Reiseopplysningar må slettast når det ikkje lenger er sakleg grunn til å behalde dei.

Datatilsynet fann vesentlege manglar. Mellom anna mangla eit rettsleg grunnlag, opplysningane var ikkje tenkt sletta i tråd med krava i personopplysningslova, informasjonsplikta overfor dei reisande var ikkje oppfylt, og det var uklårt om rettane til dei registrerte vart ivaretekne ved handsaminga.

Informasjonstryggleiken var heller ikkje tilfredsstillande, mellom anna mangla datahandsamaravtale med driftsleverandør. Det fanst ingen dokumenterte rutinar for å ivareta personopplysningslova sine føresegner i samband med elektronisk billettering.

9.8.4 eCall

eCall er ei planlagd alarmteneste for bilulykker i Europa. Tenesta er tenkt å verke slik at ein svart boks i bilen automatisk skal kunne ringje nødnummeret og opplyse om bilen sin posisjon i tilfelle ulykker.

Systemet er planlagt å bli ei felleseuropeisk alarmteneste for kjøretøy, bygd på alarmnummeret 112. Alle bilar som blir selde i EU-området frå 2010 skal etter planen vere utstyrte med satellittposisjonering og kommunikasjon via mobiltelefonnettet. Dette utstyret skal automatisk sende informasjon til nærmaste alarmsentral ved ulykker.

Datatilsynet ser at systemet kan ha visse positive sider, men gjennomføringa vil kunne innebere problem med omsyn til personvern og vern av privatlivets fred.

Det føreslåtte eCall-systemet er basert på eit nesten omgåande tale- og datasamband frå ein eCall-generator til ein offentleg alarmsentral. eCall-førespurnaden blir automatisk utløyst av sensorar i bilen i tilfelle ulykke, eller manuelt av personar som oppheld seg i bilen.

eCall-førespurnaden består av to element: eit 112-oppkall med rein tale (audio) og eit minimumsdatasett. Datasettet og talemeldinga blir overførte via mobilnettet, og behandla som ei 112-nødoppringing i mobilnettet. Mobilnettoperatøren legg derfor til opplysningar om abonnenten sitt nummer, og oppgir posisjonen til oppringaren så presist som mogleg. Dette er i tråd med vanlige prosedyrar når nokon ringjer nødnummeret 112.

Frivillig medverknad

eCall er eit overvakingsinstrument som legg til rette for ei massiv registrering. Frå ein personvernståstad bør lovlydige bilistar ha høve til å bruke vegnettet utan å bli registrerte. For Datatilsynet er derfor frivillig medverknad viktig – at kvar og ein skal ha høve til sjølv å avgjere om bilen skal overvakast eller ikkje.

eCall er meint å vere innbygd i kjøretøyet. Det er ei felles oppfatning mellom datatilsynsmyndigheitene i Europa at du sjølv skal kunne avgjere om boksen skal vere aktivert eller ikkje. Brukaren, som ikkje nødvendigvis er eigaren av kjøretøyet, skal på kvart tidspunkt ha høve til å slå systemet på eller av utan noka form for tekniske eller finansielle hindringar. Denne valmoglegheita kunne t.d. bli tilbode i form av ein brytar eller omskiftar, i likskap med den som blir nytta i samband med airbags for passasjerar.

Det vil vere problematisk for personvernet dersom bilforsikringsselskap eller bilutleigefirma pressar sjåføren til å aktivere eCall-systemet. Tilsvarande vil òg vere situasjonen dersom tilsette som nyttar firmabilar, direkte eller indirekte blir tvungne til å nytte eCall-systemet. Slik tvang vil neppe vil ha rettsleg grunnlag i personopplysningslova.

Posisjonering

Datatilsynet har fått inntrykk av at den føreslåtte eCall-ordninga ikkje medfører at bilen sin posisjon skal følgjast kontinuerleg av ein tredjeperson. Det skal likevel vere mogleg å slå fast kvar kjøretøyet er å finne. Boksen skal, etter det som er opplyst, berre få samband med kommunikasjonsnettet dersom det blir aktivert i samband med ei

ulykke eller blir aktivert manuelt av ein av passasjerane i bilen.

I den føreslåtte eCall-ordninga oppbevarer «boksen» data for dei tre seinaste GPS- /Galileoregistrerte posisjonane, men desse skal ikkje kommuniserast med mindre eCall blir utløyst. I så fall vil det vere naudsynt å fastsetje ei klår avgrensing av omfanget av dei innsamla dataa. I kva grad det i framtida vil vere mogleg å fjernaktivere sporingsverktøyet, er førebels meir uklårt.

9.8.5 Nakenskanning

Avinor gav hausten 2007 uttrykk for eit ønskje om å teste ein «bodyscanner». Dette er ein maskin som nyttar radiostråling (millimeterbølgjer) for å sjå om ein person ber skjulte objekt på kroppen. Strålinga kan ikkje «sjå» objekt under huda. Innretninga «kler deg naken», og representerer utan tvil eit vesentleg inngrep i den personlege integriteten.

Avinor var i dialog med Datatilsynet om tiltaket. I ei pressemelding har etaten uttalt at reaksjonar frå tilsette, tilbakemeldingar frå Datatilsynet og reaksjonar i opinionen gjer at uttestinga ikkje blir gjennomført som planlagt våren 2008. Avinor ønskjer å innhente ytterlegare erfaringar, mellom anna frå utprøving av utstyret i andre land, før ei eventuell vidare uttesting.

Avinors planar om å innføre kroppskanning på norske flyplassar føyer seg inn i rekkja av stadig meir integritetskrenkjande tiltak. Datatilsynet har sett med aukande uro på korleis ny teknologi blir introdusert på ein måte som gir lite rom for personvernet. Det er ikkje nødvendigvis noko motsetningsforhold mellom bruk av ny teknologi og personvern. Kroppskanninga viser likevel korleis motsetninga mellom trongen for tryggleik og personvern kan oppstå. Er det verkeleg naudsynt med tiltak av denne typen, eller kan ein oppnå tilsvarande tryggleik på meir akseptabel måte?

9.8.6 Elektronisk handsaming av reiseopplysningar

Innan luftfarten blir det registrert store mengder personopplysningar. Opplysningane skal m.a. leverast ut til offentlege myndigheiter i Noreg og andre land. Det er vanskeleg å få oversikt over korleis opplysningane flyt i desse store systema, og når dei eventuelt endeleg blir sletta. Informasjonshandsaminga er i all hovudsak lovpålagd, gjennom ratifisering av internasjonale avtalar på luftfartsområdet.

Det er ein trend at flyselskapa opprettar ein slags reisekonto, der opplysningar om bestilte og gjennomførte reiser blir oppbevarte og gjorde tilgjengelege for kunden på Internett. Opplysningane blir med andre ord ikkje sletta. Dette er rekna for å vere ein service overfor kundane, og må etter Datatilsynets vurdering derfor grunnast på samtykke.

Datatilsynet såg spesielt på oppbevaring og tilgjengeleggjering av reiseopplysningar på den enkeltes «konto» hos eitt flyselskap. Funna er nedslåande. Handsaminga manglar rettsleg grunnlag. Opplysningane blir ikkje sletta i tråd med krava i personopplysningslova. Informasjonsplikta overfor dei reisande er ikkje oppfylt, og det er uklårt om dei registrerte sine rettar blir ivaretekne ved handsaminga. Heller ikkje informasjonstryggleiken er tilfredsstillande, mellom anna manglar datahandsamaravtale med driftsleverandør. Datatilsynet fann ingen dokumenterte rutinar for å ivareta føresegnene i personopplysningslova.

9.9 Velferd, forsking og helse

9.9.1 Tilsyn hos NAV

NAV-reforma vedkjem heile folket. I november i meldingsåret gjennomførte Datatilsynet tre kontrollar med lokale NAV-kontor. Tre pilotkontor vart valde. Desse var mellom dei første som slo saman dei tre tidlegare funksjonane, arbeid, trygd og sosialtenester. Kontora har vore i drift i om lag eitt år.

Ei rekke funn ved dei tre NAV-kontora gir grunn til uro.

Personkortet, som hentar nøkkelinformasjon frå tre forskjellige fagapplikasjonar, har blitt framheva som eit samhandlingsverktøy i NAV. Funna under kontrollane viser likevel at Personkortet i praksis ikkje blir oppfatta som tilstrekkeleg. Mange av sakshandsamarane ved det lokale NAV-kontoret sit no med tilgang til alle tre fagsystema frå dei tidlegare etatane, i tillegg til Personkortet. Overslagsvis har talet på brukarar i fagapplikasjonane blitt dobla etter samanslåinga. Datatilsynet kan heller ikkje sjå at det har blitt etablert avhjelpande tryggleikstiltak, som utvida logging eller tilpassa tilgangsstyring.

Datatilsynet er uroa over at det er planlagt, og til ein viss grad bestemt, at fagapplikasjonen Arena (frå tidlegare Aetat) skal nyttast som eit oppfølgingsverktøy for NAV. Brukarane sin tilgang i Arena blir gitt på eit nasjonalt nivå.

Hovudfunna ved tilsyna er:

1. Gjennom NAV-reforma har kvar enkelt medarbeidar fått ein vesentleg større tilgang til per-

sonopplysningar. Dagens tildelinga av tilgangar er ikkje eigna for å skape tillit, spesielt på grunn av manglande loggfunksjonalitet.
2. NAV synest å ha valt eit verktøy for å følgje opp kvar enkelt tenestemottakar utan at det er etablert grunnleggjande informasjonstryggingstiltak.
3. Dei kontrollerte kommunane har ved etableringa av NAV-kontora ikkje sytt for å følgje opp si sjølvstendige plikt til å sikre personopplysningar.
4. Dei kontrollerte kommunane hadde ikkje tilfredstillande internkontroll.
5. Utforminga av publikumsmottaka ved NAV-kontora gir store utfordringar i forhold til å sikre ein fortruleg dialog.

9.9.2 Uredigerte journalar til NAV

I eit lovendringsforslag opnar Arbeids- og inkluderingsdepartementet ytterlegare for at NAV skal kunne samle inn uredigerte, fullstendige pasientjournalar.

Føremålet med lovendringsforslaget er meir effektiv tilbakekrevjing av feilutbetalingar og betre verkemiddel for å motverke trygdemisbruk. NAV får nærast uavgrensa tilgang til fullstendige og uredigerte pasientjournalar dersom forslaget skulle bli vedteke. Om ein dømmer etter dei midla det er føreslått at NAV skal få, ser det ut til at oppklaring av trygdemisbruk blir oppfatta som viktigare enn oppklaring av drap. NAVs tilgang til journalane blir iallfall enklare enn politiet har, sjølv når politiet etterforskar alvorleg kriminalitet. I tillegg får NAV utvida heimlar til å samle inn informasjon frå andre enn helsevesenet. I realiteten får NAV ein «blankofullmakt» til å innhente alle opplysningar etaten sjølv meiner er relevante, òg om andre enn stønadsmottakaren.

9.9.3 Snikinnføring av forskingsdatabase over barnehagebarn

Innbakt i Kunnskapsdepartementets høyringsforslag om ny barnehagelov ligg eit forslag om innføring av ein ny database over barnehagebarn. Tilsynet meiner det er oppsiktsvekkjande om det blir oppretta ein slik database utan noka form for diskusjon.

Databasen er skildrar som ein «nasjonal database for utarbeiding av statistikk, forskning og analyse for å undersøke langsiktige effekter av deltagelse i barnehage i forhold til senere utdanning samt andre forhold som har betydning for en sosial utjevning».

Det nye lovforslaget pålegg kommunane ei plikt til å rapportere til denne databasen. For at dette skal vere mogleg blir det òg føreslått at foreldre og føresette blir pålagde ei plikt til å opplyse om barnet sitt fødselsnummer til bruk i statistikk, analyse og forsking. Barnehagar samlar allereie inn barns fødselsnummer mellom anna i barnehagesøknaden. Fødselsnummeret blir då nytta for å skilje barna frå kvarandre. Denne bruken reknar ein oppfyller personopplysningslova. Den nye føresegna gir inntrykk av at barnehagane ikkje har fødselsnummer frå før.

Datatilsynet har gjentekne gonger rådd Kunnskapsdepartementet frå å innføre ein ny nasjonal database utan ei grundig utgreiing i forkant. Tilsynet meiner det er viktig å kartleggje kva som er føremålet med databasen, kva opplysningar den skal omfatte, kven som skal forvalte den og kva tidsaspekt databasen vil ha. Ut frå høyringsbrevet ser det ut til at Kunnskapsdepartementet ser for seg at dei skal administrere registeret. Dette er ikkje naudsyntvis mest tenleg. Andre aktørar, som til dømes Statistisk sentralbyrå, kan vere betre eigna til denne oppgåva.

Datatilsynet etterlyser òg ei klårgjering av når opplysningar eventuelt skal slettast frå databasen. Ettersom dei aller fleste barn i løpet av sine første leveår er tilknytte ein barnehage, vil ein slik database over tid inkludere nesten heile innbyggjarane. Når det i tillegg kjem fram at eit forslag om å inkludere opplysningar om skolebarn er under utarbeiding, vil denne databasen på sikt kunne bli svært omfattande.

9.9.4 Ikkje krav om nøkkelboks for å kunne ta imot heimetenester

Kommunar kan ikkje krevje at pleie- og omsorgstrengande personar har nøkkelboks utanpå huset, seier Sosial- og helsedirektoratet. Sosial- og helsedirektoratet vurderte ordninga med bruk av obligatoriske nøkkelboksar for brukarar av pleie- og omsorgstenesta, på spørsmål frå Hamar-politikaren Borgny Nygaard.

Nøkkelboksar er låsbare småskap der nøkkelen til inngangsdøra til den pleie- eller omsorgstrengande blir oppbevart. Boksen skal kunne opnast med ein universalnøkkel som pleiarane ber med seg.

Datatilsynet har erfart at fleire personar oppfattar nøkkelboksane som stigmatiserande. Boksane vil mellom anna kunne fungere som eit synleg teikn på at det bur ein hjelpetrengande per-

son i huset. Tilsynet vurderte saka, og skreiv at nøkkelboksane kan røpe eit klientforhold, og at saka blir spesielt uheldig dersom nøkkelboks ved inngangsdøra blir eit kriterium for å kunne få pleie og omsorg i sin eigen heim.

Sosial- og helsedirektoratet sluttar seg til at det ikkje kan stillast slike krav, og seier at dette prinsippet må vere retningsgivande for alle kommunar i landet.

9.9.5 Tilsyn med rusomsorga

Datatilsynet gjennomførte ti tilsyn innan rusomsorga i meldingsåret. Tilsynsobjekta utgjorde eit variert utsnitt av ulike frivillige organisasjonar, statlege og kommunale etatar, forskingsinstitusjonar og helsetilbod som handsamar personopplysningar om rusavhengige.

Innan rusfeltet blir det registrert personopplysningar av til dels svært sensitiv karakter, mellom anna fysiske og psykiske helseopplysningar og opplysningar om straffbare forhold. Datatilsynet avdekte under tilsyna at omfanget av registrerte personopplysningar var vesentleg.

Det var gjennomgåande markante manglar ved programvaren som vart nytta i rusomsorga, mellom anna i forhold til mangelfull og til dels fråverande logging, mangelfulle høve til sletting og svært varierande tilgangsstyring, frå totalt fråverande til meir eller mindre tilfredsstillande.

I all hovudsak var det òg manglar i forhold til internkontrollsystem og dokumenterte rutinar for handsaming av personopplysningar. Informasjonen gitt til den registrerte var stort sett av munnleg karakter og mangelfull i forhold til personopplysningslova sine krav. To verksemder mangla konsesjon for si handsaming av sensitive personopplysningar.

Datatilsynet ser ikkje trong for å gjennomføre fleire tilsyn med rusomsorga. Sjølv om tilsyna er gjennomførte med tilsynsobjekt av relativt ulik karakter, er manglane etter personopplysningslova relativt like. Funna gir eit godt grunnlag for vidare arbeid innan området, noko som klårt er naudsynt for å sikre grunnleggjande rettar for dei registrerte. Datatilsynet vil ta forholda opp med mellom anna hovudleverandøren av programvare til russektoren og med direktorat og departement. Dette med tanke på å få betra sikringa av personopplysningane til den enkelte, ikkje berre som gruppe, men òg som enkeltindivid. Datatilsynet kan ikkje sjå at det er grunn til å behandle personopplysningane her annleis enn det som er ønskjeleg i helsevesenet.

9.9.6 Ny helseforskingslov – unødvendig vanskeleg for forskarane

I 2004 leverte Nylennautvalet si innstilling. Utgreinga konkluderte med at rammeverket for medisinsk forsking var komplisert, fragmentert, utilgjengeleg og til dels unødvendig byråkratisk. Sommaren 2007 vart Ot.prp. nr. 74 (2006-2007) Lov om medisinsk og helsefagleg forsking (helseforskingslova), oversend til Stortinget.

Datatilsynet er einig i vurderinga av at rammeverket er unødvendig komplisert og byråkratisk. Enklare søknadsprosedyrar og mindre byråkrati vil vere positive tiltak, inkludert forslaget om éin postkasse for førespurnader. Det er òg positivt at dei forskingsetiske komiteane får ei større og meir sentral rolle enn det som er tilfelle etter dagens regelverk. Tilsynet er òg tilhengar av innføring av eit regelverk som er lettare tilgjengeleg, slik at òg personar utan juridisk spesialkompetanse kan setje seg inn i føresegnene.

Lovforslaget, slik Datatilsynet forstår det, har eit monaleg forbetringspotensial på desse områda. Tre ulike lovar er rettnok samla i éin lov. Men denne er uklar, både i seg sjølv, og når det gjeld forholdet til omkringliggjande regelverk. Dette medfører vanskar både når ein skal fastsetje bruksområdet for lova, fastslå kva krav som skal stillast til sikring av opplysningane (informasjonstryggleik), og avklare dei involverte offentlege myndigheitene sine ansvarsområde.

Føresegna om det saklege verkeområde til lova er eitt av mange døme på at lova er uklår: Etter ordlyden skal lova ikkje gjelde ved etablering av helseregister. Helseforsking vil likevel nettopp innebere ei etablering av helseregister. Skal ein leggje vekt på ordlyden aleine, vil oppretting av alle slags helseregister framleis måtte handsamast av både Datatilsynet, Sosial- og helsedirektoratet og dei etiske komiteane. Ordlyden undergrev altså alle moglegheiter for forenkling. Etter tilsynets vurdering bør ordlyden endrast i samsvar med lova sine intensjonar, om ikkje anna så av omsyn til forskarane.

Manglande informasjonstryggleik

Personopplysningslova inneheld klare krav til informasjonstryggleik, men det er lite som tyder på at desse krava skal gjelde òg for helseforsking. Etter Datatilsynets syn kan ikkje forskarar fristillast på dette området. Dei same krav til informasjonstryggleik bør gjelde for medisinsk forsking som på andre område der ein handsamar helse-

opplysningar. Det er då naudsynt at helseforskingslova anten blir komplettert med eigne tryggleiksføresegner, eller at det blir teke inn ei tydeleg tilvising til krava til informasjonstryggleik i personopplysningslova.

Òg myndigheita til Datatilsynet etter lovforslaget er uklår. Det blir lagt opp til at dei forskingsetiske komiteane skal førehandsgodkjenne prosjekt som medfører forsking på helseopplysningar. Datatilsynet og Helsetilsynet er tillagde delt tilsynsmyndigheit, og skal gjennomføre etterkontrollar av forskingsprosjekta. For Datatilsynet er det likevel uklårt om rolla blir å sjå til at prosjekta blir gjennomførte i samsvar med vedtaka til dei forskingsetiske komiteane, eller om vi skal sjå til at dei blir gjennomførte i samsvar med tilsynet si forståing av lova.

Både dei etiske komiteane og Datatilsynet er, i medhald av lov, tillagde ei særleg uavhengig stilling. For forskingsmiljøet er det viktig å kunne ha tillit til at ei førehandsgodkjenning ikkje seinare blir sett til side av Datatilsynet. Ei ordning der Datatilsynet skal føre tilsyn ut frå korleis dei etiske komiteane forstår regelverket, vil på si side komme i konflikt med tilsynets rolle som ei sjølvstendig og uavhengig tilsynsmyndigheit.

Utholing av prinsippet om samtykke

Den formelle hovudregelen i forslaget er at forsking på helseopplysningar skal vere basert på samtykke frå den som opplysningane gjeld. Dette er i tråd med både forskingsetiske og personvernmessige grunnprinsipp, nasjonalt og internasjonalt.

Lovforslaget inneheld likevel så mange moglegheiter til å setje samtykket til side, at den reelle og praktiske hovudregelen lett vil bli at samtykke blir unødvendig.

Lovforslaget innfører òg eit nytt rettsleg omgrep, nemleg «bredt samtykke». Denne forma for samtykke strekkjer seg lengre enn det som blir akseptert i dag, og kan samanliknast med at ein inngår ein avtale utan å få lov til å lese avtalevilkåra. At det, etter utkastet til helseforskingslova, blir definert som eit «samtykke», er etter tilsynets vurdering uheldig. Ein står i fare for å uthole den grunnleggjande retten kvar enkelt har til informasjon og sjølvbestemming. Dette kan utvikle seg til ei belastning for det naudsynte tillitsforholdet mellom samfunnet og legen.

Sjølv om tanken om éin lov kan vere forlokkande, viser forslaget at det er vanskeleg i praksis å sameine regelverka. Når forslaget i tillegg inneber ein auka trussel mot personvernet, bad Datatilsynet Stortinget om at dei positive og negative verknadene ved lova skulle vurderast nærare.

9.9.7 Tilsyn: Tilgang til helseopplysningar

Hausten 2007 vart det gjennomført ein større kontroll med fokus på tilgang til helseopplysningar ved Sjukehuset i Vestfold HF.

Datatilsynet registrerer på bakgrunn av kontrollen med Sjukehuset i Vestfold at det framleis er helseføretak som handsamar helseopplysningar i journalsystem som er direkte ueigna til å ivareta fortrulegskapen overfor pasienten i eit moderne sjukehusmiljø. Det vart avdekt at det var gitt svært vide tilgangar på grunn av systemet sin konstruksjon. Dei vide tilgangane var supplerte med til dels fråverande loggfunksjonalitet. Det kom under kontrollen fram ei hending der eit høgt tal tilsette hadde gjort uautoriserte oppslag i ein del av informasjonssystemet som hadde etablert logging. Etter Datatilsynet sitt syn var ikkje hendinga adekvat følgt opp frå føretaket si side.

Dokumentkontrollane er ikkje ferdigbehandla i skrivande stund. Det er her òg parallelle saker hos Helsetilsynet i forhold til oppførsla til det involverte helsepersonellet. Datatilsynet registrerer fleire saker av denne karakteren. Datatilsynet legg til grunn at dette skuldast at eit auka fokus på informasjonstryggleik i sektoren medfører at fleire av føretaka evnar å avdekkje noko av snikinga i journalar.

9.9.8 Tilsyn: Urettmessig innsyn i pasientjournalar

Datatilsynet vart sommaren 2007 kontakta av Legeforeininga i samband med eit innsyn i pasientjournal ved Ullevål universitetssjukehus HF. Saka gjaldt ein person som var tilsett ved sjukehuset, og som òg hadde vore pasient same stad. Vedkommande oppdaga at fire personar utan behandlarrelasjon hadde gjort oppslag i hans journalnotat. Den tilsette oppdaga forholdet ved gjennomgang av journalloggen.

Tilsynet retta ein førespurnad til sjukehuset, og bad om fleire opplysningar. Dette omfatta mellom anna bakgrunnen og føremålet med kvart enkelt oppslag som ikkje var knytt direkte til behandlingssituasjonen. Ein bad òg om å få opplyst om personane som stod for oppslaga handla på vegner av andre eller i medhald av instruks. Tre av personane hadde berre gjort feiloppslag i kontaktoversikta, og ikkje lese sjølve journalen.

Snoking

Éin av personane, eit tidlegare tilsett helsepersonell ved sjukehuset, gjorde heile 37 oppslag i journalsystema over ein periode på ein månad i 2004. Oppslaga er i hovudsak gjorde i sjølve journalen. Vedkommande har ikkje hatt nokon behandlingsmessig eller annan grunn for innsyn i klagarens pasientjournal. Såkalla «aktualiseringsrett» skal vere nytta, og det er hevda at føremålet med oppslaga har vore «fagoppfølging». Oppslaga framstår som omfattande og kan gi inntrykk av å vere systematisk gjennomførte.

Helsepersonellet har i mail-korrespondanse med sjukehuset innvendingar til påstanden om ulovleg tilgang. Vedkommande uttaler at: «det forhold som beskrives er meg fullstendig ukjent og uforståelig». Det blir vidare ymta om at det må ha skjedd ein feil, eller at nokon andre har brukt vedkommandes tilgang utan at han/ho har visst om det. Sjukehuset har opplyst til Datatilsynet at det ikkje har vore mogleg å fastslå kva som er korrekt faktum, og at saka er meld som avvik til Helsetilsynet i Oslo og Akershus for vidare oppfølging. Ettersom vedkommande ikkje lenger arbeider ved sjukehuset, er arbeidsrettslege reaksjonar ikkje lenger aktuelt.

Datatilsynet ser svært alvorleg på denne type situasjonar. Forklaringa frå helsepersonellet verkar lite sannsynleg. I beste fall gir framstillinga inntrykk av svært kritikkverdig omgang med personlege tilgangskodar til journalsystema.

Når det gjeld helseføretaket, kan det sjå ut som om tilgangskontrollen ikkje er tilfredsstillande innretta. Helsepersonell bør ikkje ha ein systemtilgang som let dei gjere slike oppslag om pasientar dei ikkje har eit behandlarforhold til.

9.9.9 Snoking i pasientjournalar – trong for lovendring

Helse- og omsorgsdepartementet sende i meldingsåret ut eit forslag om å gjere det tydeleg at det er forbode å tileigne seg pasientopplysningar urettmessig. Datatilsynet er tilfreds med forslaget, men foreslår at ein vurderer å ta inn eit supplement. Tilsynets forslag er at det i tillegg blir lagt til rette for at alle pasientar kostnadsfritt får høve til å sjå sine eigne journalloggar. Pasienten vil på denne måten få høve til sjølv å gjennomgå kven som har lese i journalen. Journalloggen kan anten sendast til pasienten med jamne mellomrom, eller utleverast saman med journalutskrift/epikrise etter utskriving.

Føremålet med retten er å gi pasienten betre kontroll over kven som opnar journalen fordi dei er nyfikne. Ved at pasientane får tilgang til loggane, kan dei sjølve oppdage kor ofte – og kven – som har lese i journalane deira.

Personvernrisikoen i helsesektoren har auka som følgje av overgangen frå papir til elektroniske pasientjournalar (EPJ). Problematikken er særleg knytt til at meir informasjon er lettare tilgjengeleg for fleire, lettare å spreie til uvedkommande, og i den grad opplysningane først er spreidde, er det vanskelegare å avgrense skaden for pasientane som er ramma.

Ein fordel med elektroniske løysingar er likevel at dei gjer det mogleg å loggføre alle oppslag, altså ei automatisk registrering av kven som har opna kva for journalar og kor lenge dei har vore opne. Slike loggar eksisterer i dag, men erfaringa til tilsynet tilseier at desse ikkje blir kontrollerte eller følgde opp på ein tilfredsstillande måte.

Det er vanskeleg å gi eit kvalifisert omfang av uautoriserte oppslag i pasientjournalar. Moglegheitene for misbruk er definitivt til stades, og fleire misbrukssaker er førelagde tilsynet.

Ei MMI-undersøking, utført på oppdrag frå KFO og som stod på trykk i Dagbladet 5. juni 2005, slår fast at 86 prosent av dei tilsette i helsevesenet stadfestar at det er utbreidd å sjå i journalane ut over det som er naudsynt. Undersøkinga gir i beste fall uttrykk for at ein stor del av dei tilsette i helsevesenet ikkje er trygge på at journalopplysningar blir handterte på ein god nok måte.

Datatilsynet har lang erfaring med tilsyn retta mot helseføretak. Tilsyna har vist at det oppstår store moglegheiter for misbruk når ein kombinerer vid tildeling av tilgangsrettar til journalsystema, mangelfulle systemfunksjonar som kan avgrense tilgangen, og låg reell kontroll med heimelen for oppslag i systemet.

Det har vist seg å vere vanskeleg å avdekkje uautoriserte oppslag. Søkjelyset blir gjerne retta mot uautorisert tilgang til opplysningar om kjendisar og tilsette, men tilsynet har grunn til å tru at problemet er meir omfattande i forhold til opplysningar om folk ein kjenner. Dette kan vere langt vanskelegare å avsløre – rett og slett fordi føretaket ikkje kjenner til kven som er familiemedlemmer, venner eller kjenningar av den enkelte. Pasientane, derimot, kan sjå om den som har lese journalen er ein dei kjenner eller veit kven er.

For Datatilsynet er det viktig at både pasientar og tilsette ved norske helseføretak kjenner seg trygge på at journalopplysningar blir behandla med tilbørleg respekt for pasientanes integritet.

9.9.10 Datainnsamling bygd på medisinsk uforsvarleg prøvetaking – Aker sjukehus – Hoftebrotsprosjektet

For fem år sidan vart det ved Aker universitetssjukehus HF sett i gang ei prospektiv undersøking knytt til risikofaktorar for hoftebrot hos eldre over 65 år. Den kirurgiske delen av prosjektet innebar innhenting av muskel- og beinbiopsi i samband med den operative behandlinga. Datatilsynet gav konsesjon til dette i 2003. Datatilsynet varsla om at konsesjonen fall bort i løpet av meldingsåret. Årsaka til dette er den manglande overhaldinga av regelverket.

Vevsprøvene og alle personopplysningar knytte til, eller utleidde frå desse, vart pålagt sletta og destruerte på forsvarleg vis.

Uforsvarleg prøvetaking

I 2005 påla Statens helsetilsyn Aker universitetssjukehus HF å stanse innhentinga av biopsiar. Årsaka til pålegget var mellom anna at biopsitakinga førte med seg ein tilleggsrisiko for pasientane, utan at risikoen kunne forsvarast som ein del av den medisinsk-faglege behandlinga.

Helsetilsynet fatta vedtak om å gi åtvaring til to av prosjektdeltakarane. Vedtaket vart oppretthalde av Statens helsepersonellnemnd. Òg Arbeids- og inkluderingsdepartementet og Sosial- og helsedirektoratet uttalte seg kritisk til prosjektet. Både Helsetilsynet og Helsepersonellnemnda har lagt til grunn at prøvetakinga, uavhengig av samtykkekompetanse, var uforsvarleg. Ut frå den massive kritikken tyder alt på at Datatilsynet er villeidd i søknadsprosessen.

Pålegget om å stanse innhentinga av biopsiar vart følgd, etter det Datatilsynet er informert om. Inklusjon og klinisk oppfølging av prosjektpasientane vart likevel vidareført. Etter det Datatilsynet forstår, var ikkje dei andre delane av prosjektet omfatta av kritikken frå Helsetilsynet.

Regional Etisk Komité (REK) har uttalt at det ikkje er etisk forsvarleg å bruke opplysningar utleidde av biologisk materiale som er innsamla i strid med kravet til forsvarleg helsehjelp.

På denne bakgrunnen fann Datatilsynet det naudsynt å fatte vedtak om sletting av alle personopplysningar knytte til, eller utleidde frå, desse prøvene.

For Datatilsynets vurderingar av konsesjonar til forskingsprosjekt, er det ein føresetnad at prosjektet er i samsvar med anna lovgiving. Dersom Datatilsynet hadde vore kjent med alle sider av korleis prosjektet utvikla seg, ville konsesjon ikkje blitt innvilga.

Kritikkverdig informasjon

Datatilsynet peiker òg på at handtering av informasjonen til dei inkluderte og bruken av samtykkeskriv i denne saka verkar svært kritikkverdig. Dersom konsesjonsinstituttet skal fungere etter føremålet, er Datatilsynet avhengig av at forskingsprosjekt blir gjennomførte i tråd med den oversende prosjektbeskrivinga. Ein konsesjon er eit løyve som i stor grad føreset tillit til at informasjonen gitt av forskaren er korrekt.

9.10 Handel, finans og forsikring

9.10.1 Sletting i nettbutikkar og hotell

På ti tilsyn med hovudføremål å sjå på sletting av kundeopplysningar ved hotell og nettbutikkar, fann Datatilsynet lagring av opplysningar som skulle vore sletta. Det vart avdekt at det langt på veg skuldast eit uklårt forhold til rekneskapslovgivinga.

Rekneskapslovgivinga pålegg lagring av visse typar opplysningar i ein gitt periode. Dei kontrollerte verksemdene hadde IT-system med tett integrasjon mellom rekneskapsopplysningar og kundeopplysningar. Dette gjer det vanskeleg å skilje mellom opplysningar som skal oppbevarast og opplysningar som skal slettast.

9.10.2 Tilsyn hos eigedomsmeklarar

I samband med omsetning av eigedom er det naudsynt å utveksle ei rekkje personopplysningar. Datatilsynet var usikker på om innhenting og utveksling av personopplysningane innan eigedomsmeklarbransjen skjedde på ein tilfredsstillande måte. Tilsynet ønskte derfor å utføre eit avgrensa tal tilsyn mot aktørar i bransjen for å få ein indikasjon på tilstanden.

Det vart i hausten 2007 gjennomført fem tilsyn med ulike eigedomsmeklarføretak, av desse dreiv éi verksemd med utleige av bustad. Datatilsynet fann ein overraskande manglande kjennskap til personopplysningslova.

Eigedomsmeklarbransjen handsamar som hovudregel ikkje sensitive personopplysningar, men det blir handsama opplysningar om økonomiske forhold. Slike opplysningar blir oppfatta av publikum som svært ømtolige, og informasjonsmengda bransjen handsamar må i tillegg reknast for å vere relativt stor.

Den manglande kjennskapen som vart avdekt under tilsyn, ser ut til å vere gjennomgåande for heile bransjen. Datatilsynet vil ta forholda opp med bransjen for å sikre betre kunnskapar om personopplysningslova.

Vedlegg 2

Personvernnemndas årsmelding 2007

1 Samandrag

Dette er Personvernnemndas sjuande årsmelding. I løpet av året har det komme sju klager, av desse er fem ferdighandsama i 2007. Dessutan er seks klager frå 2006 ferdighandsama. I alt har ein altså gjort seg ferdig med 11 klager i løpet av året. Datatilsynets vedtak er omgjort heilt eller delvis i to av dei 11 sakene.

Saksmengda har vore stabil i forhold til 2006. Personvernnemnda går ut frå at saksmengda no vil stabilisere seg på ca 10 – 15 klagesaker i året.

Fleire av sakene har vore komplekse og prinsipielle. Personvernnemnda kan berre ta stilling i konkrete saker, men ser at det på fleire område er trong for ein sektorovergripande rettspolitisk debatt. Nemnda er derfor glad for at Personvernkommisjonen er blitt oppretta. Ein av varamedlemmene i nemnda – Mari Bø Haugstad – er òg medlem av Personvernkommisjonen.

2 Innleiing

Personvernnemnda er oppretta med heimel i lov om behandling av personopplysninger (2000:31). Lova trådde i kraft 1.1.2001. Personvernnemnda er eit klageorgan for vedtak fatta av Datatilsynet etter personvernlova og etter helseregisterlova (2001:24).

Personvernnemnda er eit uavhengig forvaltningsorgan administrativt underlagt Kongen og Fornyings- og administrasjonsdepartementet (FAD). Arbeidet til Personvernnemnda er regulert av personopplysningslova, føresegner til denne, pluss ein instruks som departementet har utarbeidd. Forvaltningslova og offentleglova gjeld òg som for forvaltninga elles.

Jamvel om departementet utarbeider instruks, inneber dette ikkje noka form for instruksjonsmyndigheit i enkeltsaker. Departementet kan ikkje gi generelle instruksar om lovtolking eller skjønnsutøving.

Personvernnemnda skal kvart år orientere Kongen om handsaming av klagesakene.

3 Medlemmer

Personvernnemnda har sju medlemmer som blir oppnemnde for fire år med høve til oppnemning for ytterlegare fire år. Leiar og nestleiar i Personvernnemnda blir oppnemnde av Stortinget, medan dei andre medlemmene blir oppnemnde av Kongen. Første gongs oppnemning skjedde i 2001. I 2005 vart leiar og nestleiar, og medlemmene Siv Bergit Pedersen og Hanne I. Bjurstrøm, oppnemnde for fire nye år. I tillegg vart det oppnemnt tre nye medlemmer.

Personvernnemnda er sett saman av desse personane:

Jon Bing, leiar
Gro Hillestad Thune, nestleiar
Siv Bergit Pedersen
Hanne I. Bjurstrøm
Tom Bolstad
Leikny Øgrim
Jostein Halgunset

I tillegg er det oppnemnt personlege vararepresentantar.

4 Andre organisatoriske forhold

Sekretariatet til Personvernnemnda er Tonje Røste Gulliksen, som vart tilsett som seniorrådgjevar i departementet med tiltreding 1.3.2006. Sekretariatet har frå same dato vore samlokalisert med Forbrukarrådet og Forbrukarombodet i Rolf Wickstrøms veg 15 i Nydalen. Nemnda er svært tilfreds med sekretariatsordninga. Sekretæren avviklar såkalla gradert uttak av fødselspermisjon. Dette har ikkje skapt praktiske problem for arbeidet i nemnda.

Personvernnemnda held møta sine i lokale utanfor Datatilsynet og Regjeringskvartalet for òg på denne måten å markere si sjølvstendige rolle.

Personvernnemnda har eiga heimeside, *www.personvernnemnda.no,* der mellom anna vedtaka er publiserte i sin heilskap. Heimesida har lenke frå Datatilsynets heimeside, og lenker til

personvernrelatert materiale tilgjengeleg på internettet. Personvernnemndas vedtak blir òg publiserte i ein eigen database hos Lovdata, lenka til det andre dokumenterte materialet. Dermed kan ein brukar lett slå opp på Personvernnemndas vedtak ved oppslag på paragraf i personopplysningslova, andre lovar, dommar mv. som vedtaka viser til.

5 Møte og konferansar 2007

Personvernnemnda har i 2007 hatt i alt ni møte. Møta vart i hovudsak nytta til å handsame klagesaker, men òg administrative forhold har vorte handsama. I tillegg til nemndmøte har det vore førebuande møte med sekretariatet og ein eller fleire medlemmer, og enkelte tilsvarande møte med klagaren i samband med handsaming av klagesaker.

Personvernnemnda hadde to kontaktmøte med departementet i 2007, i mai og desember.

Personvernnemnda deltok på den internasjonale konferansen for datatilsynsmyndigheiter i Montreal, Canada. Opphavleg skulle Jon Bing og Tonje Røste Gulliksen delta, men begge vart forhindra frå å møte og varamedlem Mari Bø Haugstad deltok i staden.

Personvernnemnda ytte økonomisk støtte til «Personvernkonferansen 2007», som vart arrangert av Avdeling for forvaltningsinformatikk, Universitetet i Oslo, 7.12.2007. Fleire av medlemmene i Personvernnemnda deltok på konferansen. Tema for konferansen var «Personvern – òg i fremtiden?». Konferansen drøfta framtida for personvernet i ei tid der mange ser ut til å vere pessimistiske når det gjeld utsiktene for personvernet. Konferansen sette lys på personvern og tiltak mot terror og organisert kriminalitet, misbruk av personopplysningar på Internett og arbeidsgivar sin kontrolltrong som kan setje personvernet på prøve. Konferansen var fullteikna.

6 Klagesakshandsaming

Personvernnemnda mottok i 2007 totalt *sju* klagesaker. Fem av desse var ferdighandsama ved utgangen av året. I tillegg vart seks saker frå 2006 ferdighandsama i 2007. Oversikt over vedtaka og vedtaka i sin heilskap er publisert på Personvernnemndas heimesider. I tillegg er vedtaka publiserte i ein eigen database hos Lovdata.

Saksmengda har halde seg stabil i forhold til 2006. Fleire av sakene har vore prinsipielle.

Personvernnemnda vil særleg framheve to forhold i årsmeldinga.

Det første forholdet gjeld dei generelle forvaltningsrettslege problemstillingane som oppstår i nemnda sitt arbeid. I enkelte av sakene som Datatilsynet sender over til Personvernnemnda har det vore forvaltningsrettslege aspekt som nok kunne vore betre førebudde og avklarte før saka vart send til klageorganet.

Det andre forholdet gjeld unntaket i personopplysningslova § 7 for visse formål av omsyn til ytringsfridomen. Nemnda har hatt to saker – PVN-2007-03 Budstikka og PVN-2007-05 Fosterforeldre – som gjaldt personopplysningslova § 7 om journalistiske og opinionsdannande føremål. Når ein nyttar eit funksjonelt journalistomgrep, vil «alle» som skriv på Internett (til dømes på Facebook, i bloggar og nettdebattar) vere unnatekne frå dei vesentlegaste av føresegnene i personopplysningslova. Dermed fell eit stort område – og ei stor gruppe personar, særleg unge menneske – utanfor denne lova. Dette gir ein betydeleg fridom, mellom anna vil det ikkje vere krav om handsamingsgrunnlag for å handsame personopplysningar. Nemnda understrekar at andre materielle lovreglar vil kunne nyttast på dette området, men meiner at det likevel er grunn til rettspolitisk ettertanke.

Saker som er handsama i 2007 er:

PVN-2006-08 Oxigeno Fitness

Klage på Datatilsynet sitt vedtak om at Oxigeno Fitness må avslutte bruken av fingeravtrykk ved inngangskontroll til treningssenter

Fingeravtrykkspålogging. Klage over at Datatilsynet stansa bruk av fingeravtrykkslesar i inngangskontrollen ved treningssenteret Oxigeno Fitness i Oslo. Datatilsynet meinte at det kunne seiast å liggje føre ei sakleg trong for sikker identifisering i tilknyting til inngangskontrollen, men at kravet i lova til nødvendigheit ikkje var oppfylt. Personvernnemnda var einig i Datatilsynets vurdering og tok ikkje klagen til følgje. Nemnda meiner at treningssenteret kan nytte seg av «andre og mindre sikre identifikasjonsmiddel», som likevel er sikre nok til å tilfredsstille det treningssenter treng.

PVN-2006-09 Oslo trimsenter

Klage på Datatilsynet sitt vedtak om at Oslo trimsenter må avslutte bruken av fingeravtrykk ved inngangskontroll til treningssenter

Fingeravtrykkspålogging. Klage over at Datatilsynet stansa bruk av fingeravtrykkslesar i inngangskontrollen ved treningssenteret Oslo trimsenter. Datatilsynet meinte at det kunne seiast å liggje føre ei sakleg trong for sikker identifisering i tilknyting til inngangskontrollen, men at lova sitt krav til kva som er naudsynt ikkje var oppfylt. Personvernnemnda var einig i Datatilsynets vurdering og tok ikkje klagen til følgje. Nemnda meiner at treningssenteret kan nytte seg av «andre og mindre sikre identifikasjonsmiddel», som likevel er sikre nok til å tilfredsstille det treningssenterets treng.

PVN-2006-10 Esso Norge AS

Klage vedrørande bruk av fingeravtrykk ved inngangskontroll

Fingeravtrykkspålogging. Dissens. Klage på Datatilsynets vedtak om at Esso Norge må avslutte bruken av fingeravtrykkslesar på tankanlegg. Esso ønskte å nytte fingeravtrykk i tilknyting til inngangskontroll ved fire ulike tankanlegg, i Fredrikstad, Tønsberg, Trondheim og Bergen. Bruken skulle vere basert på ei samtykkeerklæring og ein «Safety Policy» og skulle sikre at berre autorisert og trena personell vart gitt tilgang til anlegget. Datatilsynet meinte at klagaren har misforstått det første vilkåret i § 12 slik at ei stor trong for fysisk sikring òg gir stor trong for sikker identifisering. Tilsynet fann at fingeravtrykket ikkje blir nytta til identifisering, men til autentisering etter at identifiseringa har skjedd. Datatilsynet meinte òg at lovkravet til nødvendigheit ikkje var oppfylt. Etter Datatilsynets oppfatning kan klagaren oppnå like sikker identifisering ved døgnbemanna inngangskontroll. I følgje tilsynet er manuell visuell kontroll opp mot inngangsbevis eit godt alternativ til bruk av fingeravtrykk. Personvernnemnda meiner at personopplysningslova § 12 dekkjer begge former for bruk av fingeravtrykk som eit «identifikasjonsmiddel», det vil seie både identifisering og autentisering. Ved bruken av kort og fingeravtrykkslesar ved inngangsporten vil (1) personen vere identifisert, og (2) personen vere autentisert. Personen vil dermed få tilgang til tankanlegget. Personvernnemnda er av den oppfatning at det ikkje kan påleggjast – og derfor heller ikkje vurderast – andre typar sikring slik som vakthald, gjerder, høge murar etc, idet dette ligg utanfor personopplysningslova § 12 og middel for sikker identifikasjon ved inngangskontrollen. Nemnda kjem til at det ligg føre sakleg trong for bruk av fingeravtrykkslesar, og at bruken er nødvendig for å oppnå sikker identifisering. Ein medlem kjem til at nødvendigheitsvilkåret i § 12 utelukkar bruk av samtykke som handsamingsgrunn, og vil avvise klagen.

PVN-2006-11 REMA 1000

Klage vedrørande bruk av fingeravtrykk ved registrering av timar

Fingeravtrykkspålogging. REMA 1000 har påklaga Datatilsynets vedtak om at REMA 1000 må avslutte bruken av fingeravtrykk i samband med timeregistrering for dei tilsette. Registrering i terminalen skjer ved at den tilsette tastar sitt tilsettnummer eller ID-nummer. Deretter blir vedkommande bedt om å leggje ein finger på leseplata eller sensoren for å verifisere at det er tasta rett nummer. Datatilsynet er ikkje ueinig i at REMA 1000 har eit sakleg trong for å sikre at lønn blir ført korrekt. Men tilsynet er av den oppfatning at fingeravtrykket ikkje blir nytta for sikker identifisering slik dette er formulert i § 12. Identifisering skjer ved hjelp av tilsettkoden, mens fingeravtrykket blir brukt til autentisering, noko som fell utanfor § 12. Datatilsynet meiner at lovkravet til nødvendigheit heller ikkje er oppfylt. Personvernnemnda har i sak PVN-2006-10 (Esso Norge) komme til at personopplysningslova § 12 dekkjer begge former for bruk av eit «identifikasjonsmiddel» når bruk av fingeravtrykk til autentisering er ein del av eit system for sikker identifisering. Personvernnemnda meiner at det ligg føre eit sakleg trong for sikker identifisering i samband med timeregistrering. Men nemnda finn at nødvendigheitsvilkåret ikkje er oppfylt. Etter nemndas oppfatning kan REMA 1000 nytte seg av «andre og mindre sikre identifikasjonsmiddel» som likevel tilfredsstiller butikkjeda si trong. Klagen blir derfor ikkje teken til følgje.

PVN-2006-12 Bokettersyn hos advokat

Klage på Datatilsynet sitt vedtak om at opplysning om bokettersyn hos advokat ikkje er ein personopplysning

Datatilsynet mottok klage frå ein advokat fordi opplysning frå Tilsynsrådet for advokatverksemd om at det var bestemt å gjere bokettersyn hos advokaten, var blitt offentleggjort. Datatilsynet vedtok at slik opplysning om ein advokat ikkje er ei personopplysning i personopplysningslovas forstand. Personvernnemnda vurderte om det å offentleggjere ei liste over advokatar som er underlagde bokettersyn er i strid med teiepliktføresegna i forvaltningslova fordi dette er «noens

personlige forhold», jf forvaltningslova § 13, 1.ledd nr 1. Nemnda kom til at slike verksemdsrelaterte opplysningar, inkludert bokettersyn hos advokat, fell utanfor teieplikta om personlege forhold. Opplysninga er derfor offentleg. Personopplysningslova § 6 angir at innsynsretten etter forvaltningslova eller offentleglova ikkje blir avgrensa. Klagen vart derfor ikkje teken til følgje.

PVN-2006-13 Personopplysningar i forsikringssak

Klage på Datatilsynet sitt vedtak om å ikkje intervenere i sak om spesialisterklæring utarbeidd i forsikringssak som inneheldt personopplysningar om andre personar enn klagaren

Saka gjeld klage frå ein person om ei spesialisterklæring utarbeidd for Vesta forsikring som inneheld personopplysningar om andre personar enn klagaren. Klagaren skreiv under ei fullmakt til Vesta – Erklæring om fritak for taushetsplikt. Legen tok likevel med informasjon om andre enn klagaren i si spesialisterklæring, mellom anna utleverte denne personopplysningar om klagarens nærmaste familie. Saka vart først klaga inn for Helsetilsynet i Vestfold, som konkluderte med at spesialisterklæringa ikkje er utarbeid i samsvar med god praksis. Helsetilsynet vurderte reaksjonskapittelet i helsepersonellova, men fann at det ikkje dreidde seg om så grov aktløyse at saka burde oversendast Statens helsetilsyn til vurdering som mogleg pliktbrot ut frå helsepersonellova § 55. Datatilsynet viser til at det ikkje har kompetanse til å overprøve den sakkyndige vurderinga, og når Helsetilsynet i Vestfold ikkje meiner at utlevering er i strid med reglane om teieplikt, finn Datatilsynet at det ikkje har rettsleg grunnlag som gjer det naturleg å ta vidare skritt i samband med saka. Personvernnemnda meiner at utlevering av personopplysningar om andre enn den som har samtykt, sannsynlegvis er eit brot på teiepliktføresegnene i helseregisterlova og helsepersonellova. Slik nemnda ser det, har Helsetilsynet i Vestfold funne at utleveringa er eit teiepliktsbrot etter helsepersonellova, men Helsetilsynet konkluderer med at reaksjonskapittelet i helsepersonellova likevel ikkje skal nyttast. Personvernnemnda må derfor leggje dette til grunn. Det finst ingen ytterlegare sanksjonar etter personopplysningslova.

PVN-2007-01 Arvelighetsregisteret

Klage på Datatilsynet sitt vedtak om å plassere handsamingsansvaret for «Arvelighetsregisteret» hos Universitetet i Oslo. Avgjerda inneber samtidig eit avslag på klagaren sin konsesjonssøknad for det aktuelle materialet

Klagaren har påklaga Datatilsynet si avgjerd om å plassere ansvaret for handsaminga av «Arvelighetsregisteret», inkludert «Tvillingregisteret», hos Universitetet i Oslo. Plasseringa av handsamingsansvaret hos UiO inneber samtidig eit avslag på klagarens søknad om konsesjon til det same materialet. Personvernnemnda tek ikkje klagen til følgje og Datatilsynets vedtak blir ståande. Etter nemndas meining kan ein ikkje søkje om å få ein «arbeidskonsesjon» eller «brukskonsesjon» til det same materialet. Etter nemndas meining må det korrekte vere å be om ein tilgang til det materialet som UiO disponerer over som handsamingsansvarlig. Det vil vere opp til UiO som handsamingsansvarleg å handtere førespurnader om tilgang til forskingsmaterialet. Etter nemnda sitt syn er ein professor emeritus ved institusjonen normalt ikkje ein utanforståande tredjeperson ved slike førespurnader. UiO må derfor ta stilling til om vidare forsking skal skje ut frå forskingsetiske prinsipp og arbeidsrettslege retningslinjer.

PVN-2007-02 Bibliotek-Systemer

Klage på Datatilsynet sitt avslag som inneber at Bibliotek-Systemer AS ikkje får utvikle bibliotekteneste som inneber å lage knytingar mellom boktitlar som ulike låntakarar låner – såkalla korrelasjonsdatabase

Bibliotek-Systemer AS har påklaga eit vedtak frå Datatilsynet som går ut på at dei ikkje får utvikle ei bibliotekteneste som inneber å lage knytingar mellom boktitlar som dei ulike boklåntakarane låner – ein såkalla korrelasjonsdatabase. Datatilsynet er av den oppfatning at tenesta inneber ein personverntrussel. Det blir vist til at det opphavlege formålet med biblioteka sine låneopplysningar er å administrere låneforholdet. Som ei følgje av dette skal opplysningane normalt slettast når boka blir levert tilbake, jf personopplysningslova § 28. Nemnda meiner at personverntrusselen er liten, men kjem likevel til at Bibliotek-Systemer AS berre har høve til å etablere ein korrelasjonsdatabase dersom det blir henta inn samtykke f rå dei registrerte.

PVN-2007-03 Budstikka

Klage på Datatilsynet sitt vedtak om å avvise ein førespurnad frå Norsk Eiendomsinformasjon AS om å vurdere om Asker og Bærum Budstikke (her-

etter Budstikka) sin internettbaserte eigedomsbase er lovleg ut frå grunnkrava i personopplysningslova. Datatilsynet meiner at Budstikka si teneste er eit journalistisk produkt som fell innanfor personopplysningslova § 7, og grunngivinga for avvisninga er dermed at grunnkravet i personopplysningslova ikkje kan nyttast på forholdet. Tenesta er med andre ord ikkje i strid med personopplysningslova

Norsk Eiendomsinformasjon AS påklaga Datatilsynets vedtak om at Budstikka si Internettbaserte eigedomsbase er lovleg. Datatilsynet meinte at Budstikka si teneste er eit journalistisk produkt som fell innanfor unntaket i personopplysningslova § 7, og personopplysningslova sine grunnkrav kjem dermed ikkje i bruk. Personvernnemnda er einig i vurderinga til Datatilsynet. Budstikka har brukt dei «tørre» tal og fakta frå NE til å lage ein lesevennleg, brukarvennleg og søkbar database over eigedomsoverdragingar i Asker og Bærum. Nemnda har likevel merknader fordi partane ikkje er verna etter personopplysningslova og Datatilsynet burde ha eksplisitt oppgitt lovheimel for vedtaket.

PVN-2007-04 Kolumbuskortet

Klage på Datatilsynet sitt vedtak om at Rogaland Kollektivtrafikk FKF må endre løysing for etablering av elektronisk billettering for passasjerar

Rogaland Kollektivtrafikk FKF påklaga Datatilsynet si avgjerd om etablering av eit elektronisk reisekort, Kolumbuskortet, der passasjeren har «reisekonto» på internett og reisemønster blir lagra. Kolumbus sende ei risikovurdering til Datatilsynet. Datatilsynet meinte at denne risikovurderinga ikkje var i samsvar med kva personopplysningsforskrifta kapittel 2 krev, eller i alle fall var den ikkje tilstrekkeleg dokumentert. Tilsynet konkluderte derfor med at dette var ein vesentleg mangel som gjorde at løysinga ikkje kunne brukast. Personvernnemnda er kommen til at det må liggje føre ei tilfredsstillande risikovurdering før løysinga kan vurderast. Tilsynet burde derfor ha påpeikt manglar ved den oversende risikovurderinga, og gitt Kolumbus høve til å rette opp desse, før tilsynet vurderte løysinga. Nemnda er derfor kommen til at vedtaket frå Datatilsynet skal opprettholdast på formelt grunnlag, slik at Kolumbus kan skaffe fram ei risikovurdering som er i samsvar med forskrifta. Først når det ligg føre ei risikovurdering som er i samsvar med lov og forskrift, kan ein vurdere sjølve løysinga, irekna spørsmål om lagringstid for reisemønster og informasjonstryggleiken.

PVN-2007-05 Fosterforeldre

Klage på Datatilsynet sitt vedtak om at publisering av personopplysningar om fosterforeldre på internettside fell inn under unntaket i personopplysningslova § 7 om handsaming av personopplysningar utelukkande for journalistiske, irekna opinionsdannande, formål

Klage på Datatilsynets vedtak om at publisering av personopplysningar om fosterforeldre på internettside fell inn under unntaket i personopplysningslova § 7 om handsaming av personopplysningar utelukkande for journalistiske, irekna opinionsdannande, formål. Nemnda var einig med Datatilsynets vurderingar. Det var på det reine at oppførselen, utsjånaden etc til fosterforeldra var kommentert på nettsida, men dette måtte likevel seiast å liggje innanfor rammene av ytringsfridomen, og dermed ytringar med «utelukkande opinionsdannande formål». Datatilsynets vedtak vart oppretthalde.

7 Rekneskap og budsjett for 2007

Personvernnemnda hadde i 2007 ei budsjettramme på kr 1 600 000, og kjem fram under kap 1500 Fornyings- og administrasjonsdepartementet i statsbudsjett for 2007. Totalt forbruk: kr 812 293. Personvernnemnda disponerte løyvinga si til innkjøp av nødvendig teknisk utstyr, litteratur, tenester, økonomisk støtte til konferanse, deltaking på seminar og den internasjonale konferansen, arbeidsgodtgjersle og reisegodtgjersle til medlemmene i nemnda, lønn til sekretariat og leige av lokale.

Oslo, 8. februar 2008
For Personvernnemnda
Jon Bing (leiar)

Offentlege institusjonar kan tinge fleire eksemplar frå:
Servicesenteret for departementa
Post og distribusjon
E-post: publikasjonsbestilling@dss.dep.no
Faks: 22 24 27 86

Opplysningar om abonnement, laussal og pris får ein hjå:
Akademika AS
Avdeling for offentlege publikasjonar
Postboks 84 Blindern
0314 OSLO
E-post: offpubl@akademika.no
Telefon: 22 18 81 00
Telefaks: 22 18 81 01
Grønt nummer: 800 80 960

Omslagsillustrasjon:
Departementenes servicesenter

Publikasjonen er også tilgjengeleg på:
www.regjeringa.no

Trykk: 07 Gruppen AS – 10/2008